FATF

EAG

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Anti-money laundering and counter-terrorist financing measures

Russian Federation

Mutual Evaluation Report

December 2019

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CTF) standard.

For more information about the FATF, please visit the website: **www.fatf-gafi.org.**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

This assessment was adopted by the FATF at its October 2019 Plenary meeting.

Citing reference:

FATF (2019), *Anti-money laundering and counter-terrorist financing measures – Russian Federation,*
Fourth Round Mutual Evaluation Report, FATF, Paris
http://www.fatf-gafi.org/publications/mutualevaluations/documents/russian-federation-2019.html

Table of Contents

Executive Summary

1. This report summarises the AML/CFT measures in place in the Russian Federation (hereafter referred to as Russia) as at the date of the on-site visit (11-29 March 2019). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Russia's AML/CFT system, and provides recommendations on how the system could be strengthened.

Key Findings

1. Rosfinmonitoring is core to the functioning of Russia's AML/CFT regime, as it is responsible for leading and co-ordinating policy and operational activities in the field of AML/CFT. This work is strongly supported, including legislatively, as AML/CFT is afforded the highest priority by the Russian government. Domestic co-ordination and co-operation is a major strength of the Russian AML/CFT system.
2. Russian authorities have an in-depth understanding of the country's ML and TF risks, as outlined in Russia's 2018 ML and TF NRAs and communicated by authorities to the assessment team. Both ML and TF risks are well identified and understood by all authorities. FIs have a good understanding of these risks, while other reporting entities' understanding varies.
3. Rosfinmonitoring has a wealth of available data, including a large volume of reporting, and employs sophisticated technologies and high degree of automation, to prioritise, generate, and contribute to investigations pursued by law enforcement authorities (LEAs). LEAs routinely and effectively access and use this financial intelligence to investigate ML, TF, predicate offenses, and to trace criminal proceeds. Prosecutors further ensure the use of financial intelligence in case development by systematically reviewing investigations to verify that LEAs pursue all financial aspects.
4. Russia is investigating ML partly in line with its risk profile. LEAs routinely conduct financial investigations alongside predicate offences. Most ML investigations involve the acquisition or sale of criminal proceeds, so the majority of cases relate to less serious offences. Self-

laundering is frequently investigated, unlike third-party ML, which is detected and investigated to a lesser extent. Some complex ML is pursued, however more opportunities for LEAs to uncover and investigate sophisticated and/or high-value ML may exist, especially in the financial sector and involving proceeds sent abroad, particularly those related broadly to corruption. Sanctions applied against natural persons for ML are moderately effective, and while Russia cannot prosecute legal persons, the use of administrative sanctions against legal persons was not demonstrated. Alternative measures are a notable part of Russia's toolkit to combat financial and shell company-related offences potentially related to ML.

5. Russia has a robust legal framework for combatting TF, which is largely in line with international standards. On average, Russia pursues 52 TF prosecutions per year. Since 2013, Russia has convicted more than 300 individuals of TF, with the majority resulting in sentences of imprisonment ranging from 3-8 years. Russia demonstrates that it deprives terrorists, terrorist organisations and terrorist financiers of assets and instrumentalities through various approaches, such as through terrorist designations, administrative freezes, court orders, and confiscation. While the total amount of assets and instrumentalities deprived is relatively low, this is consistent with Russia's risk profile.

6. Overall, Russia has an adequate system to implement TF and proliferation financing (PF) targeted financial sanctions (TFS), but has gaps and weaknesses in some areas, including TFS implementation without delay and a lack of explicit, legally enforceable requirements that extend to all natural and legal persons (beyond reporting entities).

7. There is a widespread and persistent trend of non-compliance with preventive AML/CFT obligations particularly in the financial sector. Although breaches have been decreasing in recent years, the absolute figures are still worrisome. The threshold for suspicious transaction reporting is low and automation in filing leads to a massive number of reports, which, while used in the FIU's datamining, are not detailed or suited for flagging a high level of suspicion or urgency. This increase in STRs could be leading to more terminations of business relationships and refusals to conduct transactions due to ML/TF concerns. Group-wide information sharing among FIs was not possible in Russia until the on-site visit.

8. The Bank of Russia (BoR) has implemented some aspects of risk-based supervision since 2013, and has recently improved the risk-based approach to supervision. Licensing requirements for FIs were strengthened in 2013 and now largely mitigate the risk of criminals being the owners or the controllers of FIs. However, supervision is mostly based on prudential factors and the BoR over- relies on remote monitoring. While a number of licence revocations have occurred, sanctions are not effective or dissuasive in all cases and monetary penalties imposed are low.

9. Russia has improved its legal framework and operational approach to enhance transparency of legal persons, which makes it more difficult to misuse a legal person established in Russia. Registration requirements have been enhanced and legal persons are constantly being reviewed and removed for providing inaccurate information or for inactivity. Legal persons maintain information on their beneficial owners and authorities effectively supervise the implementation of this requirement. FIs and DNFBPs also collect beneficial ownership information of customers, but have somewhat limited capacity to verify it.

Risks and General Situation

2. Russia is generally perceived as a source country for proceeds of crime, and is not a major centre for laundering the proceeds of crime committed in other countries. Nevertheless, Russia is exposed to a wide range of ML risks.

3. Russia has conducted NRAs for ML and TF. Assessors largely agree with the results. The ML NRA identifies embezzlement of public funds, crimes related to corruption and abuse of power, fraud in the financial sector, and drug trafficking as the prevalent types of criminal activity with the potential to generate illicit proceeds. A large proportion of criminal proceeds generated in Russia are laundered abroad, as recognised by the ML NRA, which makes the pursuit of proceeds of crime to other countries an important focus for the assessment. The assessment team also considered the risks associated with organised crime and cyber-crimes, which occur alongside the threats identified in the NRA.

4. Russia is not a global financial centre, but does have a significant banking sector primarily serving domestic customers and including many small banks. The sector has undergone significant structural changes in recent years primarily driven by supervisory actions – through closures, mergers, and acquisitions – which has halved the number of active banks. The assessment team looked at the reasons for this consolidation and its impact on how well the sector implements preventive measures against ML and TF.

5. The main TF risks in Russia relate to foreign terrorist fighters (FTFs) destined for and returning from ISIL-controlled areas of Iraq and Syria, but Russia also faces domestic terrorist threats. The assessment team reviewed the measures taken to combat all terrorist threats and associated financing, including the remaining threat posed by armed groups in the North Caucasus.

Overall Level of Compliance and Effectiveness

Assessment of risk, co-ordination and policy setting (Chapter 2; IO.1; R.1; 2; 33 & 34)

6. Russian authorities have a very developed understanding of the country's ML/TF risks. Identification and assessment of ML/TF risks is done as a systemic exercise, which benefits from the high-level political commitment and the participation of all major stakeholders from both the public and the private sectors. The ML NRA uses a large amount of quantitative and qualitative data from a multiplicity of public

and non-public sources. The methodology of the ML NRA is generally sound, although some improvements could be made.

7. The ML risks identified seem comprehensive and reasonable. The authorities met on-site demonstrated advanced understanding of and clear views on the constituents of risk, are aware of the most relevant countrywide and sector-specific risks, including the applicable risk scenarios, methods and tools.

8. TF risks are well identified and understood. The TF NRA is high-level and does not provide granular information about specific threats. Nevertheless, it is usefully supplemented by the in-depth knowledge of the criminal intelligence and investigation staff of the LEAs involved in counter-terrorism. Rosfinmonitoring has a key role in identification of TF-related threats and generation of relevant intelligence output.

9. National AML/CFT policies appropriately address identified ML/TF risks. There is an on-going and consistent policy development process in Russia, which builds on the outcomes of formal risk assessments and other articulations of risks (such as the annual threat assessment reports produced by Rosfinmonitoring since 2013). Relevant national strategies and ML and TF action plans derived from the outcomes of 2018 NRAs represent the national policies at the strategic and operational levels aimed at combating ML/TF in the country. Domestic co-ordination and co-operation is a major strength of the Russian AML/CFT system.

Financial intelligence, ML investigations and prosecutions, and confiscation (Chapter 3; IO.6, 7, 8; R.1, 3, 4, 29–32)

10. Russian LEAs routinely and effectively access and use financial intelligence and other relevant information to develop evidence to investigate ML, TF, predicate offenses, and to trace criminal proceeds. Prosecutors further ensure the use of financial intelligence in case development and they systematically review investigations to verify that LEAs pursue all financial aspects.

11. Rosfinmonitoring is core to the functioning of Russia's AML/CFT regime. Rosfinmonitoring has a wealth of available data, including a large volume of STRs (20 million per year, on average) and MCRs (another 10 million per year, on average). It employs sophisticated technologies and a high degree of automation, to prioritise, generate, and contribute to cases pursued by LEAs. Rosfinmonitoring is a well-resourced and data-driven FIU with competent analysts that has a uniquely wide view into the Russian financial system.

12. To a large extent, Rosfinmonitoring's financial analysis and dissemination support the operational needs of relevant LEAs. LEAs also demonstrated that the financial intelligence either received from Rosfinmonitoring, spontaneously or upon their request, is of high quality and integral to their activities.

13. Rosfinmonitoring's close co-operation and co-ordination with its domestic counterparts greatly contributes to Russia's effectiveness.

14. ML is generally well identified through financial investigations, and when it is identified, the authorities open ML investigations in more than 91% of instances, with most cases resulting in charges. LEAs routinely conduct financial investigations when looking into predicate offences, but usually do not pursue ML outside of

predicate investigations. Self-laundering is frequently investigated, unlike third-party ML, which is detected and investigated to a lesser extent. The investigative process is rather formal, which brings efficiency and productivity, but ML investigations may not be opened or completed when there is evidence of a more easily provable alternative charge.

15. Russia is investigating ML activity partly in line with its risk profile, as approximately 85% of ML offences detected related to the high-risk areas denoted in the NRA, such as drug crimes and crimes with public funds. In the area of bribery, the number of ML cases pursued is not entirely aligned with risk, even though there are many corruption predicate investigations and thousands of recent convictions. While Russia is investigating and prosecuting offences stemming from some notorious, multinational laundromats, including by investigating complicit professionals in the financial sector, the authorities are not sufficiently targeting bankers who facilitate ML.

16. Sanctions applied against natural persons for ML are partly effective, proportionate, and dissuasive, as terms of imprisonment for ML and fines are on the low-end, with some exceptions. Per fundamental principles, Russia cannot prosecute legal persons, but the use of administrative sanctions against legal persons was not demonstrated.

17. Russia beneficially employs alternative measures to prosecute financial crimes that could be indicative of, or occur in connection with, ML activity. These offences do not necessarily involve proceeds of crime and it is not always apparent why ML investigations or charges are not simultaneously pursued. The most impactful alternative offence used is illegal banking, followed by the outflow offence and offences related to shell companies. These measures disrupt schemes that may represent third-party ML infrastructure. However, they require less investigation into the full scope of the criminal conduct and may not be as easily recognised by other countries when co-operation is sought.

18. Russia pursues confiscation as a policy objective and traces the proceeds and instrumentalities of crime. Provisional measures are used well, including for equivalent value. The overall statistical picture on many of the facets of confiscation, broadly defined, is solid.

19. Authorities focus on compensating victims, so restitution figures are higher than criminal confiscation figures. This is appropriate in the Russian context where many offences in the high-risk areas of crimes with public funds, as well as financial sector crimes such as fraud, embezzlement, and misappropriation, have identifiable victims. Restitution is the priority and criminal confiscation is used when legal owners cannot be identified or for offences that create proceeds but do not cause pecuniary loss. Confiscation of the unexplained wealth of public officials is showing more results year over year.

20. Confiscation regarding falsely or non-declared movements of currency and bearer negotiable instruments (BNI) is pursued to a lesser extent, partly due to the lack of a declaration obligation within the Eurasian Economic Union (EAEU). Considering Russia's vast land borders and other relevant risk and context, a relatively low percentage of smuggled cash that is identified is confiscated. However, detected smuggling offences and imposed fines appear to partly offset these limited confiscations.

21. Russia recognises the threat posed by the misuse of virtual assets (VA), especially as related to drug trafficking and internet-enabled crime. LEAs can trace but cannot confiscate virtual assets until they are exchanged into property, as legally defined, and while some ML cases have featured VA, an ML charge cannot yet be solely based on transactions involving VA.

Terrorist and proliferation financing (Chapter 4; IO.9, 10, 11; R. 1, 4–8; 30-31; and 39)

22. Russia has a robust legal framework for combatting TF, which is largely in line with international standards.

23. LEAs and prosecutors must consider in the course of each criminal investigation whether there are indications of other crimes and whether property has been used or intended for use to finance terrorism or groups engaged in such activity. This requirement has the effect of ensuring that the investigation of the financial aspects of terrorist crimes is mandatory. In practice, LEAs systematically consider the financial component of terrorist activities, which had led to the detection, identification and investigation of TF. Russia is able to identify different methods of TF and the role played by financiers.

24. On average, Russia pursues 52 TF prosecutions per year. Since 2013, Russia has convicted more than 300 individuals of TF, with the majority of cases resulting in sentences of imprisonment ranging from 3-8 years.

25. Russia demonstrates that it deprives terrorists, terrorist organisations and terrorist financiers of assets and instrumentalities through various approaches, such as through terrorist designations, administrative freezes, court orders, and confiscation. While the total amount of confiscated assets and instrumentalities is relatively low, this is consistent with Russia's risk profile.

26. Overall, Russia has an adequate system to implement TFS, but major gaps and weaknesses exist in some areas, including TFS implementation without delay and a lack of explicit, legally enforceable requirements that extend to all natural and legal persons (beyond reporting entities).

27. Russia's domestic TFS regime has both terrorism and extremism activity as potential grounds for designation. The process for accessing frozen funds differs between the "international" list (which relates to UN designations) and the domestic list. As a result, the assessment team noted confusion among reporting entities met on-site regarding the various lists (UN lists, domestic terrorism list, domestic extremism list) and their respective procedures to seek special exemptions or access to frozen funds.

28. While Russia identified the overall TF risk associated with NPOs as low, some parts of the sector were assessed as medium-risk and subject to additional controls. Russian authorities are conducting risk-based outreach to and supervision of NPOs.

Preventive measures (Chapter 5; IO.4; R.9–23)

29. FIs have procedures in place to identify, assess, understand and document their individual risks, including through a periodic risk assessment exercise. FIs have implemented adequate mitigation measures by profiling their customers based on ML/TF risks and applying adequate measures for CDD, record-keeping and monitoring.

30. Overall, there is a fair level of implementation of the requirements among FIs related to the identification of BO, but some FIs apply a rules-based definition of BO (i.e. identifying senior management officials as soon as no natural person is identified as owning 25% or more of legal persons). This may be due to a superficial understanding of the definition of BO.

31. The understanding of risks by DNFBPs, as a whole, is fair. Certain sectors have a good understanding (e.g. accountants and auditors). Others have a less developed (casinos, real estate agents) or superficial (lawyers and notaries) risk understanding. Risk understanding by DPMS is not considered to be in line with the risk identified in the ML NRA.

32. DNFBPs rate customers based on ML/TF criteria and apply CDD and EDD measures accordingly. While DNFBPs are aware of their STR obligations, few are filing an adequate amount of STRs.

Supervision (Chapter 6; IO.3; R.14; 26–28; 34-35)

33. The banking sector is exposed to a high level of threat from criminals. Since 2013, the number of credit institutions (CIs) licenced in Russia was halved due to mergers and the revocation of many licences (including for serious violations of AML/CFT provisions). The licensing requirements for FIs has improved since 2013 and now largely mitigate the risk of criminals being the owners or the controllers of FIs; however, deficiencies in licensing remain.

34. Since 2013, the Bank of Russia (BoR) has put in place an intense bank supervisory programme informed by AML/CFT risks. Planned on-site inspections follow a time-bound cycle, to which AML/CFT components can be added. Targeted (ad hoc) inspections, solely focused on AML/CFT can be organised, however, few have been carried out. BoR has shifted its supervisory strategy from on-site inspections to remote supervision, which uses algorithms to identify possible involvement in suspicious transactions and detect potential AML/CFT breaches. Assessors are concerned that an insufficient number of on-site inspections for AML/CFT issues is taking place, and consider that the current BoR supervision model over-relies on remote forms of supervision. AML/CFT supervision for non-credit FIs has only recently moved to a risk-based approach and the resource allocation to sectors is not fully in line with sector risks.

35. Overall compliance by FIs has improved in recent years. A significant number of licence revocations for serious AML/CFT violations has had a cleansing effect. However, monetary penalties imposed for AML/CFT breaches are relatively low.

36. Roscomnadzor and DNFBP supervisors have their own risk assessment methods, however, the ML/TF risk understanding was largely improved after the NRA process. Rosfinmonitoring has conducted AML/CFT specific on-site and off-site inspections of DNFBPs under its remit using a risk-based approach. Other DNFBP

sectors undergo supervision for prudential and conduct of business purposes, which can include AML/CFT issues. Supervision of the DPMS sector should be more focused on AML/CFT compliance, based on a comprehensive understanding of risk exposure, including as identified in by the NRA.

Transparency and beneficial ownership (Chapter 7; IO.5; R.24, 25)

37. The risk of misuse of legal persons in ML schemes is high. Russia has put in place a number of mechanisms that significantly mitigate the misuse of legal persons for ML/TF purposes. In particular, there are stringent rules at registration, and since 2017, authorities have strengthened measures to identify inaccurate information and inactive companies. As a result, the accuracy of the company register (the USRLE) has improved, which makes its information more useful for LEAs and others.

38. The company register is mainly source of legal ownership information, but it can be a source of BO information where (i) all the shareholders are in the register and (ii) no doubts arise as to other persons being the BO. Credit institutions are also a source of BO information, although the verification of information by reporting entities is largely based on the company register, which may not always hold BO information. A challenge exists in relation to accessing accurate BO information when a foreign person owns a Russian legal person.

39. There is a good co-operation in investigative activities between the Federal Tax Service (FTS) and Rosfinmonitoring, as well as between FTS and LEAs. This has resulted in a large number of administrative and criminal sanctions, which contribute to making legal persons less attractive to criminals. The sanctions have, however, a limited range and level of dissuasiveness.

40. TCSPs are not considered as a distinct economic activity and are not covered by the AML/CFT law. While services provided to companies are tightly regulated, they are not properly supervised. Certain legitimate corporate services are provided, in particular by legal professionals. Legal professionals are AML/CFT obliged entities, yet they are not properly supervised and, as such, cannot be relied upon to hold adequate, accurate and current basic or BO information.

International co-operation (Chapter 8; IO.2; R.36–40)

41. In general, Russia provides mutual legal assistance (MLA) in a constructive and timely manner and swiftly executes extradition requests. Russia prioritises its responses based on the urgency indicated by the requestor, whether the request corresponds with the risks identified in the ML/TF NRAs, and legal constraints on detention of persons. An electronic case management system for the entirety of GPO assists in controlling the execution of incoming requests. Formal co-operation appears to function well in practice. Feedback on MLA and extradition as provided and sought by Russia was mainly positive.

42. Co-operation provided by Russia pertaining to asset tracing appears to be adequate. The majority of Russian requests to identify assets stem from ML investigations and the number of requests for asset identification and seizure are beginning to keep pace with suspected proceeds moved offshore.

43. Rosfinmonitoring co-operates well with foreign FIUs. To facilitate the exchange of information, it has concluded more than 100 international co-operation

agreements and is able to co-operate on basis of reciprocity. Egmont mechanisms are used for information exchange, along with other protected channels (e.g. diplomatic), and, where necessary and practicable, face-to-face meetings with foreign counterparts.

44. There are mechanisms for supervisory co-operation by the BoR, including over 30 agreements with counterparts. In its capacity of mega-regulator for the financial sector, the BoR co-operates with foreign central banks and financial regulators, but sustained relationships have not yet been developed.

45. Russia provides information on basic and BO information of legal persons. Requests for BO information comprise a relatively modest share within the total number of incoming ML requests. The authorities suggest that Russian legal persons are rarely used in foreign ML schemes and have a simple ownership structure, which diminishes the frequency of such requests.

Priority Actions

1. Russia should refine its supervisory approach to ensure that it is sufficiently ML/TF risk sensitive and independent from prudential supervision for both FIs and DNFBPs. In particular, financial supervisors should schedule sufficient AML/CFT inspections and more frequent unscheduled inspections when merited. Off-site supervision should be modified by developing more sensitive means to determine the risk profile of individual supervised institutions.
2. LEAs and prosecutors should prioritise the investigation and prosecution of complex money laundering, including professional ML linked to proceeds generated in Russia and transferred for further laundering abroad.
3. In investigating shadow financial schemes, authorities should ensure that the sources of funds and potential links to predicate offences are fully analysed. Authorities should continue to use effective alternative offences when warranted, but pursue ML investigations and consider whether a third-party ML charge is more appropriate, especially in cases where using the ML offences may facilitate international co-operation.
4. Russia should take action to implement TFS without delay and require all natural and legal persons within Russia to freeze assets and not make any funds, financial assets or economic resources available for the benefit of UN designated persons or entities, whether directly or indirectly.
5. Russia should consider ways to strengthen obliged entities' understanding of BO requirements and their implementation, particularly to identify legal persons owned or controlled by sanctioned entities, namely through complex structures, in order to detect possible instances of PF sanctions evasion.

Effectiveness & Technical Compliance Ratings

Effectiveness Ratings[1]

IO.1 - Risk, policy and coordination	IO.2 International cooperation	IO.3 - Supervision	IO.4 - Preventive measures	IO.5 - Legal persons and arrangements	IO.6 - Financial intelligence
Substantial	Substantial	Moderate	Moderate	Substantial	High
IO.7 - ML investigation & prosecution	**IO.8 - Confiscation**	**IO.9 - TF investigation & prosecution**	**IO.10 - TF preventive measures & financial sanctions**	**IO.11 - PF financial sanctions**	
Moderate	Substantial	High	Moderate	Moderate	

Technical Compliance Ratings[2]

R.1 - assessing risk & applying risk-based approach	**R.2** - national cooperation and coordination	**R.3** - money laundering offence	**R.4** - confiscation & provisional measures	**R.5** - terrorist financing offence	**R.6** - targeted financial sanctions – terrorism & terrorist financing
LC	C	LC	LC	LC	PC
R.7- targeted financial sanctions - proliferation	**R.8** -non-profit organisations	**R.9** – financial institution secrecy laws	**R.10** – Customer due diligence	**R.11** – Record keeping	**R.12** – Politically exposed persons
PC	LC	C	LC	LC	PC
R.13 – Correspondent banking	**R.14** – Money or value transfer services	**R.15** –New technologies	**R.16** –Wire transfers	**R.17** – Reliance on third parties	**R.18** – Internal controls and foreign branches and subsidiaries
LC	LC	C	PC	LC	LC
R.19 – Higher-risk countries	**R.20** – Reporting of suspicious transactions	**R.21** – Tipping-off and confidentiality	**R.22** - DNFBPs: Customer due diligence	**R.23** – DNFBPs: Other measures	**R.24** – Transparency & BO of legal persons
LC	C	LC	LC	LC	LC
R.25 - Transparency & BO of legal arrangements	**R.26** – Regulation and supervision of financial institutions	**R.27** – Powers of supervision	**R.28** – Regulation and supervision of DNFBPs	**R.29** – Financial intelligence units	**R.30** – Responsibilities of law enforcement and investigative authorities
PC	LC	LC	LC	C	LC
R.31 – Powers of law enforcement and investigative authorities	**R.32** – Cash couriers	**R.33** – Statistics	**R.34** – Guidance and feedback	**R.35** – Sanctions	**R.36** – International instruments
C	LC	C	LC	LC	LC
R.37 – Mutual legal assistance	**R.38** – Mutual legal assistance: freezing and confiscation	**R.39** – Extradition	**R.40** – Other forms of international cooperation		
LC	LC	LC	LC		

1 Effectiveness ratings can be either a High- HE, Substantial- SE, Moderate- ME, or Low – LE, level of effectiveness.

2 Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC – partially compliant or NC – non compliant.

MUTUAL EVALUATION REPORT

Preface

This report summarises the AML/CFT measures in place as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT system, and recommends how the system could be strengthened.

This evaluation was based on the 2012 FATF Recommendations, and was prepared using the 2013 Methodology. The evaluation was based on information provided by the country, and information obtained by the evaluation team during its on-site visit to the country from 11-29 March 2019.

The evaluation was conducted by an assessment team consisting of:

- Mr. José Luis GRACIA, SEBLAC, Spain (FIU expert)
- Ms. Marybeth GRUNSTRA, Department of Justice, United States of America (legal/law enforcement expert)
- Mr. Nuno MATOS, AML/CFT Coordination Commission, Portugal (legal/financial expert)
- Mr. Arakel MELIKSETYAN, Financial Monitoring Center, Central Bank of Armenia (financial and FIU expert)
- Ms. Giovanna PERRI, Directorate for Prevention of Financial Crimes, Ministry of the Economy and Finance, Italy (sanctions/law enforcement expert)
- Ms. Zhongyuan ZHANG, AML Bureau, The People's Bank of China (financial expert)

The assessment process was managed by Mr. Tom NEYLAN, Senior Policy Analyst, Ms. Kristen ALMA and Mr. Francesco POSITANO, Policy Analysts, all FATF Secretariat. The report was reviewed by Mr. Jaakko CHRISTENSEN (Finland); Ms. Bhumii BHATT (United Kingdom); Mr. Timur SABIROVTO (Kyrgyz Republic); and Mr. Andrew STRIJKER (MONEYVAL Scientific Expert).

Russia previously underwent a FATF Mutual Evaluation in 2008, conducted according to the 2004 FATF Methodology. The 2008 evaluation and six follow-up reports (last one published in 2013) are available at www.fatf-gafi.org/countries/n-r/russianfederation/documents/fur-russia-2013.html.

The 2008 Mutual Evaluation concluded that the country was compliant with 10 Recommendations; largely compliant with 13; partially compliant with 21; and non-compliant with three (and received not applicable on two). Russia was rated compliant or largely compliant with 11 of the 16 Core and Key Recommendations.

In October 2013, the FATF recognised that Russia had made significant progress in addressing the deficiencies identified in the 2008 Mutual Evaluation Report and was removed from the regular follow-up process. At that time, Russia received re-ratings on all Core and Key Recommendations rated non-compliant and partially compliant in its 2008 MER (i.e. old R. 1, 5, SRIV, 23, SRIII).

CHAPTER 1. ML/TF RISKS AND CONTEXT

46. The official name of the country is the Russian Federation. The territory of Russia is 17 million square kilometres (the largest in the world) and the country's population is 142.8 million people.[3] Russia is a multi-ethnic state characterised by ethnocultural diversity. Russia is divided into eight federal districts.

47. Russia has international borders with 16 states. On the eastern side, Russia borders DPRK, China, Mongolia, Kazakhstan, Azerbaijan, and Georgia. On the western side, it borders Ukraine, Belarus, Latvia, Estonia, Finland, and Norway. Part of Russia, the Kaliningrad region, is bordered by Lithuania and Poland. Russia also has sea borders with the United States and Japan

48. The Russian economy is the eleventh largest in the world in terms of GDP. According to the IMF, the volume of GDP in 2018 amounted to USD 1.61 trillion (USD 11 000 per capita).[4] The monetary unit is the Russian rouble.

49. Russia is a democratic, federative state with a republican form of government exercised through three branches—legislative, executive, and judicial. Russia is a presidential republic and the president is the head of state, chosen by universal election. State power in Russia is exercised by the President, a parliament of two houses known as the Federal Assembly (consisting of the State Duma and the Federation Council), the Government of Russia (headed by the Prime Minister), and the courts. Russia has a Constitution dating from 1993 and law is made at the federal level.

ML/TF Risks and Scoping of Higher Risk Issues

Overview of ML/TF risks

50. Russia's exposure to ML risks is primarily as a source of proceeds of crime. Russia is not a major international financial centre (although it is a regional centre for Eurasian countries), nor is it a major hub for company formation or corporate services. However, it faces significant ML risks as a result of the proceeds of crimes committed within Russia, including those related to its high levels of corruption and its role as both a transit and destination country for narcotics trafficking. Russia's 2018 ML NRA identifies the most significant proceeds-generating predicate offences as: embezzlement of public funds and tax crimes; crimes related to corruption/abuse of power; fraud in financial sector; and drug trafficking. Organised crime is also identified as a threat in numerous state policies relevant for the understanding of risk. It is not considered as a distinct category of predicate offending, but rather as an organised manner of committing another underlying type of criminal activity. There is no overall

[3] All-Russia Census of 2010

[4] *World* Economic *Outlook*, IMF, April 2019, www.imf.org/external/datamapper/NGDPD@WEO/OEMDC/ADVEC/WEOWORLD/RUS

estimate available of the value of criminal proceeds in Russia. Authorities estimate the damages and losses resulting from all investigated criminal cases as averaging approximately RUB 220 billion per year during 2014-18.

51. Russia faces significant threats from domestic and international terrorism, and their associated financing. Russia has for several decades faced a severe domestic terrorism threat related primarily to illegal armed groups operating from the North Caucasus and the country has been the site of numerous major attacks. In recent years, the threat from North Caucasus groups has reduced, but Russia has faced increasing threats from international terrorist organisations, notably ISIL, resulting both from Russia's major role in combating ISIL in Syria and from the activity of FTFs.

Country's risk assessment & scoping of higher risk issues

52. Russia has prepared annual reports on ML and TF risks since 2013 and completed its first comprehensive national risk assessments for ML and for TF in June 2018. Both assessments were led by Rosfinmonitoring, using its own methodology. The NRAs drew input from a wide range of relevant stakeholders and authorities and used a comprehensive base of information, as set out below in the assessment of IO.1. While formal NRAs were completed for the first time in 2018, Rosfinmonitoring has since 2013 been responsible for identifying and assessing risks and has drawn on its prior risk analysis when preparing the formal NRAs.

53. The ML NRA seeks to identify the most significant proceeds-generating offences (noted above) and the methods most commonly used to launder the proceeds of crime in Russia. The high-risk group includes the most frequently used ML methods and tools, such as the use of front/ shell companies, the use of non-resident legal persons and arrangements, trade-based ML through fictitious economic activity abroad, people affiliated with public officials, the misuse of electronic payments and virtual currencies, and cash operations. It is notable that, while a number of different methods are used to achieve this, most of the high risk methods and tools identified in the NRA involve moving funds out of Russia illicitly in order to further launder those funds in other countries.

54. The TF NRA considers the specific threats posed by different forms of terrorist activity, including illegal armed groups operating in the North Caucasus, cells of international terrorist organisations operating in the country, Russian FTFs traveling to or returning from conflict zones, FTFs transiting through Russia to travel to or return from conflict zones, and perpetrators recruiting Russian nationals in terrorism through the use of social media or the Internet. The assessment takes into account the different stages of TF, and the mitigating measures in place. It concludes that the methods and techniques used are common to all the terrorist groups active in Russia.

55. The assessors reviewed Russia's 2018 ML and TF NRAs, as well as information from reliable third party sources (such as reports from other international organisations) in order to identify issues for enhanced focus in the course of this assessment. The issues identified were the following:

a) **Corruption and embezzlement of public funds:** The assessors consider corruption as a high-risk area for ML. The ML NRA identifies corruption and

embezzlement of public funds as generating significant criminal assets.[5] Levels of corruption are steadily high in Russia.[6] While important initiatives have been taken in recent years to combat corruption, corruption remains a significant proceeds-generating crime.[7] The assessment team considered how authorities identify, investigate and prosecute the laundering of the proceeds of corruption—particularly relating to PEPs—and the authorities' activities to identify and recover these assets wherever located.

b) **Proceeds of organised crime, particularly drug trafficking:** Russia's criminal environment is characterised by the presence of organised criminal groups with international links. Some of these groups are large, and generate profit from an array of complex criminal activity, particularly drug trafficking, including that related to Afghanistan. According to the ML NRA, drug trafficking is the principal predicate offence for ML and is one of the crimes generating the most revenue.[8]

   The assessment team considered the actions taken by authorities to investigate ML committed by organised criminal groups and their ability to confiscate proceeds and instrumentalities (both domestically, and abroad, through outgoing MLA requests), and how these are used to disrupt the groups and their activities. Given the risk identified in the ML NRA, the assessment team also considered the use of virtual assets in the sale of narcotics, and the corresponding actions taken by law enforcement authorities.

   A large number of criminal proceeds generated in Russia are laundered abroad, as recognised by the ML NRA. Assessors focused on how the authorities are seeking assistance to pursue domestic ML cases with trans-national elements, and in particular to pursue the proceeds of drug trafficking and other crimes when these are laundered in other countries.

c) **Laundering of proceeds through the banking sector:** The NRA recognises that the financial sector is vulnerable to ML. Banks represent 92.6% of the total financial sector assets in Russia and there are some whose business models focus on carrying out high-risk financial services.[9] The assessors examined how the authorities prevent criminals from infiltrating or misusing banking institutions and how these institutions apply preventive measures, including CDD, record-keeping and suspicious transaction reporting. The role of the banking sector insiders involved in or enabling financial crime, including corruption, was also examined. Given that ML schemes often involve

5 According to official statistics, the main volume of illegal proceeds in Russia is generated by economic and corruption-related offences. The amount of assets generated by these crimes in 2017 was RUB 190 billion (approximately USD 3 billion). Fraud with public funds, misappropriation or embezzlement, and economic crimes against the state amounted to around 30% of the total sum, or USD 1 billion. See non-public ML NRA, pages 12-13.

6. https://databank.worldbank.org/data/reports.aspx?source=worldwide-governance-indicators&preview=on.

7 www.coe.int/en/web/greco/evaluations/russian-federation.

8 As part of crimes predicate to ML, the share of crimes related to drug trafficking in the period from 2014 to 2017 was about 40%. Non-public ML NRA, page 14.

9 *Ib.*

transfers to foreign jurisdictions, the assessors also focused on the risk management of banking institutions with international exposure, particularly towards countries where, or through which, Russian criminal proceeds are primarily laundered.

d) **Cash intensive/ informal economy:** The ML NRA recognises the use of cash as high in the Russian economy, even though it has declined in recent years. Russia states that illicit cash is used in the informal economy, and reintroduced in the formal financial system through deposits on accounts held by front persons and front companies, and subsequently withdrawn as cash. These accounts are opened in large FIs, but also in regional banks and branches. A main factor of vulnerability is the use of cash to conduct real estate transactions, even though this dropped from 87% in 2010 to 27% in 2017. The assessors considered the mechanisms deployed by Russian authorities to mitigate the risk of ML using cash, including cross-border transportation of currency, as well as on remittances and the use of cash in real estate transactions.

e) **TF:** Russia faces a high risk of TF, with main threats represented by armed groups in North Caucasus, cells of international terrorist organisations in Russia, FTFs from Russia or transiting through Russia, and terrorist organisations raising funds on the Internet. Terrorist attacks have occurred on Russian territory, mainly in North Caucasus, but also in major cities such as Moscow and Volgograd. Furthermore, a significant number of Russian FTFs have departed Russia to join ISIL in Syria and Iraq (approximately 4 000).[10] According to the TF NRA, terrorist groups mainly raise funds on the Internet (including social networks), not only from persons deliberately involved in the financing of terrorism, but also from individuals who are unaware of their true purpose. Other electronic payments, including virtual assets, may also be used for TF purposes. The assessment team focused on the effectiveness of measures to combat TF in all its forms, including the financing of FTFs, implementation of TFS, and the integration of CFT in the broader counter-terrorism strategy.

56. Through the scoping exercise, several areas were identified for lesser focus:

a) **Mutual insurance companies, mutual investment funds, investment fund management companies, and private pension funds:** these are identified by the ML NRA as posing a low risk. Furthermore, their share of financial sector assets is low, and assessors found no information that these areas deserve increased attention in the assessment.

b) **Casinos:** this is not a significant sector in Russia, and casinos are permitted in only four special gambling zones while online casinos are prohibited. The assessment team focused less on this sector while assessing the effectiveness of the DNFBP sectors as a whole.

57. In the course of the scoping exercise, assessors also noted that Russia's AML/CFT system also makes use of modern IT systems to a high degree within the

[10] https://themoscowtimes.com/news/russia-named-top-source-of-foreign-fighters-in-syria-and-iraq-59380.

federal AML/CFT system, in particular by the FIU. Assessors paid particular attention to how these systems are deployed and their effect on the implementation of AML/CFT measures.

Materiality

58. The Russian economy is the eleventh largest in the world in terms of GDP. According to the IMF, the volume of GDP in 2019 amounted to USD 1.61 trillion. Natural resource extraction makes up a major part of Russia's economy: Russia has large oil, natural gas, and precious metals industries that account for a significant share of GDP, a majority of exports and almost half of federal tax receipts.[11] Russia is an industrialised country with an extensive manufacturing sector. One notable contextual factor is the significant size of the informal or "grey" economy in Russia – it is estimated that in 2016, up to 21% of the labour force did not have a contract for their main job. The presence of a significant informal economy may make it easier for criminals to conceal serious criminal activity.

59. Russia is not a major financial centre, trade hub, or centre for company formation and administration, although it does function as a regional hub for the Eurasian Economic Union countries, giving it some exposure to cross-border ML and TF risks emanating from Central Asian and Caucasian countries, and Belarus. Its FIs and DNFBPs primarily serve domestic customers. One exception to this is Russia's DPMS sector: Russia is a significant centre for mining precious metals and stones.

Structural Elements

60. Russia has all of the key structural elements required for an effective AML/CFT system, including political and institutional stability, a significant high-level commitment to address AML/CFT issues across various parts of government, governmental accountability, rule of law, and a professional judiciary.

61. However, there are doubts from some sources that the judicial system is fully independent and fair. Concerns have been raised by the Council of Europe Commissioner for Human Rights in 2016[12] about the Russian judiciary, including that, notwithstanding recent positive reforms, the current procedures and criteria to appoint, dismiss and sanction judges still provide insufficient guarantees for objective and fair proceedings and expose judges to potential pressure, and that this is further compounded by a criminal justice system which favours the prosecutorial position. Similar concerns were highlighted in 2014 by other experts[13], and since 2010, several

11. World Bank, Russia Economic Report 41 http://pubdocs.worldbank.org/en/115001560108403019/rer-41-english.pdf

12. COE Commissioner for Human Rights, 25 Feb. 2016, www.coe.int/en/web/commissioner/-/as-long-as-the-judicial-system-of-the-russian-federation-does-not-become-more-independent-doubts-about-its-effectiveness-remain.

13 Gabriela Knaul, Report of the Special Rapporteur on the Independence of Judges and Lawyers – Mission to Russia, 30 April 2014, A/HRC/26/32/Add.1, considered by the U.N. General Assembly, Human Rights Council, http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/26/32/Add.1; *Russian Federation: Independence and Impartiality; Judicial Integrity and Accountability*, International Commission of Jurists, 16 June 2014, www.icj.org/cijlcountryprofiles/russian-

applicants from Russia have had their complaints upheld by the European Court of Human Rights concerning violations of the impartiality of tribunals and right to a fair trial. This issue is beyond the scope of a FATF evaluation, but such perceptions of the judicial system may potentially contribute additional challenges to effectively implementing some elements of the FATF standards, such as those involving international co-operation.

Background and Other Contextual Factors

62. Russia's economy and financial sector have undergone significant structural changes during the last 30 years, which continue to be relevant to the ML/TF risks. Following the fall of the Soviet Union, during the period 1989-95, a large number of banks were created in response to the new need for financial services and intermediaries. Many banks were linked to companies or particular industries and did not take deposits or make loans. During this initial post-soviet period, there were no effective market entry controls (for either prudential or AML/CFT purposes), and some banks came to be controlled by criminal interests. Since 2013, the BoR has significantly reinforced the requirements for owners and top management of banks. In recent years, there has been a significant reduction in the number of banks, such that there are 469 banks in Russia as of May 2019 (down from 923 in 2013, and from around 2 500 in 1996). This reduction reflects the revocation of licences by BoR for both prudential and AML/CFT reasons, mergers and acquisitions, as well as the closure of unprofitable banks.

63. The trend towards consolidation has progressed "organically" as a result of specific cases, and remains ongoing. However, it has had a significant effect on the ML/TF risk environment in the banking sector: removing the weakest institutions, and increasing the size and professionalism of those which remain. Nevertheless, many small non-credit FIs remain, which may have less capacity and resources to make investments in tools or processes for AML/CFT compliance.

64. On anti-corruption issues, Russia is a party to both the UN Convention against Corruption (UNCAC / Merida Convention) and the Convention on Combating the Bribery of Foreign Public Officials in International Business Transactions (Anti-Bribery Convention), and is also a member of GRECO.[14] Russia has dedicated significant resources to combating corruption, including through the 2011 restructuring of a specialised agency (the IC, see below).

65. However, assessors note that some parts of Russian law enforcement agencies have a corruption problem, including agencies charged with investigating ML.[15] Russian authorities are making noteworthy efforts to deal with this problem and

federation/russian-federation-judges/russian-federation-independence-and-impartiality-judicial-integrity-and-accountability-2/.

14 See Fourth Round Evaluation Report of Russia, GRECO, 22 March 2018, https://rm.coe.int/fourth-evaluation-round-corruption-prevention-in-respect-of-members-of/1680794c4f.

15 For example, the acting head of a Department within MoI's Economic Security and Combating Corruption Unit—a key AML office—was arrested in 2016 for hiding approximately RUB 9 billion (USD 125 million) in cash and bank accounts abroad. Another former official from FSB was recently arrested for taking bribes from banks and businesses and had RUB 12 billion (USD 185 million) in cash seized from him.

have convicted many law enforcement officers of corruption offences in recent years, in most cases for low-level bribery. Protections for whistle-blowers have also been seen as limited and corruption in Russia has been highlighted as a concern by international anti-corruption NGOs.

66. In terms of context for proliferation financing, Russia shares a border with the DPRK, and the two countries share a long-standing bilateral relationship focused on trade. In previous years, over 30 000 workers from the DPRK resided in Russia. As of March 2019, less than 4 000 DPRK workers continued to be employed in Russia and are expected to be repatriated in due course. Russia and Iran share a long-standing bilateral relationship and trade relations. Russia is not an international financial centre or a trade and transhipment hub, nor is it a significant centre for the formation of international companies. However, Russia does have a significant high-technology manufacturing sector, producing proliferation-sensitive goods and materials. Nevertheless, although outside the scope of this assessment, Russia applies an export and technical control regime for trade in relevant goods and to ensure compliance with UN sanctions, and applies measures for control of the underlying financial transactions related to possible proliferation-related activities.

AML/CFT strategy

67. Russia's high-level strategy for combating ML and TF is set out in the 2018 *Concept for Development of the National AML/CFT System.*[16] This is a presidential document, which sets out prevalent risks for the country, and defines the high-level objectives to prevent and mitigate those risks, such as increasing the efficiency of the national AML/CFT system, providing for the compliance of the obliged entities with AML/CFT legislation, increasing the level of transparency in the economy, preventing the misuse of public funds and enhancing the effectiveness of public expenditures, and suppressing terrorist/extremist threats and enhancing transparency of NPO activity.

68. To achieve these objectives, the *Concept* sets the high-level directions for the development of the national AML/CFT system in further developing the state policy and legislation in the area of AML/CFT, improving the mechanism for the obliged entities' engagement in the national AML/CFT system, reducing criminality related to ML/TF/PF, and enhancing the national AML/CFT system.

69. At the level beneath these, the *Concept* outlines specific tasks which should be undertaken towards achieving the high-level objectives (e.g. under the direction of reducing criminality related to ML/TF/PF, improving law enforcement practice for the identification of the BO of legal persons; establishing specialised investigators, judges and prosecutors focusing on financial crimes, etc.). This provides the basis for a series of agency-level action plans which reflect the results of the 2018 ML and TF NRAs and include more specific and time-limited objectives.

Legal & institutional framework

70. Russia is a civil law country. The Constitution (adopted on 12 December 1993) and all other federal legislation is applicable throughout the territory of the country. AML/CFT measures are primarily set out through federal laws: criminal justice measures are found mainly in the Criminal Code and the Criminal Procedure

16 Published on the official Kremlin website on May 30, 2018

Code, while preventive measures are set out mainly in the AML/CFT law. Some AML/CFT requirements are set out in laws governing the wider activity of which they are part (e.g. on company formation and registration). These are supplemented by a range of regulations (i.e. by-laws) issued by specific authorities.

71. The organisation of the executive is determined by the President, who is responsible for the structure of the Russian executive branch (which includes almost all bodies concerned in AML/CFT), and can, by decree, set up interagency working groups to develop policy plans. Executive power is shared by the President, who is the head of state, and the Prime Minister (officially the "Chairman of the Government"), who is the head of government. The executive includes 22 federal ministries, 28 federal services (of which Rosfinmonitoring is one), and 19 agencies.

72. The institutional framework for AML/CFT in Russia involves a wide range of Federal Ministries and Executive Bodies. The work of the different agencies is co-ordinated through an Inter-Agency Working Group (chaired by the Chief of Staff of the President) and an Inter-Agency Commission on AML/CFT/CPF (Chaired by the Director of Rosfinmonitoring). These are responsible for national policy co-ordination, and exist both nationally, and in each federal district, where they are responsible for interagency co-operation at regional level.

73. ***Rosfinmonitoring*** (the Federal Financial Monitoring Service), is the Russian Financial Intelligence Unit (FIU) and is the central authority co-ordinating the activities of all state bodies involved in AML/CFT issues. It was established in November 2001, initially within the competence of the Ministry of Finance, but since 2007, it has been a separate federal service. As an FIU, Rosfinmonitoring receives, processes and analyses information connected with ML/TF and forwards information to law enforcement bodies, if necessary. Rosfinmonitoring is also the registration and supervisory authority for sectors including leasing companies, and real estate agents.

74. The ***Ministry of Finance*** (MoF) is responsible for policy and regulation for budget, tax, insurance, foreign currency and banking activities, credit co-operation, micro financial activity, financial markets, public debt, auditing activity, business accounting and book-keeping, and processing and circulation of precious metals and precious stones, among others. The Ministry of Finance co-ordinates and controls the activities of the FTS, the Federal Service for Alcohol Market Regulation, the Federal Customs Service and the Federal Treasury.

75. The ***Ministry of Justice*** (MoJ) is responsible for policy and regulation in a several areas. With regard to AML/CFT, the MoJ is the authorised body for state registration and federal state supervision over the activities of NPOs. MoJ carries out entering of data in the register on branches and representations of the international organisations, foreign non-profit non-governmental organisations.

76. The ***Ministry of Foreign Affairs*** (MFA) is the responsible authority for international relations, in order to establish a unified foreign affairs policy. The MFA is also responsible for the signing and implementation of international agreements.

77. The ***Ministry of Internal Affairs*** (MoI) is responsible for law enforcement and immigration issues and services. It is not just the governing body for law enforcement, the MoI is also the police. It is the responsibility of the MoI to detect, prevent, disclose, suppress and investigate crimes and administrative offences. The

MoI is also concerned with public order and road traffic security issues, and the protection of state property.

78. The ***Federal Security Service*** (FSB) is the Russian domestic state security and counterintelligence service, responsible for counterintelligence, federal border protection, anti-terrorism operations and the fight against organised crime. AML/CFT issues are within the competence of the FSB.

79. The ***Investigative Committee*** (IC) is an investigative agency originally established under the General Prosecutor's Office in 2007. As of 2011, it is independent. The IC is a law enforcement authority charged with investigating the most serious and complex crimes in high-risk areas as TF, corruption, financial sector, and budget spending and taxes.

80. The ***Federal Customs Service*** (FCS) is an executive body that controls imports and exports to Russia, supervises the activities of customs and currency transactions and takes enforcement actions against smuggling, other crimes and administrative offences. The FCS has law enforcement duties and powers.

81. The ***General Prosecutor's Office*** (GPO) is an independent, centralised, uniformed prosecution authority. Its main task is to supervise the observance of all laws in Russia, including AML/CFT related laws. As with many civil law countries, the GPO co-ordinates all law enforcement activities related to combating crime. One of its main tasks is the prosecution of suspected criminals before the courts. It is the central authority co-ordinating the provision of MLA in criminal matters. The Prosecutor General heads the GPO and is the highest officer in the prosecution system. The Prosecutor General is constitutionally independent from the three branches of government.

82. The ***Bank of Russia*** (BoR) is responsible for regulating and supervising the activities of credit institutions (CI) and non-credit financial institutions (NFI), as set out in more detail below, but also plays a central role in national policy and coordination.

83. Judicial authority is exercised by the ***courts***. The Supreme Court is the highest judicial body on civil, criminal, administrative and all other cases that are within the competence of general courts. The Supreme Court also supervises general courts and issues judicial interpretations. As in other civil law countries, stare decisis (courts applying the same reasoning as in similar previous cases) does not apply in Russia, although judges may follow earlier decisions by higher courts, and the supreme court prepares guidance for lower courts based on analysis of lower-court decisions, with a view to ensuring consistency in reasoning. Russia also has district courts for criminal trials and regional courts having the power of appellate review. Military district courts are the venue for terrorism and TF trials, using the same procedures as district courts, but different court premises and with trials taking place before either a single judge or a panel of three judges of the district military court.

Financial sector and DNFBPs

84. This section gives general information about the size and makeup of the financial institution and DNFBP sectors in Russia. These are not all of equal importance given their role and size within Russia, and their different levels of exposure to ML and TF risks. The level of risk also varies greatly between different individual FIs and DNFPBs within the same sector. Assessors ranked the sectors based on the relative

1

importance, materiality and the level of risk. These rankings have been used to weight positive and negative implementation issues throughout the report, as a basis for assessors' conclusions – particularly under IO.3 and IO.4.

a) **Credit institutions (mostly banks)** is weighted as by far the most important in the Russian system, reflecting both the size of the sector, and its degree of exposure to ML and TF risks. The banking sector plays a key role in Russia as the primary means of accessing financial and related services. As of 31 December 2018 there were 484 credit institutions licenced in Russia, with 11 being considered systemically important banks. The number of credit institutions has steadily reduced in the last two decades, with 2 925 banks licenced in 1995 and 923 banks in 2013, which reflects a process of consolidation of the market as well as, in recent years, a more thorough application of entry requirements and AML/CFT supervision. Banks offer a variety of services, including retail, correspondent banking, and private banking. The NRA indicates a high level of threat from criminal elements (fraudsters, corrupt officials, organised crime) with vulnerabilities accentuated by the presence of a limited number of FIs prone to carrying out high-risk financial services or being involved in illegal activity.

b) ***Micro-finance institutions and credit co-operatives*** are heavily weighted for ML/TF risks. The vulnerability of the MFIC and CCC sectors is partly due to the relative simplicity of registration process (as compared to banking sector) and also the specifics of the sectors (the possibility to attract funds of legal persons and redistribute them among individuals). In 2017, there were 2 271 micro-finance organisations and 2 666 credit consumer co-operatives (in 2013, there were 3 860 microfinance organisations and 3 602 co-operatives).

c) The ***DPMS sector*** is also heavily weighted for ML/TF, with threats associated with tax evasion, illegal extraction of precious metal, illegal refining and smuggling of precious stones. One of the main vulnerability factor in the sector is the insufficient level of implementation of the AML/CFT legislation by participants in certain segments of the sector, as well as the need to improve the sanctioning measures and state control. In 2017, there were 430 natural or legal persons licenced to deal in precious metals and stones.

d) Five sectors are weighted moderately:

   i. The ***securities sector*** is a significant segment of the financial market in terms of the volume of transactions. In 2017, there were 614 licence-holding participants in the securities market, which represents a significantly lower number than the 1 149 holding licences in 2013. One of the vulnerability factors of the securities market is the possibility of carrying out settlements using bills of exchange (in particular, commodity bills) which makes it difficult to establish a connection between the buyer and the seller.

   ii. The ***insurance sector***: In 2017, there were 309 insurance companies or brokers licenced, which is about half of those licenced in 2013 (594). This reduction is in part explained by revocation of licences following the activities of BoR.

iii. The ***real estate sector***: There were 10 634 real estate individual agents and companies in 2017. A main factor of vulnerability is the use of cash to conduct real estate transactions, even though this dropped from 87% in 2010 to 27% in 2017. A notary is usually involved in a real estate transaction, while banks and real estate agents intervene sometimes.

iv. ***MVTS services***: Apart from providing traditional postal services, Russia Post is also allowed to provide some financial services. This includes the right to deliver pensions, allowances and other targeted payments, sale of securities, accepting and delivering payments, receive utilities, goods and services payments and provide debit card, MVTS and ATM services. Russia Post has approximately 42 000 offices all over Russia. Russia Post is supervised by Roscomnadzor.

v. ***Payment acceptance services***: Certain commercial non-banking legal entities have the right to accept cash from the public and to transfer these funds to other entities. This service is allowed for the payment of telecommunication services, rent and utilities, but can only be used for these purposes, not for other payments or transfers, greatly decreasing its vulnerability to ML and TF.

e) Other sectors are weighted as being of relatively low importance. These include:

i. ***Advocates, notaries, and legal professionals***: The activities carried out by advocates and notaries are regulated in their professional codes, and to some extent allow for activities that should be covered by AML/CFT legislation. Advocates are marginally involved in those activities, and Russia indicates that there were around 600 such advocates. Legal professionals are subject to the AML/CFT legislation but are not required to register, although about 1 000 have done so. They mainly offer consultancy services for the creation of legal persons. In 2017, there were 7 933 notaries.

ii. ***Accountants and auditors*** (and TCSP activities): In 2017, 4 223 audit organisations and 618 individual auditors, who provided audit and accounting services, were members of self-regulatory organisations of auditors. As for TCSPs, the legal framework does not regulate these as a separate profession or class of activities. According to the authorities, some of the relevant services are provided by other regulated professions - primarily by legal professionals, and notaries, while some services are prohibited. .

iii. ***Casinos***: In 2017, there were seven casinos in Russia, with a combined annual turnover of RUB 13 billion. Online casinos are prohibited.

iv. ***Mutual insurance companies, mutual investment funds, investment fund management companies, and private pension funds***: There were 309 mutual insurance companies and 305 companies holding licences to manage investment funds, mutual funds and private pension funds in 2018.

1

Preventive measures

85. Russia's preventive measures are set out in the AML/CFT Law (Federal Law 115-FZ), which came into force in February 2002. In addition, there are specific regulations set out in numerous subsidiary legal instruments pertaining to specific sectors or activities.

Legal persons and arrangements

86. Commercial and non-profit organisations can be set up in Russia. The former includes general partnerships, limited (commandite) partnerships, limited liability companies, joint-stock companies, production co-operatives, unitary enterprises, business partnerships, state and municipal enterprises and other commercial organisations (including simple partnerships and investment partnerships which do not form a separate legal entity). Non-profit organisations include consumer co-operatives, and other non-profit organisations such as charities. Foreign legal entities operate in Russia through representative offices and branches under the Law on Foreign Investment, subject to prior accreditation by Russian authorities. Legal persons operating in special economic zones are regulated by the provisions of Federal Law 116-FZ. These special economic zone companies are subject to the same registration and information requirements of other companies, including on their obligations to provide information to competent authorities and be the subject of inspection.

87. Legal persons (commercial and non-profit organisations) are required to be registered in the Uniform State Register of Legal Entities (USRLE), which is maintained by the FTS. The State register must record basic information of all legal persons, to include name of the legal person, the original or a copy of the founding documents attested by a notary (which include basic regulating powers, legal form and status, address of the registered office, directors).

88. Limited liability companies make up over 80% of all the legal entities registered in Russia, and have therefore been the main focus of assessors. Joint stock companies are the next most popular type of legal entity, and were also examined carefully. The less intensively-used forms of legal person were not weighted so heavily. The table below summarises the forms of legal person which exist in Russia and their basic characteristics.

Legal entities registered in the USRLE, 2018

Commercial organisations	Number Registered	Key Characteristics
General partnerships	145	Commercial organisation. Partners share unlimited liability.
Limited (commandite) partnerships	296	As a general partnership, but with non decision-making investors as well as general partners
Limited liability companies	3 338 503	The most common form of legal person used in Russia. Can be established with a minimum capital of RUB 10 000.
Joint stock companies	73 098	Companies governed by their shareholders
Including:		
Non-public joint stock companies	26 283	…where shares held by a limited range of up to 50 persons
Public joint stock companies	1 176	…where shares are publicly tradeable
Production cooperatives	10 990	Voluntary associations of 5+ persons for joint production
Unitary enterprises	15 194	State and municipal enterprises, which do not take ownership of property used
Other commercial organisations	8 768	
Sub-total	3 446 994	
Non-commercial organisations		
Consumers cooperatives	84 086	Mutual organisations to meet the needs for goods and services
State and municipal enterprises	221 433	
Other non-profit organisations	323 903	
Sub-total	629 422	
Total	4 076 416	

89. Express trusts and other similar legal arrangements cannot be created under Russian law. However, nothing prevents a person in Russia from setting up or managing a legal arrangement created under foreign law.

90. As noted in Russia's NRA, the misuse of legal persons is a key ML methodology in Russia. Legal persons are misused either as front companies to conceal fictitious activity in trade-based ML schemes or to conceal the real owners through strawmen managers/shareholders. Concealment of the BO of a Russian legal person through a foreign complex structure was also identified.

Supervisory arrangements

91. Russia has AML/CFT supervisors for the various sectors and activities covered by the AML/CFT measures. The main supervisory authorities are:

a) The BoR is independent from other government bodies and only reports to the State Duma. The head of the BoR is appointed or dismissed by the President, with the approval of the State Duma. BoR is responsible for the stability of the national currency, for the development of the banking system and for an efficient payment system. BoR is also the regulator and supervisor for credit institutions and banking groups, as well as non-credit FIs (insurance organisations, pawnshops, non-state pension funds, professional participants of the securities market, microfinance organisations, management companies of investment funds, unit investment funds, non-governmental pension funds, and credit consumer cooperatives, including agricultural credit consumer cooperatives).

b) Rosfinmonitoring is the supervisory authority for sectors including leasing companies, real estate agents, factoring companies and payment acceptance providers.

c) Roscomnadzor supervises the Russian Post.

d) The Assay Chamber is the supervisory body that controls entities' compliance with rules concerning trade in precious metals and stones, jewels and scrap, and is subordinate to the MoF.

e) The FTS is tasked with the collection of federal taxes in Russia. It also exercises supervision over currency operations, the gambling sector, and lotteries. The FTS is also responsible for the registration of legal persons and lotteries. All of its duties are carried out under the authority of the MoF.

f) For Auditors, there are two self-regulatory organisations: the "Russian Union of Auditors" and the "Sodruzhestvo Association". These represent the interests of their members and supervise their activities, including compliance with AML/CFT legislation, and membership is mandatory for the profession. In addition, the Federal Treasury is responsible for supervision of the activity of the two self-regulatory organisations and of the auditors themselves, including AML/CFT compliance, and is independent from the audit profession.

International co-operation

92. Russia co-operates with a wide variety of jurisdictions, receiving over 6 000 requests for MLA each year, and sending approximately 4 800 requests each year, with the General Department of International Legal Co-operation (GDILC), within the General Prosecutor's Office co-ordinating MLA. In addition, Russia engages in direct co-operation by law enforcement, FIU, and supervisory authorities. The geographic coverage of both outgoing and incoming requests reflects Russia's risk profile as a "source" country for criminal proceeds, and key partners for outgoing requests include Cyprus, Latvia, Switzerland, British Virgin Islands, Germany, the UK, the US, Czech Republic and Belarus.

CHAPTER 2. NATIONAL AML/CFT POLICIES AND CO-ORDINATION

Key Findings and Recommended Actions

Key Findings

1. Russian authorities have a very developed understanding of the country's ML/TF risks. Identification and assessment of ML/TF risks is done as a systemic exercise, which benefits from the high-level political commitment and the participation of all major stakeholders from both the public and the private sectors. The ML NRA uses a large amount of quantitative and qualitative data from a multiplicity of public and non-public sources. The methodology of the ML NRA is generally sound, although some improvements can be made.
2. The ML risks identified seem comprehensive and reasonable. The authorities demonstrated advanced understanding of and clear views on the constituents of risk, are aware of the most relevant country-wide and sector-specific risks, including the applicable risk scenarios, methods and tools.
3. TF risks are well identified and understood. The TF NRA is high-level and does not provide granular information about specific threats. Nevertheless, it is usefully supplemented by the in-depth knowledge of the criminal intelligence and investigation staff of the LEAs involved in counter-terrorism. Rosfinmonitoring has a key role in identification of TF-related threats and generation of relevant intelligence output.
4. National AML/CFT policies appropriately address identified ML/TF risks. There is an on-going and consistent policy development process in Russia, which builds on the outcomes of formal risk assessments and other articulations of risks (such as the annual threat assessment reports produced by Rosfinmonitoring since 2013). Relevant national strategies and the Action Plans derived from the outcomes of 2018 ML and TF NRAs represent the national policies at the strategic and operational levels aimed at combating ML/TF in the country.
5. Russian legislation does not provide for the non-applicability of any FATF Recommendations requiring FIs or DNFBPs to take certain actions. Simplified measures have been defined with due regard to the findings and conclusions of risk assessments, through consultation with relevant public and private stakeholders in AML/CFT. Results of risk assessments are used to support application of enhanced measures in higher risk scenarios.

6. The NRAs have informed the objectives defined and activities taken by Russian authorities. Alignment of objectives, priorities and activities with national ML/TF policies is achieved through, inter alia, the adjustment of agency-level policies with risk assessment outcomes and their incorporation into the roles and priorities of competent authorities.
7. Domestic co-ordination and co-operation is a major strength of the Russian AML/CFT system. Rosfinmonitoring is responsible for leading and co-ordinating legislative and operational activities in the field of combating ML/TF and enjoys a very high level of support from the top of the legislature and the government. There are also a variety of interagency co-ordination mechanisms.
8. FIs, DNFBPs and other sectors affected by the application of AML/CFT requirements have been directly involved in the NRA and sectoral risk assessment (SRA) processes. Results of risk assessments are duly communicated to the FIs, DNFBPs and SROs through institutional and operational arrangements.

Recommended Actions

1. The ML risk understanding would benefit from a more systematic and in-depth strategic analysis of the financial flows potentially associated with organised criminality generally and its transnational aspects particularly. Such analysis should cover all relevant predicate offences to provide a holistic understanding of the respective ML risks. The product of such analysis should either be integrated into the relevant sections of the existing national strategic documents or developed in the form of a dedicated strategy for combating national and transnational organised crime.
2. When the ML NRA or other SRAs are updated, the NRA methodology could be improved by delineating more clearly different types of risk determinants and subjects so as to avoid the potential confusion stemming from the mixed use of product and activity-based definitions of the risk domains. Also, further improvements are needed in the SRA methodology to, *inter alia*, provide a more granular understanding of the different exposure of sectors and firms to the various kinds of ML/TF risks; and better discriminate between prudential and ML/TF risk factors.
3. The next update of the NPO TF risk assessment should incorporate certain parameters (such as information on the number and types of registered entities, data on the founders, members and participants (including BO), amount of assets under control, number and amount of significant financial transactions, sources of donations and directions of expenditures), as well as the findings of supervision for different types of higher TF risk NPO, into the assessment report to enhance its utility for public and private users.

93. The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this section are R.1, 2, 33 and 34.

Immediate Outcome 1 (Risk, Policy and Co-ordination)

Country's understanding of its ML/TF risks

94. Russian authorities have a very developed understanding of the country's ML/TF risks. This finding is based on the analysis of the risk assessments produced by the authorities, and interviews. Since 2013, Rosfinmonitoring leads and co-ordinates the risk identification and assessment of ML/TF. This is done as a system-wide exercise, which benefits from a high level of political commitment and has the participation of all major stakeholders from both the public and the private sectors. The understanding of ML/TF risks has developed and evolved over the years and has been systematised for the first time in the two NRAs – one on ML and one on TF – issued in June 2018. Russia created its own methodology to conduct these assessments following a well-organised process.

95. The ML NRA uses a large amount of quantitative data from many public and non-public sources. Operational information mainly comprises data on financial and cash flows from the BoR and the FCS, statistics on criminal actions, STRs and mandatory reports, supervisory findings, as well as data from the FTS. Qualitative information analysed includes independent reports from the IMF, World Bank and other international organisations, expert judgments from supervisors, LEAs and other key stakeholders, and responses to perception surveys from the private sector and self-regulatory bodies (SROs).

96. Following the completion of the ML and TF NRAs, separate sectoral risk assessments (SRAs) were conducted by supervisors. These built on the analysis and conclusions of the NRAs and provided further details of the understanding of risk in the respective areas of responsibility of those authorities. However, improvements are still needed to these SRAs (see IO.3), including to provide a more granular understanding of the differing exposure of sectors and firms to the various kinds of ML/TF risks; to better discriminate between prudential and ML/TF risk factors; and to update and iterate the SRA processes in order to verify the conclusions and refine the approach to risk-based supervision on the basis of the first assessments.

97. The ML risks identified seem largely comprehensive and reasonable. Risks are ranked into four groups. The High Risk group comprises the most frequently used ML methods and tools, such as the use of front/shell companies, the use of non-resident legal persons and arrangements, trade-based ML through fictitious economic activity abroad, intermediaries affiliated with public officials, the misuse of electronic payments and virtual assets, and cash operations. The Heightened, Moderate and Low Risk groups assess the susceptibility of different FIs and DNFBPs to the potential misuse for ML.

98. The methodology of the ML NRA seems generally sound, although some improvements could be made. In particular, the ML NRA methodology employs a mixed use of product and activity-based definitions of the risk domains, which might create confusion when considering the exposure of individual sectors to the threats materialised through specific ML methods and tools. The same is true for the SRAs.

Whereas the conclusions on certain risks are not inappropriate as a result of the methodology used, when the ML NRA or other SRAs are updated, the methodology could be improved by delineating more clearly different types of risk determinants and subjects.

99. The risk understanding has developed overtime. The 2018 NRAs built on the findings and conclusions of earlier risk assessments, notably the annual threat assessment reports produced by Rosfinmonitoring since 2013. Going forward, recurrent and regular verification and feedback should play an important role in improving the NRA process and analysis.[17] Updating the NRA would allow Russia to identify trends in order to complete the picture obtained at one point in time. The risk understanding is likely to evolve when updating the NRAs with further refinement of both the processes and the depth of understanding.

100. The ML NRA defines threats in terms of specific domestic and foreign predicate offences, and identifies embezzlement of public funds, tax crimes, crimes related to corruption/abuse of power, fraud in financial sector (e.g. illegal banking activities perpetuated by unscrupulous managers and owners of FIs), and drug trafficking as the prevalent types of criminal activity with the highest potential to generate illicit proceeds. Vulnerabilities are considered within the context of the applicable legislative framework, contextual factors (e.g. shadow economy and circulation of cash), financial and non-financial sectors, etc. In addition, cybercrime[18] and organised crime[19] generally considered in the ML NRA are identified as threats in numerous other state policies relevant for the understanding of risk. Organised crime is considered in a broader context with overarching implications in terms of various types of criminal activity (including corruption, drug trafficking, fraud, etc.) where criminals endeavour to unite efforts and resources to maximize the effect of their wrongdoing.

101. The authorities demonstrated advanced understanding of on the constituents of risk, and are aware of the most relevant country-wide and sector-specific risks, including the applicable risk scenarios and ML/TF methods and tools. Nevertheless, it is not clear that authorities have exhausted the potential for the NRA to produce valuable conclusions on organised and large-scale criminal activities, particularly regarding cross-border activity and the internal structure of criminal groups. Despite the good knowledge of the operational situation in relation to

17 This includes, for example, feedback from operational and supervisory authorities on priority areas where the NRA could provide more specific information on risks as a basis for planning their activity; feedback on effect of the published NRA on the quality and type of STR reports; feedback from regulated entities on risk areas where deeper analysis is required; and verification of whether the conclusions of the risk assessment are reflected in identified ML/TF activity.

18 Particularly, the ML NRA considers the threats posed by the use of credit cards/ electronic means of payment to withdraw the proceeds of cybercrime (i.e. cyber-fraud and cyber-theft). Cyber offences are criminalised under Ch. 28 of the CrC and include prohibitions on unauthorized access to computer data as well as the creation and dissemination of malware.

19 Particularly, the ML NRA considers the threats posed by organised criminal groups involved in drug trafficking, embezzlement of public funds and fraud in financial sector. Creation of and participation in an organised criminal group is criminalised under Article 210 of the CrC.

organised crime, the ML risk understanding would benefit from a more systematic and in-depth strategic analysis of the financial flows potentially associated with organised criminality generally and its transnational aspects particularly. This is important given the significant threat posed by organised crime and could enable authorities to better disrupt international activities of organised criminal groups as well as to prosecute those present in Russia.

102. TF risks are well identified and understood. The TF NRA considers the specific threats posed by illegal armed groups operating in the North Caucasus, cells of international terrorist organisations operating in the country, Russian and foreign terrorist fighters, and perpetrators recruiting Russian nationals in terrorism through the use of social media or the Internet. Risks are considered in view of the vulnerabilities in three stages of terrorism financing, i.e. raising, moving and using funds. The assessment takes into account the mitigation measures that are in place, as well as the actions to be taken in the legislative, institutional and operational frameworks for further suppression of the risks of terrorism and TF. The TF NRA considers that the methods and techniques used to raise, move, and use funds are common to all terrorist groups and actors, and that they have similar capabilities in their use. The NRA therefore does not include specific financial profiles for different groups or analyse their internal financial operations.

103. The published TF NRA is high-level and does not provide granular information about specific threats, however, TF risk understanding is usefully supplemented by the in-depth knowledge of the LEAs involved in counter-terrorism. This includes the financial activities of the specific organisations and cells active in the various parts of the country and abroad, as well as by the express ability of the Rosfinmonitoring to initiate and, where necessary, support tracing TF-related funds and assist the parallel financial investigation of TF cases. There would nevertheless be value in using the next update to the TF NRA (or a related exercise) to gather and consolidate the existing organisation-specific knowledge of TF, to enable it to be analysed and tested, and make it available as a resource to a larger number of competent authorities. Good performance in identification and assessment of terrorism and terrorism financing risks is also confirmed by the cases presented in IO.9, with convictions achieved for individuals and activities related to both domestic terrorism and international terrorism.

104. In 2018, the authorities conducted a separate TF risk assessment in the NPO sector. The public version of the assessment report provides a detailed description of the applicable legislative and regulatory framework and sets out the vulnerabilities in terms of the possible misuse of NPOs for TF purposes (e.g. the opportunity to receive cash through e-wallets bypassing bank accounts; the difficulties in establishing clear links between individuals, e-wallets and a specific NPO). It concludes that the risk of NPO misuse is low in terms of the whole sector. It also suggests a range of mitigation measures to tackle identified risks.[20] Despite a low TF risk identified in the NPO sector, FIs and DNFBPs are instructed to consider

[20] E.g. development of legislation to prohibit persons who have had their assets frozen by a decision of the Interagency Commission on CFT from acting as founders or members of NPOs; to regulate collection of funds for charity organisations through donation boxes; to apply the risk-based approach in supervision; and to carry out awareness-raising activities for the NPO sector.

NPOs as high-risk clients and to monitor transactions related to charitable purposes (see IO.4). While such precautionary measure reflects the competent authorities' intention to ensure early detection of possible adverse dynamics in the current risk exposure of NPOs, there may be merit in additional outreach and communication with the private sector to assist FIs and DNFBPs to gain a clearer understanding of risk, assess their own exposures, and align their controls accordingly.

105. Whereas the analysis in the NPO TF risk assessment is at a general level and does not provide specific details of threat assessment, detailed questionnaires and other tools were used for collecting and analysing information on NPOs, including information on the number and types of registered entities, data on the founders, members and participants (including the BO), amount of assets under control, number and amount of significant financial transactions, sources of donations and directions of expenditures. Nevertheless, the next update of the NPO TF risk assessment should incorporate the above-stated parameters, as well as the findings of supervision for different types of higher TF risk NPOs, into the assessment report to enhance its utility for public and private users.

National policies to address identified ML/TF risks

106. National AML/CFT policies appropriately address identified ML/TF risks. This finding comes from interviews with the key AML/CFT stakeholders, such as Rosfinmonitoring, the BoR, LEAs and policy makers, as well as consideration of the national Action Plans and other policy documents.

107. There is an on-going and consistent policy development process in Russia, which builds on the outcomes of formal risk assessments. The most recent nation-wide policy document, the 2018 *Concept for Development of the National AML/CFT System,* sets out high-level objectives to prevent and mitigate the identified risks, such as increasing the efficiency of the national AML/CFT system, providing for the compliance of the obliged entities with AML/CFT legislation, increasing the level of transparency in the economy, preventing the misuse and enhancing the effectiveness of public expenditures, and suppressing terrorist/extremist threats and enhancing transparency of NPO activity.

108. To achieve these objectives, the *Concept* sets the high-level directions for the development of the national AML/CFT system in further developing the state policy and legislation in the area of AML/CFT, improving the mechanism for the obliged entities' engagement in the national AML/CFT system, reducing criminality related to ML/TF/PF, and enhancing the national AML/CFT system. Under each direction, the *Concept* defines the main tasks to be undertaken towards achieving the high-level objectives[21]. Implementation of the *Concept* is expected to result in better compliance of the national AML/CFT system with international standards as well as achieve an optimal institutional structure with adequate resources and regulatory support.

21 For example, under the direction of reducing criminality related to ML/TF/PF, the Concept defined the main tasks of improving law enforcement practice for the identification of the BO of legal persons; establishing specialised investigators, judges and prosecutors focusing on financial crimes, etc.

109. Regarding organised crime, the approach employed by Russian authorities in identification and mitigation of risk is to fight and suppress the prevalent crimes identified by national risk assessments and policies, using a combination of measures comprised of criminal intelligence and investigation for the identification of criminal groups involved in any types of serious crime on one hand and, where possible, charging both the predicate offence and the organised crime offense on the other hand. The Strategy of the National Security defines "activities of criminal organisations and groups, including transnational ones, involved in the illicit trafficking in narcotic drugs and psychotropic substances, weapons, ammunition, explosives, illegal immigration and human trafficking" among the main threats to the state and public security. Similar provisions are contained in the National Anti-Drug Strategy, the Concept for Development of the National AML/CFT System and other strategic national policies.

110. In relation to cybercrime, the Strategy of the National Security speaks about the threat with "the emergence of new forms of illegal activities, in particular the use of information, communication and advanced technologies," and two Presidential Decrees[22] task the FSB to develop the national system for identification, prevention and neutralization of cyber threats. In addition, a specialized department within the MoI is tasked to combat cybercrimes, including unauthorized access to computer data, creation and dissemination of malware, and fraud with the use of computer technologies. BoR has established the Center for Monitoring and Responding to Computer Attacks in the Credit and Financial Sphere (FinCERT), which is tasked to counter, inter alia, cybercrime and computer fraud. Currently, all credit organisations and insurance companies are connected to FinCERT, and the authorities advise that co-operation with credit organisations, payment systems and LEAs prevented the theft of more than RUB 2.5 billion and lead to blocking more than 5 000 fraudulent sites since 2017.

111. The *Concept for Development of the National AML/*CFT *System* and other relevant national strategies and the Action Plans derived from the outcomes of 2018 ML and TF NRAs represent the national policies at the strategic and operational levels aimed at combating ML/TF in the country. This approach has been confirmed and further detailed during meetings of the assessment team with high-level members of the State Duma (Vice Chairman, Head of Standing Committee on Security and Corruption Control, and Head of the Committee on Budget and Taxes) and the Interagency Working Group on Combating Financial Crime (Deputy Chair, Assistant to the President of the Russia). These officials provided comprehensive information on the evolution of the relevant measures taken by the legislative and executive branches of power over the last five years. At the time of the on-site visit, both ML and TF Action Plans were in advanced stages of implementation.

Exemptions, enhanced and simplified measures

112. Russian legislation does not provide for exemptions from any FATF Recommendations requiring FIs or DNFBPs to take certain actions. Simplified measures can be taken in respect of only one element of CDD, i.e. identification of customers who are natural persons, in case of limited types of transactions and

22 The Decrees of the President of Russia No. 31c of January 15, 2013 and No. 620 of December 22, 2017.

activities under specific restrictive conditions effectively mitigating the risk of ML/TF (see R.1 and R.10).These conditions have been defined based on: the findings and conclusions of earlier risk assessments, and; through consultation with relevant public and private stakeholders in AML/CFT, representing objective characteristics of potentially low-risk relationships, which are consistent with the conclusions of the 2018 NRAs.

113. The results of risk assessments are used to generate two categories of means triggering enhanced measures in higher risk scenarios. The first category comprises the enforceable regulations specifying factors that affect the assessment of risk for customers, geographic areas and transactions, as well as the indicators of unusual or suspicious activity, which are used for determining the risk of the customer and the business relationship and, subsequently, for making decisions on filing reports with Rosfinmonitoring. To ensure adequate response to emerging threats and ML/TF methods, these factors and indicators are periodically reviewed and updated based on, inter alia, the findings of risk assessments. The second category comprises information letters, methodological recommendations and other guidance issued by Rosfinmonitoring, the BoR and other supervisors advising the obliged entities to consider and use the NRA outcomes for identification, assessment, management and mitigation of risks.

Objectives and activities of competent authorities

114. The risk assessments have informed the objectives and activities taken by Russian authorities. At operational levels, authorities have aligned their policies, roles and priorities with risk assessment outcomes through the development of Action Plans building on the findings of the most recent nation-wide policy document, the 2018 *Concept for Development of the National AML/CFT System*. Rosfinmonitoring has revised its annual work plan for 2018 based on NRA findings and the internal structure and organisation is aligned with the results of the NRA. The BoR has developed a roadmap for implementing measures in response to 2018 ML and TF NRA findings, as further elaborated in the SRA for the financial sector. Other supervisory authorities, as well as law enforcement agencies have adjusted their policies (e.g. by amending quarterly work plans) and activities (e.g. by issuing special directives) to implement findings of the NRA. Training is provided by all agencies to, *inter alia*, better understand the identified risks and target activities accordingly.

115. Among activities of the competent authorities informed by earlier risk assessments, there were legislative and regulatory measures implemented over the last five years (for example, to improve the instrumentality for revocation of licences of credit institutions, to improve the quality of information on legal persons, or to establish an interagency mechanism for mitigating the risks of embezzlement and laundering of public funds in state defence contracts). These activities have had measureable impact in the respective areas of concern (see analysis in relevant IOs below).

116. There are many examples of measures coming from the Action Plans that aim at mitigating higher risks. These include, for example, the introduction of prosecutorial control over the expenditures of public officials, or the creation of models of financial conduct of “corrupt official”, “drug dealer”, “terrorism

accomplice" to enhance identification of customers and transactions with a higher potential of ML/TF involvement. All law enforcement agencies, including MoI and FSB, have specialized units for combating organised crime. Due to the work of these units, criminal proceedings have been instituted against public officials suspected of involvement in organised crime activities. To further improve the response to the risks associated with organised crime, a legislative amendment is being passed to tighten criminal liability for the creation of a criminal community, as well as for leadership and participation in it. There are also examples of detecting and prosecuting the prevalent predicate offences identified in the 2018 ML NRA with links to organised crime.[23]

National co-ordination and co-operation

117. Co-ordination and co-operation is a major strength of the Russian AML/CFT system. Rosfinmonitoring is responsible for leading and co-ordinating legislative and operational activities in the field of combating ML/TF and enjoys a very high level of support from the top of the legislature and the government. The IAC Financial Crime and the IAC AML/CFT/CPF are the mechanisms used at federal and regional levels by the competent authorities and SRBs to co-operate and co-ordinate the development and implementation of policies and activities in AML/CFT and, where appropriate, in CPF area.

118. IAC Financial Crime chaired by the Chief of Staff of the President has been operational since 2012 is in charge of national-level development of strategies and promotion of interagency co-ordination and co-operation. At regional level, it has substructures in all federal districts in charge of regional co-operation, assessment and mitigation of local risks.

119. The IAC AML/CFT/CPF chaired by the Director of Rosfinmonitoring has been operational since 2006 and focuses on developing proposals for improvement of the national legislation, sharing information on risks, implementing pilot projects, considering new ML/TF trends and similar initiatives. The work of this interagency co-operation format is supported by the Advisory Council established in 2007 and composed of the representatives of the largest professional associations and unions in the private sector, as well as the Compliance Council established in 2016 and composed of the representatives of the largest FIs and DNFBPs (over 100 members). The structure of the Compliance Council is also replicated at the regional level.

120. The IAC AML/CFT/CPF has a special role with regard to domestic co-operation and co-ordination in matters related to the development and implementation of AML/CFT and, where relevant, CPF policies and activities. To that end, the Joint Order No. 207 provides instructions for the operational exchange of information between Rosfinmonitoring and key law enforcement agencies. Further elements of the co-ordination mechanism are provided by 25 interagency agreements on co-operation between Rosfinmonitoring and other government authorities. Other interagency co-ordination mechanisms with functions relevant for AML/CFT are provided through the National Anti-Terrorism Committee, the

[23] To further improve the response to the risks associated with organised crime, a legislative amendment is being passed to tighten criminal liability for the creation of a criminal community, as well as for leadership and participation in it.

State Anti-Drug Committee, the Presidential Council for Countering Corruption, and the Interagency CFT Committee. In all of these committees, Rosfinmonitoring is well represented.

Private sector's awareness of risks

121. FIs, DNFBPs and other sectors affected by the application of the AML/CFT requirements have been directly involved in the NRA and SRA processes. In preparation of the 2018 ML and TF NRAs, a large cross-section of the private sector was requested to fill out a questionnaire to identify the main threats and vulnerabilities of the national AML/CFT system. In the course of the NRA process, representatives of the private sector were consulted at regular meetings of the Compliance Council and the Advisory Council under the IAC AML/CFT/CPF to discuss their perception and assessment of the risks and trends in the market, as well as the measures necessary to address them. Such surveys, consultations and other fact-finding initiatives were also carried out at regional level, through the Compliance Councils in the federal districts.

122. Results of risk assessments are duly communicated to the FIs, DNFBPs and SROs by means of the personal accounts on the Rosfinmonitoring website, as well as bilateral and multilateral meetings, conferences and similar events. Communication of the results of NRAs is also facilitated by the institutional arrangements of the Compliance Council and the Advisory Council under the IAC AML/CFT/CPF. Based on the results of the NRAs, specialised training courses for the representatives of the private sector have been developed by the International Training and Methodology Centre for Financial Monitoring (ITMCFM).

123. All competent authorities and SROs have posted public versions of the national risk assessments and, where applicable, SRA reports on their official websites. Supervisors have recommended the private sector to consider and use the NRA and SRA outcomes for identification, assessment, management and mitigation of risks. Awareness-raising activities for the obliged entities on the findings of the risk assessments have been conducted through, inter alia, practical workshops to model the situations that require application of risk management measures. SROs advise of including the NRA and SRA reports in the list of recommended reading for certification and professional development programs of their members.

124. Representatives of obliged entities are fluent in discussing the findings of the NRAs and SRAs, as well as in elaborating on the relevant implications in terms of specific threats, vulnerabilities and risks pertinent to their activities.

Overall conclusions on IO.1

125. Russian authorities have a very developed understanding of the country's ML/TF risks. ML risks identified seem comprehensive and reasonable, and TF risks are well identified and understood. National AML/CFT policies produced through an ongoing and consistent policy development process appropriately address identified ML/TF risks. The risk assessments have informed the objectives defined and activities taken by Russian authorities, with domestic co-ordination and co-operation being a major strength of the AML/CFT system. Results of risk assessments are communicated to FIs, DNFBPs and SROs through institutional and operational arrangements. There is room for further development by means of

improving the ML NRA methodology, systematising the understanding of the risks associated with organised criminality, and enhancing utility of the TF NRA for public and private users.

126. Russia is rated as having a substantial level of effectiveness for IO.1.

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 6

1. Russian LEAs, including MoI, FSB, IC, routinely and effectively access and use financial intelligence and other relevant information to develop evidence to investigate ML, TF, predicate offenses, and to trace criminal proceeds. The GPO further ensures the use of financial information in case development as it systemically reviews each ML and predicate offence investigation to verify that LEAs pursue all possible financial elements of an investigation.
2. Rosfinmonitoring is core to the functioning of Russia's AML/CFT regime. Rosfinmonitoring has a wealth of available data, including a high volume of STRs (20 million per year, on average) and MCRs, and employs sophisticated technologies, and high degree of automation, to prioritise, generate, and contribute to cases pursued by LEAs. Rosfinmonitoring is a well-resourced and data-driven FIU with competent analysts that has a uniquely wide view into the Russian financial system.
3. The information in the Rosfinmonitoring database is used to inform ongoing investigations, as well as to initiate new investigations into predicate offences, ML and TF. Case studies and statistics demonstrate that strategic and tactical analysis is used to generate cases for spontaneous dissemination to LEAs, and to inform ongoing investigations.
4. Financial intelligence is also used to develop numerous risk-based indicators (e.g. FTF indicators), which are shared with reporting entities and to predictively identify shell companies and potentially fraudulent government contracts.
5. Rosfinmonitoring's financial analysis and dissemination supports the operational needs of relevant LEAs to a very large extent. LEAs also demonstrated that the financial intelligence either received from Rosfinmonitoring, spontaneously or upon their request, is of high quality and integral to their activities.
6. Rosfinmonitoring's close co-operation and co-ordination with its domestic counterparts greatly contributes to Russia's effectiveness.

Financial intelligence plays an important role in informing supervisory actions by BoR, and helps to enhance the understanding of reporting entities through the development of typologies and risk indicators.

7. Rosfinmonitoring receives cross-border declarations of currency and BNIs (incoming and outgoing) from the FCS, which are directly integrated into its database. These declarations are limited, however, to cash or BNI transported across the borders of the EAEU (there is no obligation to submit a declaration within the EAEU borders).

Immediate Outcome 7

1. ML is generally well identified through financial investigations, and when it is identified, the authorities open ML investigations in more than 91% of instances, with most cases resulting in charges. LEAs routinely conduct financial investigations when looking into predicate offences, but usually do not pursue ML outside of predicate investigations. Self-laundering is frequently investigated, but third-party ML is detected and investigated less. The investigative process is rather formal, which brings efficiency and productivity, but ML investigations may not be opened or completed when there is evidence of a more easily provable alternative charge.
2. Most ML investigations involve the acquisition or sale of criminal proceeds, so the majority of cases relate to less serious offences involving smaller amounts of money, and a minority relate to more sophisticated ML involving concealing or disguising proceeds. Some complex ML is pursued and multiagency task forces yield good results. More opportunities for LEAs to uncover and investigate sophisticated and/or high-value ML may exist, especially in the financial sector and involving proceeds sent abroad, particularly those related broadly to corruption.
3. Russia is investigating ML activity partly in line with its risk profile, as approximately 85% of ML offences detected related to the high-risk areas denoted in the NRA, such as drug crimes and crimes with public funds. In the area of bribery, the number of ML cases pursued is not entirely aligned with risk, even though there are many corruption predicate investigations and thousands of recent convictions. While Russia is investigating and prosecuting offences stemming from some notorious, multinational laundromats, including by investigating complicit professionals in the financial sector, the authorities are not targeting enough bankers who facilitate ML in addition to those who raid their own institutions.
4. There has been an incremental increase in the number of core ML prosecutions. Since 2014, there have been more than 530 prosecutions each year under Articles 174.1 (self-laundering) and 174 (third-party laundering). Russia convicts approximately 323 individuals per year for these crimes, which is merely adequate, but the percentage of persons successfully prosecuted for ML is better when considered next to the large amount of lower-level ML prosecuted under Article 175.

5. Prosecutions are mostly for self-laundering, with few prosecutions of stand-alone or foreign predicate ML. Third-party ML is not prosecuted sufficiently, although some professional money launderers are charged with a combination of participation in an organised criminal group and self-laundering when they play a distinct financial role in a larger conspiracy.
6. Sanctions applied against natural persons for ML are partly effective, proportionate, and dissuasive, as terms of imprisonment for ML and fines are on the low-end based on statistics capturing ML as the primary offence of conviction. Through case examples, it was not possible to parse the ML sentence from the predicate sentence, but there were some instances of lengthy concurrent sentences. Considering that more than 2 155 individuals are convicted for all ML crimes annually, imprisonment is not a frequent penalty, which further suggests the lower-scale nature of many ML cases. Per fundamental principles, Russia cannot prosecute legal persons, but the use of administrative sanctions against legal persons was not demonstrated.
7. Russia beneficially employs alternative measures to prosecute financial crimes that could be indicative of, or occur in connection with, ML activity. These offences do not necessarily involve proceeds of crime and it is not always apparent why ML investigations or charges are not simultaneously pursued. The most impactful alternative offence used is illegal banking, followed by the outflow offence and offences related to shell companies. These measures disrupt schemes that may represent third-party ML infrastructure. However, they require less investigation into the full scope of the criminal conduct and may not be as easily recognised by other countries when co-operation is sought.

Immediate Outcome 8

1. Russia pursues confiscation as a policy objective and traces the proceeds and instrumentalities of crime. Provisional measures are used well, including for equivalent value. Between 2014 and 2018, criminals were finally deprived of RUB 318 billion or EUR 4.9 billion through the application of all available legal mechanisms. The overall statistical picture on many of the facets of confiscation, broadly defined, is solid.
2. Authorities focus on compensating victims, so restitution figures are higher than criminal confiscation figures. This is appropriate in the Russian context where many offences in the high-risk areas of crimes with public funds, as well as financial sector crimes such as fraud, embezzlement, and misappropriation, have identifiable victims. Restitution is the priority and criminal confiscation is used when legal owners cannot be identified or for offences that create proceeds but do not cause pecuniary loss. Approximately RUB 52 billion, or EUR 816 million, is restituted on an annual basis.
3. Criminal confiscation amounts are relatively modest in comparison with other types of recovery, particularly with regard to ML offenders. On

average, approximately RUB 3.2 billion or EUR 50 million is confiscated annually.

4. A strong point of the confiscation regime in Russia is the pursuit of the unexplained wealth of public officials whose expenditures exceed income. In 2017, approximately EUR 133.7 million was confiscated, demonstrating that GPO is becoming more assertive in its use of this anti-corruption tool. Additionally, large sums are voluntarily restituted by persons accused of corruption and civil claims are frequently filed by prosecutors to recover damages inflicted upon the state.
5. While there has been a relative increase in cases involving the pursuit of criminal assets moved abroad, including some complex, multinational examples, cross-border confiscation is not yet a routine practice for LEAs.
6. Confiscation regarding falsely or non-declared movements of currency/BNI is pursued to a lesser extent, partly due to the lack of a declaration obligation within the EAEU. Considering Russia's vast land borders and other relevant risk and context, a relatively low percentage of smuggled cash that is identified is confiscated. However, detected smuggling offences and imposed fines appear to partly offset the limited confiscations.
7. Confiscation results broadly align with identified ML/TF risks and AML/CFT priorities. However, seizure and confiscation numbers for drug trafficking are low despite drug crimes being the most common ML predicate. Per the ML NRA, in recent years, large amounts of funds of suspicious origin were moved offshore out of Russian banks using shell companies, fictitious trade, and other schemes. Although there were examples of asset recovery related to crime in the financial sector, additional confiscation results in this area, particularly for assets located abroad, were expected.

Recommended Actions

Immediate Outcome 6

1. Rosfinmonitoring intelligence could be enriched through the introduction of an obligation to report cross-border currency/BNI declarations within the EAEU or enter into MOUs to share such declarations.
2. LEAs should continue to use financial intelligence and other relevant information to be better detect bribery and abuse of office, in line with the risks identified in the ML NRA.

Immediate Outcome 7

1. LEAs and prosecutors should prioritise the investigation and prosecution of complex ML. To this end, a special focus or initiative to identify professional money launderers and networks that facilitate the movement of domestic proceeds out of Russia should be established.

Although not usually a destination country, authorities should be vigilant against the laundering of the proceeds of foreign crimes, including from neighbouring jurisdictions, and ML should be pursued independently of predicate offences, as appropriate.

2. In investigating shadow financial schemes, LEAs should ensure that the sources of funds and potential links to predicate offences are fully analysed. When pursuing alternative offences, authorities should consider whether a third-party ML charge is more appropriate, especially in cases with an international nexus where using the ML offences may facilitate co-operation.
3. While the financial sector is now more tightly regulated, competent authorities should continue to pursue the remaining bad actors. This entails prosecuting financial professionals who enable laundering by customers through the sector, in addition to those who embezzle bank assets.
4. LEAs should explore whether the laundering of bribe proceeds could be detected, investigated, and charged more frequently regardless of the amounts involved or the level of the PEP.
5. Authorities should study whether ML sanctions against natural persons are sufficiently dissuasive, especially since ML penalties are almost always an add-on to a predicate sentence, both to ensure that offenders are punished effectively and that there is an incentive to expend resources pursuing ML. Prosecutors should ask courts to prohibit persons from holding certain positions as a sanction for ML, when warranted, which should improve levels of integrity in the financial sector, public sector, and government contracting.
6. In the absence of corporate criminal liability, persons behind companies engaged in illicit activity should continue to be held accountable and consideration should be given to establishing an administrative or civil penalty regime for legal persons, as the CAO offence is of limited utility.
7. Prosecutors are encouraged to continue their practice of checking whether ML activity is sufficiently investigated by LEAs and to use other criminal justice measures where it is truly not possible to secure an ML conviction.
8. Legislation recognising virtual assets as property should be passed to guarantee that VA transactions can be the subject of an ML charge.
9. Sustain and build on the fruitful co-operation between law enforcement and Rosfinmonitoring. To this end, continue training, including at the ITMCFM, both operational agents and investigators in advanced ML methods, emerging threats, and options for international co-operation, leveraging the expertise of the FIU. Ethics should also be a component of LEA and prosecutor training.
10. Authorities should seek ways to enhance legal protections for whistle-blowers coming forward with allegations of ML or proceeds-generating

crimes. Authorities should continue to develop the use of co-operators to dismantle complex ML schemes.

Immediate Outcome 8

1. Russia should make the criminal confiscation regime, currently split between the Criminal Code and the Procedural Code, more straightforward and consolidate into a single law the power to confiscate the proceeds of all predicate offences.
2. While there are some instances of the pursuit of assets moved abroad, LEAs should search for more opportunities to conduct cross-border asset recovery and consider using criminal confiscation as the basis to seek international assistance, which may yield better outcomes than relying on restitution or other mechanisms.
3. Continue to emphasise making victims of financial crime whole. Consider the creation of a fund for confiscated assets out of which victims can be compensated, including, where appropriate, the government itself or state-owned entities in situations related to the theft of public assets.
4. Pass legislation that recognises virtual assets as property to ensure that VA can be seized, managed, confiscated and liquidated.
5. Study and potentially expand the types of assets and the categories of persons subject to non-conviction based confiscation of unexplained wealth.
6. With reference to the recommended intensification of focus on third-party and professional ML, ensure that the possibility of restraint is explored before funds are transferred abroad. Further employ mechanisms to reject suspicious transactions and swiftly restrain funds destined for foreign banks with weak controls.
7. Take steps, such as conducting a supranational risk assessment studying the primary methods of moving illicit cash and geographic vulnerability points within the EAEU, to improve the detection of cash and bearer negotiable instruments that may be linked to ML, TF, or predicate offences. In addition to imposing fines, promote the confiscation of undeclared or non-declared amounts as a predictable consequence of currency smuggling at external EAEU borders, and address the technical deficiency in R.32 to treat inter-EAEU transportation of currency/BNI as "cross-border."

127. The relevant Immediate Outcomes considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R.1, R. 3, R.4 and R.29-32.

Immediate Outcome 6 (Financial Intelligence ML/TF)

Use of financial intelligence and other information

128. Russian LEAs, including the MoI, FSB, IC, routinely and effectively use financial intelligence and other relevant information to develop evidence to investigate ML, TF, predicate offenses, and to trace criminal proceeds. As noted in IO.7 and IO.9, LEAs rely upon financial intelligence while investigating predicate conduct or ML/TF. The GPO also systemically reviews each predicate offence investigation conducted by LEAs to verify that all possible financial elements of an investigation are pursued (e.g. checking if LEAs sent requests to Rosfinmonitoring).

129. The assessment team reached their conclusions based on the quantity of sources of financial information available to Rosfinmonitoring and LEAs, statistics on effectiveness, case studies (including numerous case studies presented by Rosfinmonitoring's central and regional offices), and other discussions with LEAs (e.g. MoI, FCS, FTS, FSB, MoJ), and the GPO.

130. LEAs rely on various sources of information to identify ML, TF and predicate offences. Box 3.1 identifies the most common sources.

Box 3.1. LEA Resources and Methods to Initiate and Advance Financial Investigations

- Criminal information (criminal records)
- LEA requests to Rosfinmonitoring. There were more than 40 000 requests in each year between 2015 and 2017.
- Foreign information.
- Financial information provided by international counterparts
- Financial information obtained from FIs and DNFBPs. In the pre-investigative phase, financial records can be obtained with court permission and judges consider these requests within 24 hours. During the investigation phase, a court order is needed only for records pertaining to natural persons. On average, 72 490 motions are filed with the courts by investigators seeking financial information every year.
- BoR information. When, in the course of its regular activities, BoR detects a possible link between the financial transactions and any illicit activities it sends relevant information to Rosfinmonitoring or directly to LEAs.
- Media leads. LEAs indicated that centrally and in the territories, there are units charged with monitoring the news and suggesting investigative actions to verify potential instances of ML and TF (examples were provided).
- Information on cross-border EAEU currency declarations and customs information, including on customs declarations of imported/exported goods or transit declarations, declarations of vehicles, etc.

- Other sources of information (such as databases of improvised explosive devices, databases on serious crimes, fingerprints database of the IC, etc.)

131. While LEAs conduct analysis of financial information, such as account statements and transaction records directly obtained from FIs, all LEAs rely heavily on Rosfinmonitoring to support their financial investigations with information and analysis, and in some cases to directly conduct financial investigations as part of multiagency task forces.

132. While IO.6 relates to the use of financial intelligence and not simply an assessment of a country's financial intelligence unit, it is clear that Rosfinmonitoring is core to the functioning of Russia's AML/CFT regime. Rosfinmonitoring has a wealth of available data, including a high volume of STRs and MCRs, and employs sophisticated technologies, and high degree of automation, to prioritise, generate, and contribute to cases pursued by LEAs. Indeed, Rosfinmonitoring has a broader range of resources directly and indirectly available to it than compared to LEAs. As a result, an assessment of Russia's use of financial intelligence is directly linked to the operational and strategic work of Rosfinmonitoring. In short, Rosfinmonitoring is a well-resourced and data-driven FIU with competent analysts that has a uniquely wide view into the Russian financial system.

133. In addition to over 20 million STRs and 10 million mandatory threshold reports filed by reporting entities each year (see breakdown below), Rosfinmonitoring has direct and indirect access to databases and information held by the FTS, BoR, Federal Treasury, FCS, MoJ; Supreme Court; MoI; and others. For many of these sources, the complete data set is mirrored within Rosfinmonitoring's live database, the Uniformed Information System (UIS). This means it is available for processing by automated analysis tools, and can be integrated with other data sources for the purposes of big-data processing techniques (see below). Some additional sources of information are consulted when required in the context of an investigation. The information in the Rosfinmonitoring database is used to inform ongoing investigations, as well as to initiate new investigations into predicate offences, ML and TF. The non-exhaustive list below outlines the information accessible in Rosfinmonitoring's database:

- Information on criminal records, criminal prosecutions, searches conducted within joint financial investigations, and records on these financial investigations and all related documents;
- Income declarations of PEPs, management of the BoR and State Corporations
- Information on MLA within joint financial investigations with LEAs on cases, related to ML/TF and predicate offences;
- Information from registries (Unified State Register of Legal Entities; Unified State Register of Individual Entrepreneurs; unified registry of real estate property; information from the Federal Treasury on transactions with public funds (public tenders); registration and ownership of vehicles; maritime transport, aircrafts; passports; NPO registry);

- Supervisory information on FIs and DNFBPs, including signature samples, copies of contracts;
- Information held by the tax authorities about location and number of bank accounts held by natural and legal persons in Russia;
- Information on foreign taxpayers and tax liabilities of legal entities and individual entrepreneurs;
- Personal insurance policy numbers;
- Information provided by third parties in the framework of certain agreements (e.g. data on unreliable developers, violators on the electro-energy market, air tickets booking, etc.);
- Reports of frozen accounts or suspended transactions related to designated persons and organisations;
- Open source registers and databases.

134. Rosfinmonitoring has a very advanced IT system, with a database containing 17 years of financial intelligence (including information on over 12 million legal persons and 50 million natural persons). LEAs take advantage of the information held by Rosfinmonitoring by actively requesting information during the course of their investigations. Over the last five years, there has been a significant and growing trend in requesting financial intelligence from Rosfinmonitoring as outlined in the below table. The majority of the requests relate to suspected offences in budgetary funds spending (including taxes), financial sector, corruption and drug trafficking, which are in line with the findings of Russia's NRA (see IO.1). TF requests mostly relate to an unspecified risk or a suspicion that funds linked to TF were moved using bank accounts and cards, which is in line with the conclusions of Russia's TF NRA.

Table 3.1. LEA requests to Rosfinmonitoring for financial intelligence

Year	ML	TF	Total
2014	30 546	5 103	35 649
2015	36 607	4 250	40 857
2016	34 771	5 847	40 618
2017	35 612	7 121	42 733
2018	34 447	7 916	42 363

135. Rosfinmonitoring disseminates reports in response to LEA requests, as well as spontaneously. These disseminations can be broken into three categories: (1) responses to LEA requests without banking secrecy (pursuant to art.9 of L115)[24]; (2) responses to LEA requests when banking secrecy provisions are overridden

24 Article 9 reports may be provided in response to LEA requests. They do not divulge information covered by banking, official, tax, or commercial secrecy, but they provide sufficient lead information to permit the LEA to conduct further investigation or seek financial information through other legal processes. For example, transactions may be summarized by date range and specific FIs would be named to enable follow-up.

(pursuant to art.8 of L115)[25]; and (3) spontaneous disseminations (with and without banking secrecy).[26]

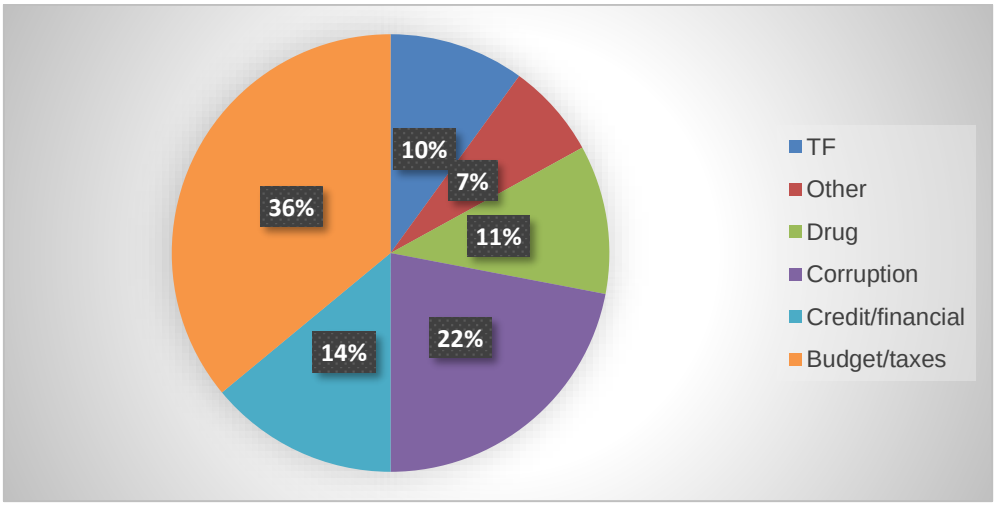
Table 3.2. Rosfinmonitoring disseminations to LEAs

Type of dissemination	2014	2015	2016	2017	2018
Art. 9 Without banking secrecy (upon request)	31 770	35 516	35 200	37 286	36 763
Art. 8 With banking secrecy (upon request)	943	1 144	1 332	1 078	1 232
TF	*126*	*179*	*194*	*102*	91
Spontaneous	3 538	4 253	4 559	4 123	4 282
Total	36 251	40 913	41 091	42 487	42 277

136. The above table demonstrates that Rosfinmonitoring actively responds to the requests of LEAs in ongoing cases, and spontaneously disseminates a large amount of information to LEAs (approximately 4 000 per year).

137. The figure below provides a breakdown on the types of disseminations provided by Rosfinmonitoring to LEAs based on risk during 2017. These disseminations align with the highest risk predicate offences for ML identified in Russia's ML NRA. As noted in IO.1, the highest risks for ML are offences in the financial sector; corruption/bribery; drug trafficking; and offences with state funds and tax offences.

Figure 3.1. 2017 Rosfinmonitoring Disseminations to LEAs



25 Article 8 "analysis reports" override bank and other secrecy and contain extensive human work product. There are primary reports and additional reports, which account for new targets or transactions. The legal trigger for Article 8 is sufficient reason to believe that a transaction relates to a predicate offence, ML or TF.

26 Spontaneous, or "initiative reports" may be disseminated to LEAs under Art. 8 or Art. 9. Rosfinmonitoring also proactively sends "risk alerts" to non-LEA federal executive authorities, which are reports without banking secrecy issued when Rosfinmonitoring detects facts relevant to the agency's competence (e.g., transactions indicative of fraud in government contracting).

138. Rosfinmonitoring further demonstrated that criminal cases were initiated based on its spontaneous reports sent to LEAs. As outlined in the below table, in the last five years, 1 307 criminal cases were opened by LEAs based on spontaneous disseminations, with the majority relating to predicate offences. The top five predicate offences in the five-year period below related to drug trafficking, embezzlement of public funds, tax evasion, abuse of office (corruption), crime in financial sector (including illicit banking). This is in line with Russia's assessment of its ML risks.

Table 3.3. LEAs investigations initiated by Rosfinmonitoring spontaneous disseminations

	2014	2015	2016	2017	2018	Total
Opened criminal investigations	160	249	199	253	446	1 307

139. Russia provided a significant number of case studies to demonstrate that the cases initiated are in line with the high-risk predicate offences in the NRA. Two examples are included below:

Box 3.2. High Risk Cases Initiated Based on Disseminations

Use of shell persons: In 2017, Rosfinmonitoring conducted analysis of STRs related to the execution of court orders amounting to RUB 64.5 million (EUR 880 880). It was identified, that the same company, M was receiving funds from a number of other companies using court orders, issued by the same court, in a short period of time. As a result of further analysis, Rosfinmonitoring detected that company M was owned by a "mass owner" (an individual owning a large number of companies), which indicated that he was likely a straw man, and almost all of the received funds were withdrawn in cash shortly after the execution of transactions. This information was disseminated to MoI in the Penza region, and LEAs later identified that debts settled in court were based on fictitious contracts between companies. As a result, the banks could not refuse to carry out transactions when suspicions arise, because the transfers were based on court decisions. As a result, in 2018, LEAs initiated a criminal case (falsification of evidence) against the BO of company M, who was identified by the bank.

The scheme was discussed within IWG and an interagency mechanism, involving courts, Rosfinmonitoring, LEAs and the GPO. Special recommendations were issued for courts to identify such schemes. The case is ongoing.

Use of cash in ML schemes: Rosfinmonitoring identified 216 transactions by four companies. The result of the analysis revealed that these transactions had no economic purpose (money was only transferred between shell companies). These four companies were registered in 2017 and received approximately RUB 71.1m

(EUR 971 069), and shortly transferred these funds into accounts in a bank, for subsequent cash withdrawal. Rosfinmonitoring disseminated a report to MoI in Saint Petersburg and Leningrad region. In 2018, the investigative authorities initiated a ML investigation.

140. In order to prevent the embezzlement of public funds (i.e. corruption) and subsequent ML, Rosfinmonitoring provides state authorities access to ready-to-use financial intelligence. In this regard, the Federal Antimonopoly Service uses this information while investigating antimonopoly cases and to identify a possible illegal agreement between competitors in order to initiate antimonopoly cases (see Box 3.11 in IO.7). However, as noted in IO.7, corruption cases pursued by LEAs largely align with the risk, but ML cases based upon bribery were not plentiful.

141. Financial intelligence is regularly accessed and used by LEAs to initiate and develop evidence to investigate predicate offences, ML and TF. In addition, financial intelligence is also used by supervisors to inform their supervisory activities. Special units exist within all nine of Rosfinmonitoring's offices dedicated to working with AML/CFT supervisors to prevent AML/CFT violations, and plan compliance enforcement measures.

142. Specifically, financial intelligence plays an important role in identifying necessary supervisory actions by the BoR, and helps to enhance the understanding of reporting entities through the development of typologies and risk indicators. Rosfinmonitoring uses STRs, MCRs, and other information available to risk-rate FIs. This risk-rating is then shared with the BoR to inform supervisory activities. If necessary, information is also disseminated to LEAs to initiate a criminal investigation into the institution.

143. Rosfinmonitoring also uses its available financial intelligence to develop and distribute to Russia's largest FIs FTF indicators, as well as on other indicators disseminated to the private sector to better identify high-risk crimes, such as the illegal export of timber in Siberia. This has led to increased suspicious reporting in these high-risk areas, resulting in an increase in investigations, prosecutions, convictions, as well as domestic designations in the case of the FTF pilot project.

Box 3.3. FTF Indicator Pilot Project

In 2015, Rosfinmonitoring initiated a pilot project to examine all FTFs departing the country to conflict zones, and developed financial profiles to enable such persons to be identified. Ten banks, (covering around 85% of the sector and equipped with sufficiently sophisticated transaction monitoring systems) were involved in the project. They worked with Rosfinmonitoring over 10 months to develop and refine the indicators. As of the on-site visit, the project remains at the pilot stage, with the indicators being used by the ten participating banks, but not universally.

There are 24 indicators, including when the customer: engages in no less than 15 transactions within 30 days – using a banking card, online

only; engages in transactions to book flights online to an ETA zone; and logs into remote banking operations (in the ETA) but does not conduct any transactions.

The project is not based on a simple financial profile, but has instead developed an algorithm that requires FIs first to identify indicators of potentially suspicious activity by their customers; then to conduct enhanced monitoring of those customers against a further set of confirmatory indicators. Customers who raise suspicions at both stages of monitoring by the FI are reported to Rosfinmonitoring under a specific code.

Information on 160 000 persons was received by Rosfinmonitoring as part of this project and 54 spontaneous requests were sent to LEAs, 39 out of which led investigations, resulting in domestic designations.

STRs received and requested by competent authorities

144. As noted above, Rosfinmonitoring receives a significant number of STRs and MCRs from FIs and DNFPBs, with the majority of reports originating from credit institutions (more than 90%). Mandatory control reports relate to required threshold reporting, including cash transactions exceeding approximately EUR 8 300, real estate transactions (where ownership is transferred) exceeding EUR 41 000, transactions over EUR 138 000 and relating to the defence industry/security of Russia. Transactions subject to mandatory reports and STRs are primarily detected via automated systems used by FIs and DNFBPs, and the reports themselves are also largely completed through such automated systems, normally with a brief manual review prior to filing. Banks met during the on-site indicated that a few sentences of narrative might be added to STRs. Given the exceptionally large volume of reports required under the Russian system and the fact that the STR form contains 274 data fields, this automation is essential in order to support the data analytics that underpins Rosfinmonitoring's analysis. Human analysis is still needed to direct, interpret, and add value to the raw information generated by Rosfinmonitoring's systems.

145. Rosfinmonitoring is also currently piloting a project for reporting entities to file suspicious activity reports (SARs), in parallel to the STR system in place. The purpose of the introduction of SARs is to allow institutions that identify suspicious activity of a client to file reports that will include consolidated data related to multiple suspicious transactions at once. For example, one project called the "Financial profile of a drug dealer", where FIs submit SARs in accordance with developed behavioural models of criminal activity, related to drug trafficking. In addition to financial information, SARs also include geolocation data, which significantly simplifies the use of this data by law enforcement operatives, as it is of particular relevance for this kind of investigations. The project has been in place since 2018, three major FIs are participating. Rosfinmonitoring received approximately 140 SARs as of March 2019.

146. Rosfinmonitoring also receives cross-border declarations of currency and BNIs (incoming and outgoing) from the FCS, which are directly integrated into its

database. These declarations are limited, however, to cash or BNI transported across the borders of the Eurasian Economic Union (there is no obligation to submit a declaration within the EAEU borders).

147. Table 3.4 below provides a breakdown of reports received by Rosfinmonitoring over the last five years. These reports are primarily filed electronically via the Rosfinmonitoring Personal Account, which is used by all FIs. The proprietary platform known as the Personal Account was introduced in 2016, which accounts for the sharp increase in STRs filed to Rosfinmonitoring as outlined in the table below. A detailed breakdown of STRs and MCRs by type of reporting entity is included in IO.4.

Table 3.4. Number reports received by Rosfinmonitoring

Type of report	2014	2015	2016	2017	2018
STRs	4 634 648	11 977 483	19 018 594	21 611 388	17 700 000
MCRs	8 000 136	10 176 104	11 004 867	12 160 104	11 550 000
Custom declarations	31 746	25 571	22 381	25 506	26 018

148. As indicated in the above table, Rosfinmonitoring received over 30 million STRs and MCRs each year since 2016. This exceptionally large volume of information requires and enables Rosfinmonitoring to use an unusual and highly automated approach to FIU analysis, which is different to the approach used by most FIUs. This has several essential features:

- STRs are automatically uploaded into Rosfinmonitoring's live database (certain types of STRs, requiring immediate attention, are analysed by relevant departments right after being uploaded into the database).
- For wholly new STR subjects or data points, dossiers are created, but if the subject matches information already held by Rosfinmonitoring, the STR is automatically linked to the existing dossier.
- Automated systems use big-data techniques to identify cases for review by analysts. These systems provide each analyst with a list of targets for further (manual) analysis, prioritised based on the degree of risk as determined by the system (of a specific activity).
- FIU analysts are assigned to specific subjects or offences (e.g. drug offences or illegal banking) consistent with the findings of the NRA. There is no specific department to identify a particular case from STRs and to assign it to the most appropriate department for analysis. These tasks are carried out automatically. Analysts can customise the automated systems to focus on specific types of activity. They can program alerts to be made aware of certain types of filings in real time (e.g. any STR related to TF).
- FIU analysts manually review those cases identified and prioritised by automated systems. A range of analytic and visualisation tools are used to support this human phase of analysis.
- The high degree of automation involved in Rosfinmonitoring's model of FIU analysis requires detailed STRs, which must be accurately coded and formatted by reporting entities. Upon entering the database, information in STRs goes through special automated format-logical control algorithms.

Information on the suspected predicate offence involved in STRs is organised through a numeric classification system, where each STR is assigned one or more codes by the reporting entities and relating to a predicate offence or description of activity. The below table indicates the five most prominent STR codes filed in the last five years. In some cases, the reporting entity links the STR with the codes of STRs previously submitted, or of a known typology or trend. Reports are further integrated into Rosfinmonitoring's database based on the information contained in the required data fields of the STR template. Many of these fields, along with other data in the database, are considered as indicators which are weighted by automated systems to calculate the aggregated risk level. Different indicators are used to build typologies, profiles and to generate new indicators.

149. The below table illustrates the most prominent STR codes assigned to STRs by reporting entities over the last five years. Some STRs may be assigned with multiple STR codes. As a result, the total number of assigned STR codes may exceed the total number of STRs received by Rosfinmonitoring.

Table 3.5. Prominent STR codes filed to Rosfinmonitoring

STR group code description	2014	2015	2015	2017	2018
14 (STRs related to cashing out schemes and the use of fictitious companies)	3 612 748	11 704 709	21 590 711	26 432 139	21 311 522
11 (STRs related to the use of fictitious companies)	1 683 824	3 682 838	8 343 442	7 959 941	7 858 205
18 (STRs related to transfers of funds overseas)	155 331	155 403	117 235	137 485	118 858
21 (STRs related to the use of electronic money transfers and bank cards)	148 135	189 205	187 210	294 859	237 754
22 (STRs related to the TF)	120 023	176 288	34 953	108 945	155 677

150. Once STRs are filed with Rosfinmonitoring, a series of automated checks occur against the extensive information contained in Rosfinmonitoring's live database. Connections are generated, a visual characteristic and risk rating is then assigned. The analyst then examines the prioritised cases under their area of responsibility for deeper analysis (e.g. drug trafficking, corruption, budget, ML, etc.). The analyst may then request additional information from reporting entities and other federal authorities where no direct access exists, such as video and photo information from video surveillance systems in ATMs, IP-addresses, and card authorisation addresses.

151. Rosfinmonitoring may also request information from FIs and DNFBPs, including when STRs are not filed. Reporting entities are required to respond to Rosfinmonitoring requests within five days (but may be extended by three working days if significant technical/analytical work in necessary to respond). Such requests can relate to particular accounts, individuals or legal entities, financial instruments,

or can be more strategic (i.e. describing a typology). The below table indicates the frequency of these requests, particularly to FIs. The number of requests increased substantially in 2017 as result of the introduction of the Personal Account, which facilitates secure, direct communication between Rosfinmonitoring and its reporting entities. The majority of the requests to FIs related to the obtainment of bank account statements, information on the BO of clients, clients' questionnaires, and copies of contracts.

Table 3.6. Rosfinmonitoring requests to FIs

Type of FI	2014	2015	2016	2017	2018
Investment companies	4	1	4	4	0
Credit Institutions	14 919	16 155	21 570	45 862	36 445
Financial leasing companies	-	4	-	-	2
Non-bank credit institutions	1 511	1 860	879	65	33
Non-credit institutions	87	21	4	1	0
Telecommunication operators	191	423	299	80	63

152. Given the large quantity of information received and requested, Rosfinmonitoring has dedicated significant resources to develop a sophisticated IT system to assess its effectiveness, perform preliminary analysis, identify trends and typologies, and organise/compare data. As noted above, based on integrated indicators and pattern recognition, the database automatically detects cases for prioritised review by analysts. Analysts may then work within their situational palettes, which allows the analyst to access aggregated information on transactions, and other information held in the database. Indeed, information contained in the database may be reviewed by analysts on their dashboard based on any indictor or content contained in the STR, such as the type of person (PEP, legal person, etc.), geography, STR trigger, value, filing institution, etc. Notably, this system has machine-learning capabilities to fine-tune its success rate it the automatic detection of ML, TF and predicate offences. The assessment team found that the automation employed in this database is leading to enhanced screening of all STRs, and better identification of promising cases for referral to LEAs. This is particularly the case in relation to the identification of shell companies. Even if the STR or other report itself is not actionable, the data inputted to the system creates norms and baselines that teach and evolve the software.

153. For example, Rosfinmonitoring has the technological capability to "predict" shell companies that are commonly used in ML schemes using specific and general traits typical of shell companies, including how many STRs were filed against a company by reporting entities (based on indicators circulated by Rosfinmonitoring). If a significant number of STRs were filed and suspect the same company as a shell, the file is referred to an analyst for manual analysis to verify the machine's assessment. According to LEAs, the success rate of Rosfinmonitoring's identification of shell companies is 100%. A case on the identification of a shell company is below.

Box 3.4. Identification of a Shell Company

Rosfinmonitoring identified financial transactions of E, which received around RUB 22 million (EUR 301 521) in 2017 from a number of legal entities, mainly, N and agricultural consumer co-operative P as payments for works on improving the quality of turf.

Most of the received funds were later transferred into accounts of B (Kazakhstan) – RUB 16.4 million (EUR 224 770) and P - RUB 4.3 million (EUR 59 000).

Rosfinmonitoring's information system classified P as a shell company, as it was suspected of not conducting legitimate economic activity. This case was then prioritised and a deeper analysis was conducted by a Rosfinmonitoring analyst. The BoR provided information that E did not submit customs declarations to prove actual movement of goods and that there were reasons to suspect that documents, submitted to a bank, may have been false.

Rosfinmonitoring concluded that E may be involved in a shadow scheme, facilitating transit financial flows. Moreover, there were indications that a criminal offence related to the carrying out currency transactions of foreign or domestic currency to non-residents' accounts with fake documents (on a large scale) (i.e. Art 193.1 CrC). Based on these conclusions, information was disseminated to MoI in the Republic of Tatarstan and was used to initiate a criminal case.

Operational needs supported by FIU analysis and dissemination

154. To a large extent, Rosfinmonitoring's financial analysis and dissemination supports the operational needs of relevant LEAs, which include the investigation and prosecution of ML, TF and predicate offences as well as the confiscation of criminal proceeds.

155. Rosfinmonitoring is a federal, autonomous agency responsible for countering ML, TF, and PF, and participates in activities to counter corruption. It is structured based on the eight federal districts of Russia, and has one central office in Moscow. Rosfinmonitoring employs over 800 individuals, with approximately 400 staff dedicated to the central office in Moscow. Analytical departments represent more than 50% of Rosfinmonitoring's staff in the central office and around 70% of staff of the territorial bodies. All federal districts are directly connected to Rosfinmonitoring's main database. The central staff of Rosfinmonitoring has direct access to all data contained in the UIS.

156. All Rosfinmonitoring offices are structured similarly and include dedicated analysis departments on: ML (which also covers corruption and drug trafficking); TF and PF; public funds and misappropriation; credit and finance fraud. The themes of these departments are based on the priority proceeds generating crimes identified in the NRA. There are also co-ordination units within each territorial body with the purpose to identify possible duplication of work, with the central office

having the responsibility to de-conflict and assign lead responsibilities. The central office also has dedicated departments on new IT developments, liaison with supervisory agencies and international co-operation.

157. Rosfinmonitoring conducts both tactical and strategic analysis. Both tactical and strategic analysis are conducted in the central and territorial offices of Rosfinmonitoring, in the Departments dedicated to Macroanalysis and Typologies, Analysis of Public Sector, and AML/CFT. Tactical analysis is the analysis of reports related to financial investigations into ML/TF and predicate offences conducted spontaneously or at the request of LEAs, and ultimately sent to LEAs for their use. All of territorial bodies of Rosfinmonitoring complete tactical analysis. Nearly 76% of incoming reporting (STRs, mandatory threshold reports, blocked transaction based on designations, etc.) are incorporated into tactical intelligence, which may only be used as intelligence (to generate leads) and not as evidence in court. LEAs use this data as a source to gather evidence and trace assets during the intelligence phase and during criminal investigations.

158. Strategic analysis, on the other hand, is completed to identify vulnerabilities, risks and threats to Russia's financial system. All STRs and MCRs are used to inform strategic analysis reports, including the identification of new risk areas, typologies and red flags. Strategic analysis is conducted by the central office of Rosfinmonitoring, and specialised units in the territorial offices. A positive, unusual feature of the Russian system is that strategic analysis conducted by Rosfinmonitoring has led, on occasion, to tactical analysis that has been disseminated to law enforcement and initiated investigations.

Box 3.5. Strategic Analysis Leading to Tactical Dissemination

In 2013, Rosfinmonitoring conducting strategic analysis of financial transaction reports and identified more than 2 300 reports in an amount of around RUB 42 billion. These transactions related to insurance companies and reinsurance contracts. As a result of Rosfinmonitoring analysis, it was suspected that it was an organised channel to transfer funds overseas. The scheme included loan payments into accounts of companies, controlled by the mastermind if the scheme – individual T –, and followed by transfers to insurance companies and subsequent transfer abroad within reinsurance contracts.

In parallel, LEAs were investigating a criminal case related to tax evasion by a company «E» and in co-operation with Rosfinmonitoring it identified that «E» was using cashing out services, provided by individual T. Individual T conducted illegal business activity, incl. cashing out for a fee, and received a criminal income in a total amount of more than RUB 450 million..

As a result, individual T was charged with illicit business activity (part 2 of CrC Article 171) and complicity to tax evasion (part 5 of CrC Article 33 and part 2 of CrC Article 199).

159. Rosfinmonitoring promptly responds to the needs and requests of LEAs, and its disseminations align with the ML and TF risks identified in the NRA (see Figure 3.1). Throughout the onsite visit, LEAs demonstrated that the financial intelligence either received from Rosfinmonitoring, spontaneously or upon their request, is of high quality and integral to their activities. Case studies presented also demonstrated the added-value of Rosfinmonitoring's information and analysis to generate and inform financial investigations into ML (including complex ML schemes), TF and predicate offences, leading to prosecutions, convictions, and the tracing, seizure and confiscation of criminal proceeds. LEAs rely on Rosfinmonitoring for intelligence and place trust in its in-depth analysis. LEAs use their comprehensive investigative techniques to corroborate this intelligence and to transform it into evidence that can be used in court. LEAs review Rosfinmonitoring's products highly, but it was also apparent that they value the role played by the FIU in coordinating and, often initiating, joint task forces for complex financial investigations.

160. When Rosfinmonitoring identifies indicators of possible criminal activity within the analysis of STRs or other reports, while conducting supervision measures, or from information received from other state authorities, the private sector, or foreign FIUs, Rosfinmonitoring proactively disseminates this information to the LEAs for operational use. Between 2013 and 2017, Rosfinmonitoring's initiative reports were used within 194 criminal cases that were submitted to court. In the same timeframe, Rosfinmonitoring's analysis reports, both initiative and responsive, were used to initiate 1 406 ML investigations under the core offences (CrC Arts. 174 and 174.1). The below table compares the total number of ML cases initiated, referred to court, and successfully concluded, with those that involved the use of Rosfinmonitoring information. The statistics demonstrate that initiated ML cases based on Rosfinmonitoring information increased from 2014 to 2018, but peaked in 2016 (59% in 2014; 61% in 2015; 84 % in 2016; and 64% in 2017).

Table 3.7. Use of Rosfinmonitoring's analysis, related to ML (core offences only)

ML Cases	2014	2015	2016	2017	2018	Total
ML investigations based on RFM info	274	312	405	272	348	1 611
Core ML investigations	618	734	679	609	712	3 352
ML prosecutions based on RFM info	85	105	141	119	191	641
Core ML prosecutions	531	627	621	533	613	2 925
ML convictions based on RFM info	53	66	96	78	100	333
Core ML convictions	248	311	412	379	426	1 776

161. Similarly, the below table compares the total number of terrorism and TF cases, and those involving Rosfinmonitoring information. Over the last five years, Rosfinmonitoring's information led to the initiation of TF cases in approximately 19% of the cases.

Table 3.8. Use of Rosfinmonitoring's analysis, related to terrorism and TF

TF Cases	2014	2015	2016	2017	2018	Total
Terrorism cases investigated based on RFM info	55	61	145	137	179	577
TF cases opened based on RFM info	4	10	34	63	73	184
All Initiated TF cases	124	127	109	236	364	960
Terrorism and TF taken to court based on RFM info	29	13	19	17	37	115
Terrorism and TF cases resulting in convictions based on RFM info	12	15	29	26	43	125
All Terrorism and TF cases resulting in convictions	342	360	556	647	574	2 479

162. Moreover, Rosfinmonitoring's disseminations are also used to initiate criminal cases into suspected predicate offences. Based on a number of the case studies reviewed, the initiated predicate offence cases are in line with the risks of the NRA. For example, in 2017, 60 criminal cases related to illegal banking were initiated with the use of information from Rosfinmonitoring.

Table 3.9. Use of Rosfinmonitoring's analysis, related to predicate offences

Predicate Cases	2014	2015	2016	2017	2018	Total
Predicate cases initiated based on RFM info	829	999	1328	1412	1 528	6 096

163. The following case studies demonstrate the initiation of criminal cases on predicate offences, based on Rosfinmonitoring's information:

Box 3.6. Initiated Predicate Offence Cases Based on RFM Information

Embezzlement: Financial investigation into the activity of the director of S, suspected of embezzlement of funds, allocated for the construction of a perinatal centre in Sochi in the amount of more than RUB 200 million (EUR 2 745 700). Rosfinmonitoring analysed 1 162 STRs, the results were disseminated to the state security authorities in Krasnodar region. Rosfinmonitoring's information was used to initiate a number of criminal cases related to embezzlement.

Offences in the financial sector: Financial investigation into the activity of the management of a credit institution (D, Rostov) and third parties, who organised a criminal scheme to illegally grant loans to affiliated companies in an overall amount of more than RUB 725 million (EUR 9 953 163). Rosfinmonitoring analysed 60 STRs

and disseminated the results to the MoI. Rosfinmonitoring's information was used to initiate a number of criminal cases related to fraud and organised crime, resulting in convictions in 2017.

Drug Trafficking: Financial investigation into the activity of a group of individuals, suspected of illicit drug dealing through Internet. Rosfinmonitoring analysed 886 STRs as well as additional information received from reporting entities on request. MoI in the Republic of Ingushetia used Rosfinmonitoring's information to initiate a number of criminal cases related to drug trafficking.

164. As noted in IO.8, Rosfinmonitoring's information is also used to identify assets that can be seized, in order to provide for future confiscation or restitution. This was also further evidenced through case studies.

Co-operation and exchange of information/financial intelligence

165. As noted in IO.1, domestic co-operation is the pillar of Russia's AML/CFT regime. Rosfinmonitoring has an integral role in the facilitation of this co-operation and co-ordination amongst competent authorities, as well as within its own territorial bodies.

166. Rosfinmonitoring actively exchanges information within its territorial bodies, including the development of regional risk indicators. Annually, Rosfinmonitoring issues around 20 methodological recommendations, which include risk indicators, methods and techniques for analysts. Exchanges occur via Rosfinmonitoring's secure system (UIS). Moreover, Rosfinmonitoring's central and regional offices are located in secure buildings that are guarded on a round-the-clock basis.

167. Several Russian authorities co-operate at the federal and regional levels, including through the following working groups to exchange financial intelligence and information:

- Multiagency task forces (for certain financial investigations)
- Working group at the Prosecutor General's Office (as well as at the regional offices) on investigating economic crimes
- Expert-consultative group at the National Anti-terrorism Committee on issues of combating the financing of terrorism.
- Interagency Working Group for Countering Illegal Financial Transaction (IWG) – a coordination agency, established to facilitate effective co-operation of supervisory, law enforcement authorities and the BoR, aimed on prevention, identification and disruption of illegal activity with a goal of obtaining and laundering criminal proceeds.

168. FIs, supervisors and LEAs are also members of the Compliance Council, which provides an active gateway between the public and private sectors on emerging ML/TF trends and typologies. An example of effective collaboration between Rosfinmonitoring and the Compliance Council participants involved the development of a list of special indicators aimed at identifying bankcard and e-

wallet transactions related to drug trafficking. These indicators notify LEAs about the patterns of suspicious activity, which obliged entities use to identify suspicious transactions possibly linked to drug couriers, stashers and laboratory staff. Furthermore, the Council members helped detect an illegal encashment scheme involving payroll payments and the use of a fake temporary identity card of a Russian national and a fake military ID to obtain bankcards.

169. In addition to general co-operation, LEAs and other relevant authorities, including Rosfinmonitoring establish task forces when investigating complex cases on predicate offences, ML and TF. A consistent feature of these task forces is the role of Rosfinmonitoring. It may host LEAs for monthly meetings on large cases and LEAs and Rosfinmonitoring engage in a constant dialogue, both in terms of formal disseminations (spontaneously and upon request) and daily, informal communication. Task forces are common at the headquarters level of competent authorities in Moscow, but the model is also replicated in the federal districts. These multidisciplinary task forces have produced dozens of successful cases.

170. Rosfinmonitoring also works closely with other AML/CFT supervisors, in support of their function to regulate, control and audit the reporting entities under their supervision and improve the overall quality of STRs. This is evidenced through the aforementioned FTF indicators pilot project. Non-confidential information is exchanged with supervisors and FIs/DNFBPs through the secure, password-protected Personal Account. The exchange of confidential information delivered by the State Courier Service of Russia to ensure security.

171. All financial information and intelligence exchanged between Rosfinmonitoring and LEAs, as well as amongst LEAs, is securely protected. Egmont requests are processed within the central unit, which further protects the confidentiality of requests and ensures timely responses. Rosfinmonitoring has a dedicated unit in its central office, as well as in each territorial office, dedicated to information security and the protection of classified and confidential information. The protection of classified and confidentiality of information exchanged is strictly enforced as required by law (see c.29.6).

172. Rosfinmonitoring's database is protected by a number of safeguards and can only be assessed by approved officers of Rosfinmonitoring. Access is granted through three-factor authentication: biometric information, smart card, and password.

173. Personalised access privileges are also used to implement differentiated access to confidential information contained in the database so that employees can only use those components of the system that are relevant to their official duties. Requirements are applied to technical devices, program components, and a unified key-card is used to access office space and computers. To protect databases from unauthorised access various security software are used, access privileges to components of the database are assigned, internal networks for analysts are created along with personal access to computers.

Overall conclusions on IO.6

174. Russian LEAs routinely and effectively request, receive (including spontaneously) and use financial intelligence and other relevant information to develop evidence to investigate ML, TF, predicate offenses, and to trace criminal proceeds. Rosfinmonitoring is core to the functioning of Russia's AML/CFT regime, as it has a wealth of available data, including a high volume of STRs and MCRs, and employs sophisticated technologies, and high degree of automation, to prioritise, generate, and contribute to cases pursued by LEAs. LEAs request and receive financial intelligence in line with Russia's identified risks. Information and intelligence are protected when exchanged by competent authorities.

175. Russia is rated as having a high level of effectiveness for IO.6.

Immediate Outcome 7 (ML Investigation and Prosecution)

ML identification and investigation

Organisation of money laundering investigations

176. The main LEAs that identify and investigate ML offences are the MoI and FSB, and the IC conducts a large number of ML investigations once the offence has been identified. These LEAs have either ML units or dedicated ML experts in their central offices, in their regional or territorial branches, and within specialised departments.

177. MoI, FSB, IC, and FCS have personnel who specialise in identifying and/or investigating financial crime, including ML. The IC focuses on, among other things, corruption-based ML cases. MoI has five units dealing with ML, including one dedicated to combatting the laundering of drug proceeds. MoI's General Administration for Economic Security and Combatting Corruption houses an ML/TF division and regional departments of MoI have similar ML and/or TF units. FCS has a General Directorate for Anti-Smuggling and regional directorates that conduct financial investigations. Financial investigators are trained extensively and on a continuing basis, including at the ITMCFM.

178. Only investigators with significant experience investigate complex ML or major economic crime. As noted in the TC Annex, all investigators are expected to be able to conduct financial investigations, and it appears that training for new or junior staff usually enables them to, at a minimum, spot potential ML and determine whether a case should be escalated if it is beyond their capability. When necessary, LEAs can transfer investigations to different regions or central offices, or send investigators on secondment within their agencies or to the FIU. If there is a conflict between LEAs over jurisdiction or the performance of tasks, the prosecutor resolves disputes.

179. The LEA that identifies the ML activity may not be the agency that formally investigates it. The agency that detects the crime may hand off the investigation to another based on the nature of the predicate offence. However, in practice, Russia provided numerous case examples where a multiagency task force was formed to investigate ML. In such task forces, one LEA generally plays a leading role, but it is common to have some combination of MoI, FSB, or IC working on different aspects

of an investigation depending on resources, expertise, and primary jurisdiction. A consistent feature of any task force investigating sophisticated ML is Rosfinmonitoring. It will, for example, host LEAs for monthly meetings on large cases. LEAs and Rosfinmonitoring engage in a constant dialogue, both in terms of formal disseminations (spontaneously and upon request) and daily, informal communication. Task forces are common at the headquarters level of the competent authorities in Moscow, but the model is also replicated in the federal districts. These multidisciplinary task forces have produced several successful cases.

Investigative process

180. There are two distinct phases of a criminal investigation in Russia which are key to understanding effectiveness under IO.7, IO.8, and IO.9. Both phases may entail financial investigation. The first phase is known as the pre-investigative phase, or criminal surveillance. The second is the investigation, also known as the public investigation.

181. The criminal surveillance phase lasts for two months—with the possibility of extension—during which time LEAs interact with Rosfinmonitoring, identify suspects and financial transactions, and follow the money. Criminal surveillance is undertaken by operational units with field agents who use criminal intelligence and operational search measures to identify crime and carry out covert investigative work, such as surveillance of targets and gathering of financial records.

182. If a crime is identified during the pre-investigative phase, a report is submitted to an investigator, who must then decide within three days whether to initiate a formal criminal investigation. The assessment team explored whether the short three-day period was problematic, but found that the deadline can be extended up to thirty days. Further, if it is not clear whether an ML investigation should be opened, the investigator can ask field agents to gather additional information. Investigators confirmed that if information is inconclusive, they pursue rather than drop ML investigations. Nevertheless, assessors consider that in some circumstances, the two months (or slightly more) of covert investigation may not be long enough to map complex ML networks.

183. In the second phase, the public investigation, LEA activities are overt and suspects have certain constitutional rights. Examples of techniques used at this stage are searches, seizures, arrests, and ex parte motions to the court for provisional measures.

184. Prosecutors oversee both phases, and Russian authorities demonstrated that there is sufficient communication and fluidity between the field agents, the investigators, and the prosecutors. If the prosecutor believes that a decision by an investigator not to initiate a criminal investigation was incorrect, he or she can reject the decision and order one. An ML investigation can be opened at any time based on new information uncovered in the course of a predicate investigation, and investigations are initiated against unknown perpetrators. Prosecutors must review case files at least once every six months for potentially "missed" ML. Eighty-eight ML cases were reopened in 2017, showing the advantage of prosecutorial oversight and indicating that there is room for additional training for investigators on ML. There are reportedly prosecutors within GPO dedicated to supervision, as opposed to

casework and prosecution, but there were no indications of a shortage of prosecutors or any impact on the timeliness of litigation.

185. When an ML investigation is completed (or if a person is arrested and charges must be laid), the investigator presents his or her file to the prosecutor. While prosecutors exercise discretion on the particular charges brought, the percentage of cases refused was estimated to be less than 1%. As part of the prosecutor's oversight role during prior phases of the investigation, he or she is supposed to guarantee that the financial aspects of the case have been examined and all appropriate investigative measures have been exhausted. GPO considers it a serious problem if an investigator presents a file that does not contain sufficient evidence, and LEAs confirmed that there may be discipline incurred by the investigator in such circumstances. Closing a case at this stage, or dropping certain charges, requires approval from the prosecutor. Judges may rarely "requalify" an offence if they deem the criminal conduct or penalty is better served by another charge.

186. The assessment team found that the investigation of ML was a methodical, highly-defined process. The benefits of such a system are efficiency and caseload productivity. Investigations are likely to result in charges and they do not linger on without resolution: nearly 94% of predicate investigations in key ML risk-areas end in criminal charges and most ML investigations do result in prosecutions. However, a potential drawback of such a system is that especially complex cases with many avenues of investigative interest or possible links to other schemes may remain unexplored, especially if the pre-investigative (covert) phase cannot be prolonged. This could be one reason why 3PML and stand-alone ML charges are not routinely developed when another offence becomes apparent, as discussed further below.

Pursuit of potential cases of money laundering

187. There are over two million crimes committed in Russia every year, of which approximately one-third are proceeds-generating offences that could be a basis for ML under Russia's all-crimes approach. ML is well-detected through financial investigations, and when it is detected, the authorities initiate investigations in more than 91% of instances, which generally result in charges for ML or another offence. This indicates that Russian authorities take possible ML activity seriously. By comparison, only 54% of all predicate offences identified result in the opening of criminal investigations, as the other 46% of crimes cannot be confirmed to have occurred. The analysis below examines the circumstances in which ML is detected, investigated, and prosecuted.

188. Russian authorities explore potential ML as a matter of course when investigating predicate offences, and leads on potential laundering are often spotted and analysed by the FIU and further investigated by LEAs. However, offences that might be ML when there is no pre-existing predicate investigation are not generally investigated as such, hence the reliance on alternative offences and a lack of autonomous ML prosecutions.

Table 3.10. Number of ML Offences Identified

	2013	2014	2015	2016	2017	2018
Art. 174.1 (self-laundering)	372	695	802	794	674	968
Art. 174 (3PML)	210	79	61	24	37	25
Art. 175 (acquisition/sale of proceeds)	3,438	2,916	2,590	2,410	2,464	2,143
Total Identified	4,020	3,690	3,453	3,228	3,175	3,136
Percentage of Offences Constituting Art. 175 Violations	85%	79%	75%	74%	77%	68%

189. As calculated from the data below, Russia opens an average of 652 ML investigations per year into the core ML offences under CrC Articles 174.1 (self-laundering) and 174 (3PML), plus another 2 484 investigations per year into violations of CrC Article 175 (acquisition/sale of proceeds).

Table 3.11. Number of ML Offences Investigated

	2013	2014	2015	2016	2017	2018
Art. 174.1 (self-laundering)	358	533	688	655	584	696
Art. 174 (3PML)	198	85	46	24	25	16
Art. 175 (acquisition/sale of proceeds)	3 257	2 728	2 413	2 193	2 260	2 052
Total Investigated	3 813	3 346	3 147	2 872	2 869	2 764
Percentage of Investigations Relating to "Core" ML Offences	14%	18%	23%	24%	21%	25%

190. Russia is predominantly investigating the acquisition, possession, or use of criminal proceeds, as opposed to concealing or disguising (i.e., laundering) of proceeds. There are approximately 3 135 ML investigations per year. The vast majority of these, around 75%, comprise violations of Article 175, which criminalises the acquisition or sale of property that has been illegally obtained. Authorities characterised this offence as likely to involve smaller amounts of money derived from minor theft and drug crime. The core ML offences (Articles 174 and 174.1) that tend to include higher-end laundering make up a smaller proportion of initiated investigations. Within the 25% that represent core ML offences, most of the cases identified are self-laundering. The number of 3PML offences detected has been surprisingly low given Russia's threat picture (24 in 2016; 37 in 2017; and 25 in 2018).

191. In addition, a lower percentage of detected 3PML cases lead to investigations than for other types of ML. 66% of detected instances of 3PML resulted in investigations in 2017 and 2018. Recalling that most ML identified is investigated – 91% of it, in fact – this discrepancy is noteworthy. Russian authorities contend that this balance between the different types of ML detected and

investigated accurately reflects the range of ML activity committed in the country, whereby offences are mostly low value and more likely to involve acquisition/possession than complex laundering. In light of the low and declining number of 3PML investigations—e.g. only 16 in 2018—the authorities state that the initial findings of LEAs during criminal surveillance are more likely to indicate that an alternative offence was committed. Nevertheless, the comparatively low rate of detection of 3PML indicates that more opportunities may exist for LEAs to uncover sophisticated and/or high-value ML, especially in the financial sector and involving proceeds sent abroad, particularly those related to public funds and corruption. Decisions not to move forward with an ML investigation simultaneously with an alternative offence investigation are also potentially missed opportunities.

192. Russia uses numerous offences, including alternative criminal justice measures, to prosecute activity that may be 3PML (such as the illegal banking charge, as noted below). However, this does not fully explain the low rate of initial detection of 3PML or the decision made approximately one-third of the time not to formally pursue a 3PML investigation. Perpetrators providing "shadow financial services"—a major issue according to the ML NRA—should be investigated as potential launderers when their conduct is detected, even if the exact nature of the money they are handling is initially unknown to authorities or if the known dirty money is commingled with clean money.[27] When potential shadow financial service providers are identified by the authorities, the fact that such suspects may have a percentage of licit business does not mean that they may not also be laundering proceeds. Indeed, dealing in legal-origin money in addition to illicit money may serve to further conceal proceeds.

Box 3.7. Financial Investigations Uncovering Upstream Criminal Activity

- An investigation was conducted into an organised crime group (OCG) using 150 shell companies to move money through an illegal bank under CrC Article 172. The investigation revealed that some of the clients of the group were the managers of three Russian banks who were stealing assets through unrecoverable loans. These managers were later charged with fraud and embezzlement.
- In the course of another investigation into numerous persons for illegal banking under CrC Article 172, LEAs uncovered a public funds embezzlement scheme carried out by a state

[27] Russia defines the shadow economy in the ML NRA: "the economic activity hidden from society and the state, which is outside the state control and accounting. It is an unobservable, informal part of the economy. In fact, any business that results in the concealment of income from state bodies, or tax evasion, can be considered a shadow economic activity. It may also include, but is not limited to, illegal, criminal economies." Shadow financial services can be understood as both natural and legal persons providing licenced services who conspire with criminals to launder their funds, as well as unlicenced operators, such as illegal banks.

contractor in Orenburg. Prosecutors charged the head of the contractor with fraud and self-laundering (through the use of the underground bank).

193. ML charges seem not to be consistently developed when another offence becomes more readily provable, such as illegal banking. LEAs stated that in such cases, the clients of the illegal bank are identified and investigated and their sources of funds are examined. Some examples of LEAs working backwards to uncover the predicate criminality of the clients of an illegal bank are set out in Box 3.7 above. This demonstrates that Russian LEAs, particularly when working in co-ordinated task forces, can start investigating a criminal financial enterprise and uncover both the "clients" and their sources of illegal proceeds. It is not clear that this upstream work is done in every instance or that ML charges will be used against money movers. These and other examples demonstrate that certain shadow schemes could rightly be considered 3PML and that ML investigations should not be prematurely ceased because the nature of the proceeds may actually be uncovered in due course. LEAs do not seem to undertake sufficient efforts in all cases to investigate facts that might demonstrate, even circumstantially, that the perpetrators had knowledge of or were wilfully blind to the criminal source of the funds they handled, therefore providing a basis for 3PML charges. While the activity may be disrupted sooner, the level of culpability of the defendants are the extent of complex networks handling criminal proceeds may not be uncovered. And when alternative offences are chosen for the sake of speed, ML investigations may be ceased, potentially rendering international co-operation more of a challenge when less common offences, less likely to satisfy dual criminality, are used.

194. Authorities are pursuing some 3PML as self-laundering or prosecuting alternative offences that do not require a full understanding of the underlying predicates. The former choice does not provide any strategic advantage. The latter choice may have a detrimental effect on identifying predicate crimes (and thus, the chance to investigate and charge them), or result in punishing true laundering activity with alternative offences, which, while considered serious crimes in Russia, may not be recognised by other countries when Russia seeks international co-operation, including for confiscation purposes. Furthermore, while both illegal banking (CrC Article 172) and the "outflow offence" (CrC Article 193.1) are punished proportionally to ML, the alternative offence that has resulted in the most convictions (CrC Article 173.2) is not punished as stringently. Russia should pursue more 3PML investigations alongside alternative offence investigations, so that international co-operation is easier to obtain and actual money launderers are sanctioned as such. This is particularly relevant in Russia's context, where domestically generated proceeds are being sent for further laundering abroad on a large-scale.

FIU's role in money laundering investigations

195. As noted in IO.6, Box 3.1, various sources of information are used by LEAs to identify ML through financial investigations. However, ML is most commonly identified in the course of predicate investigations or through Rosfinmonitoring information. The assessors found that reactive and proactive disseminations from

Rosfinmonitoring have a high conversion rate in terms of ultimately charging ML. LEAs routinely make requests to Rosfinmonitoring in ML investigations of any significant scope, and Rosfinmonitoring often delivers a "ready-made" product that links suspects and transactions and shows the flow of criminal funds.

196. Although authorities emphasised that Rosfinmonitoring was a trusted source, LEAs routinely take steps to corroborate information provided by Rosfinmonitoring. Upon receiving FIU reports, investigators will, for example, conduct searches of premises, obtain tax information from FTS, or seek company ownership information from the USRLE. Rosfinmonitoring responses and records obtained from FIs help LEAs uncover BO information or investigative leads. LEAs collect evidence usable in court to substantiate intelligence provided by Rosfinmonitoring and they equally employ traditional and sophisticated techniques to investigate ML. LEAs have also begun using co-operators to help dismantle ML networks, enabled in part by an increasing acceptance of plea bargains. For instance, in the case described in Box 3.15, lesser participants in the OCG were used as witnesses or co-operating defendants who underwent a separate, simplified trial and received benefits in sentencing in exchange for co-operation. However, as mentioned in Ch. 1, enhanced protections in law for whistle-blowers in financial crime cases would contribute to detection, investigation and prosecution efforts, including by enabling persons to confidentially report crimes within large and/or state-run FIs or other businesses.

197. As a source for initiating and enhancing ML investigations, Rosfinmonitoring's responses and spontaneous disclosures are important to LEAs. Of the 3 196 investigations into core ML offences conducted between 2013 and 2017, nearly half—or 1 406—were estimated to be initiated based on information from Rosfinmonitoring. Assessors tested the hypothesis that LEAs might be overly dependent on Rosfinmonitoring, but the FIU model in Russia is unique in its resources and integration into the investigative process and this is not viewed by the assessors as compensating for any weakness among LEAs. On the contrary, the LEAs and prosecutors interviewed in three regions and Moscow demonstrated their expertise in leading ML investigations.

Consistency of ML investigations and prosecutions with threats and risk profile, and national AML policies

198. Russia is a large country that faces a range of ML risks which vary from region to region. The assessment team sought to answer whether ML was an investigative priority only in Moscow or whether it was equally pursued in the regions by skilled investigators and prosecutors. Statistics show that ML is identified across all federal districts, with the most ML offences identified in the Siberian, Volga, and Central districts between 2013 and 2018. Select case examples (see Boxes 3.9-3.10) demonstrate the geographical and topical diversity of ML prosecutions. During the on-site visit, assessors met with LEAs and prosecutors from Nizhny Novgorod (Volga), St. Petersburg (North West), and Siberia, to confirm that quality investigations are carried out at the regional level in line with both local risks and national priorities.

Box 3.8. Siberian ML Case, Based on Regional Risk

Crime in the timber industry is a key local risk is the Siberian region. In 2015, a spontaneous disclosure from Rosfinmonitoring prompted authorities to investigate firms appearing to export wood to China and submitting inflated VAT reimbursements. Financial intelligence allowed LEAs to connect companies controlled by the same individuals that engaged in VAT fraud to suspicious trade activity. A task force was formed consisting of FCS, MoI, FSB, and the FIU, overseen by the local GPO. The OCG had around a dozen accomplices in two cities; one team falsified documents for VAT reimbursement and the other made the trade revenues appear real. The scheme yielded 250 million RUB or EUR 3.4 million. Proceeds were used to buy buildings, through a chain of shell companies, which were incorporated into the scheme, e.g. for use as offices, and to acquire luxury cars for D, the main defendant, who arranged fake leases with entities he controlled. D was charged with self-laundering (Art. 174.1), participating in an OCG (Art. 210), misappropriation (Art. 160), and VAT fraud. To date, eight people have been arrested and charged, and two remain fugitives, including D. One person pled guilty and provided co-operation to identify assets, many of which have been seized.

Box 3.9. St. Petersburg Cases, Based on Regional Risk

Due to its proximity to Baltic countries and status as a transport and logistics hub near Europe having many regional and national banks, the team explored with LEAs in St. Petersburg ML cases involving key local threats such as organised crime, transfers through the banking system based on fictitious economic activity, and corruption.

- A Leningrad drug trafficking organisation, operating its own laboratory and laundering money out of Russia, was recently dismantled. LEAs sent a request to Bulgaria containing information about one wire transfer that was received by a Russian national in Bulgaria linked to the organisation. Within days, this person was identified as the leader of the scheme who was involved with numerous OCGs. Russian authorities cooperated closely with LEAs in Bulgaria. MoI seized more than 1 ton of methamphetamine. ML was accomplished through ATM cash withdrawals and transfers through companies established in Bulgaria. The leader was extradited to Russia and additional Bulgarian and Lithuanian suspects were identified. The case is ongoing.

- Russian financial intelligence identified a company that financed construction and development in Baltic countries. Upon financial investigation and FIU co-operation with Latvia, it was determined that the alleged land plots did not exist, contracts were fabricated, and there was no economic activity justifying transfers to Latvia, Estonia, Poland, and Lithuania exceeding RUB 300 million or EUR 4 million. The investigation is ongoing into the source of funds moved offshore, but they are suspected to be the proceeds of tax evasion and corruption. The organiser of the scheme – a Russian national living in Estonia – had a criminal history and was the former president of a bank whose licence was revoked. He was charged in early 2019 with self-laundering (Art. 174.1) and remitting currency to non-resident accounts using fake documents (Art. 193.1, the outflow offence).
- A Russian individual, S, was previously known to authorities for laundering money through the purchase of private jets, although the case against him could not be made without foreign evidence. FSB began investigating S for the theft of public funds intended for regional transportation projects when they received a lead from disclosures in the Panama Papers. S, as the manager of a large industrial site, siphoned government funds and laundered them through offshore companies. The financial investigation involved co-operation with 17 FIUs, including the Greek FIU, which detained a yacht beneficially owned by the suspect. S laundered stolen money with the help of a law firm with offices in two offshore havens, mostly through the purchase of luxury assets, concealed using foreign foundations and shell companies. Six persons have been charged, and five have been sentenced. S remains wanted and has been charged with self-laundering (Art. 174.1) and the outflow offence (Art. 193.1). A parallel civil lawsuit has been filed to recover RUB 300 million already seized.

199. Russia is detecting and investigating ML activity partly in line with its risk profile and national policies, but there are some areas where alignment could be closer. According to the ML NRA, the highest ML risks pertain to crimes committed within the areas of budget spending and taxes ("public funds"), corruption, the financial sector, and drug trafficking. Between 2013 and 2018, approximately 85% of ML offences detected related to these high-risk areas. By a significant margin, most ML offences investigated relate to drug trafficking, although this is on a decline, while financial sector predicates for ML are on the rise. This trends appears consistent with the current risk picture. MoI explained that the relative decrease in drug ML may be based on publicised drug seizures in 2015-2016 and a preventive counter-narcotics approach that focuses on stemming the wholesale importation of drugs into Russia, especially by Central Asian trafficking organisations. Meanwhile, the MoI and the FSB confirmed that financial sector crime is a major emphasis of

their current work at the direction of senior leadership and the IC described a tactical working group established with BoR to combat ML in the banking sector.

Box 3.10. Drug Trafficking Case

An international OCG led by G trafficked in large quantities of heroin along the Northern Route. Ten units of the organisation were active in Russia, Tajikistan, Afghanistan, UAE, and elsewhere. The investigation was initiated by Rosfinmonitoring. STRs related to drug trafficking and associated ML are coded and are risk-rated after the integration of other sources of information, e.g. travel patterns of individuals along routes known for opiate trafficking. Based on a dissemination, LEAs further uncovered the financial network supporting the trafficking organisation, including the money manager who was only responsible for laundering proceeds. Drug revenues were used to acquire prestigious real estate and open bank accounts in Dubai, which were seized with assistance from UAE (this co-operation experience subsequently resulted in the signing of a permanent MOU). The equivalent of USD 37.7 million was laundered. G was extradited and convicted in Russia of self-laundering (Art. 174.1) and participating in an OCG (Art. 210) and 35 people have been sentenced in Russia, Kazakhstan, and Tajikistan.

Proceeds of corruption

200. The high-risk area identified in the ML NRA as budget spending and taxes is a slight misnomer, as it actually encompasses many offences qualifying as corruption, such as misappropriation, theft, and embezzlement by public officials, including officials of state-run enterprises, and government contractors. The "cost of corruption" in Russia was estimated by the IC to have exceeded RUB 123 billion or EUR 1.69 billion in the last seven years. The private sector also rated bribery as a generator of proceeds on par with offences involving public funds.

201. Using sophisticated technology and human analysis, Rosfinmonitoring identifies the potential misuse of public funds and flags suspicious government contracts and collusive schemes to defraud the state. Results are disseminated to LEAs, who pursue both predicate and ML investigations based on Rosfinmonitoring information and other sources, including citizen complaints.

202. Public funds offences make up the second-greatest share of ML investigations and prosecutions (after drug predicates), which is consistent with the risk environment. Prosecutions under Article 175 (handling proceeds) outnumber those under the core ML provisions in this and all other risk areas. Public funds-ML prosecutions peaked in 2013-2014, and have declined since then. Several case examples in this area were discussed during the on-site visit, including one summarised in Box 3.11. Even though the number has decreased by half in recent years, there were still around 10 000 offences related to public funds and tax crimes recorded in 2018, so authorities need to maintain their focus on ML associated with this key threat.

Box 3.11. ML Case Involving Public Funds

In 2018, the Siberian branch of Rosfinmonitoring identified suspicious contracts awarded by a large state hospital. Upon investigation and consultation with the Federal Anti-Monopoly Service, the FIU uncovered that the bidders on the contracts secretly had the same owners. Disseminations were made to the FSB and MoI on suspicion of large-scale misappropriation and theft. The Deputy Director of the hospital allegedly abused his public office by establishing a group of associates to bid on lucrative contracts he was in charge of, and this group won the tenders at inflated prices. Nearly RUB 1.35 billion or EUR 18.4 million was misappropriated and laundered through shell company accounts. The Deputy Director and three others have been charged with self-laundering (Art. 174.1) and fraud (Art. 159), and numerous searches and asset seizures have been conducted. Documents and cash were seized from the Deputy Director's bank box and a deed for an undeclared apartment was uncovered, which is being considered by GPO for potential confiscation under Federal Law 230 (unexplained wealth).

203. In contrast, in the separate risk area of corruption specifically related to bribery and abuse of office, the number of ML cases is low, relative to the number of predicate offences, and not entirely aligned with risk. Corruption violations have increased more than threefold from 2007 to 2016, and 7 400 law enforcement officers and officials at various levels of government have been convicted of corruption in the last 3.5 years—around 2 000 each year on average. In 2018, there were 2 612 identified offences of paying a bribe and 3 499 instances of receiving a bribe. But the number of corruption-based ML investigations was fewer than forty per year between 2013 and 2017, with just over one dozen in 2017. Although very recent, it is a positive sign that the number of ML investigations opened into this type of corruption predicate has increased more than twelve-fold—to 162—in 2018, which is more commensurate with risk.

204. The authorities state that most bribes are small and proceeds are often immediately spent or are simply stored, not laundered: according to the GPO, the average bribe amount in 2018 was around RUB 609 000 (EUR 8 062).[28] They also argue that some public funds cases would have involved bribery as a secondary offence and that national statistics may not fully reflect bribery cases. However, assessors do not find these arguments convincing. There are hundreds of large-scale bribes detected every year, and even smaller or "average" bribes can be laundered to allow corrupt officials to enjoy the fruits of their crimes. Furthermore, Russia criminalises the acquisition, possession, or use of criminal property (i.e., the spending of proceeds), and a 2013 law removed the monetary threshold in place for

28 *The Prosecutor General's Office Calculated the Average Size of a Bribe in Russia in 2018*, 18 Dec. 2018, www.rbc.ru/society/18/12/2018/5c18cf2e9a79471a4d084c63. Overall bribe amounts were estimated as totalling RUB 1.8 billion (EUR 23.8 million) in 2018, RUB 6.7 billion (EUR 97 million) in 2017, and RUB 2.3 billion (EUR 33 million) in 2016.

ML offences. Smaller bribery offences could be the basis for ML charges under Article 175, however, zero prosecutions for this offence with bribery as the main predicate have been brought since 2015. LEAs pointed out that bribery offenders are often caught in the act and thus have no chance to launder proceeds. While this may be the case sometimes, there is undoubtedly sophisticated and well-hidden bribery occurring that is not known to LEAs in advance and which can be uncovered through financial investigations.[29]

205. Given the prevalence of bribery and abuse of office offences in the country, Russia could be expected to use ML prosecutions to a greater extent in order to lessen the ability of PEPs to spend bribe money to acquire luxury goods and other assets. Domestic officials[30] engaged in bribery schemes involving significant sums that are harder to conceal are more likely to launder their funds abroad, such as through expensive real estate, so the investigation of gatekeepers who launder bribe proceeds is equally important. Technical deficiencies in R.12 and less robust identification of PEPs and close associates by DNFBPs—as well as questions surrounding the fullness of measures by FIs to verify beneficial owners—increase the importance of investigations and prosecutions to combat the laundering of the proceeds of corruption that are not simply "stored," but which find their way into the legitimate economy through the financial and DNFBP sectors. There is room for improvement in combatting ML linked to this strain of corrupt conduct, particularly since the risk of participation of individuals (intermediaries) associated with public officials in ML schemes is rated highly in the ML NRA.

Box 3.12. Komi Corruption Case

The IC led a task force, including the FSB, MoI, and Rosfinmonitoring, in investigating a corruption and ML scheme. G, the Governor of Komi, his Deputy, a number of PEPs including local MPs, and several businessmen engaged in a scheme whereby a foundation controlled by G for state investment was used to acquire state assets and enterprises and sell them extremely undervalue to companies ultimately owned by G through a series of legal entities. The group also engaged in bribery and embezzlement. LEAs began looking into citizen complaints and made requests to Rosfinmonitoring, just as the FIU was investigating STRs filed by banks concerning the non-payment of loans guaranteed by Komi and interest free loans to state entities. LEAs carried out undercover operations and 80 searches in three cities, and used information from Rosfinmonitoring. The OCG was active from 2006 to 2015 – over EUR 47 million was embezzled, nearly EUR 3 million was received in bribes, and amounts laundered exceeded EUR 13 million. N, the Moscow-based financier, as a member of the OCG, facilitated the

29 The assessment team did not see the deterrent impact of corruption-related predicate prosecutions in terms of a decrease in identified corruption offences. These have remained around 30 000 per year since 2014.

30 As for foreign officials, since ratifying the OECD Anti-Bribery Convention, Russia has opened one investigation into bribery of foreign public officials.

laundering of its funds. He was convicted of self-laundering (Art. 174.1) and participation in an OCG (Art. 210) and sentenced to six years. Other members of the OCG were also convicted of ML, including the Deputy. The Governor was convicted of fraud, bribery, and self-laundering and was sentenced to 11 years in prison, fined the equivalent of EUR 2.2 million, and banned from holding a position for five years.

Laundering through the financial sector and "laundromats"

206. The ML NRA notes that in recent years, substantial amounts of licit and illicit money have been moved offshore through Russian FIs, particularly via non-resident legal persons and structures.[31] The authorities conclude that the banking sector is highly exposed to threats posed by criminal elements due to its dominant role in the financial sector and the wide availability of financial services. The assessors' view of effectiveness on IO.3 is that risk-based supervision for AML purposes within the sector is moderate, which means that criminal enforcement in the sector becomes relatively more material. Russian authorities understand that FIs are used to conduct high-risk transactions, including cash transactions and cross-border financial transactions. They also acknowledge the existence of "laundromat" schemes touching Russia and other countries. This is borne out in public media and reporting, and in MERs of transit and destination countries.

207. In terms of the threat identified in the NRA related to the financial sector, ML linked to theft, fraud, embezzlement, and forced bankruptcy schemes that generate significant proceeds are pursued diligently. Laundering linked to dishonest bank managers and owners is charged in line with Russia's risk profile, especially when the FI or its shareholders are the victim. Many bank licences have been revoked and the sector is being cleansed of risky institutions. However, while supervisory actions have resulted in consolidation and presumably increased levels of stability and AML compliance, the work is not done: LEAs are still uncovering banks controlled by criminal associations through holding companies or concealed beneficial ownership. For example, the IC conducted an investigation in early 2019 in which an OCG abused several medium-sized credit institutions in Moscow by lending money to their own affiliated companies and then liquidating them, essentially collapsing the banks and laundering their proceeds.

Box 3.13. Cases Involving Crimes in the Financial Sector

Bank president: A spontaneous dissemination from FIU Gibraltar in 2015 and Rosfinmonitoring analysis helped to add an ML component to an ongoing bank investigation. The IC led the multiagency task force. It was reported that a DNFBP in Gibraltar declined to establish a trust for an individual who claimed to have made his money in the stock market. The DNFBP could not verify documents provided by the

[31] See also IO.8.

individual. The suspect was a bank president, whose bank was already under investigation in Russia by DIA and LEAs as a result of an inspection. He and the chairman of the bank allegedly embezzled RUB 27 billion through loans to shell companies guaranteed by the bank, never to be repaid. Laundering occurred through trusts in Cook Islands, St. Kitts and Nevis, and the Caymans, as well as accounts in Liechtenstein. The investigation is ongoing: the two bank managers are fugitives, several people have been arrested, and two were convicted. Charges against the bankers include embezzlement (Art. 160) and ML (Art. 174.1 and 174). Russia co-operated with 28 FIUs and has frozen USD 116 million in Liechtenstein and USD 4 million in Cook Islands.

Bank management: A complaint to the Deposit Insurance Agency (DIA) triggered a high-level meeting of MoI, Rosfinmonitoring, BoR, and DIA, as a one of the largest banks in the Tula region, whose customers included many state entities, was being raided. The top four managers of the bank issued unrecoverable loans and moved the proceeds between bank accounts of 33 legal entities they controlled. They used embezzled funds to purchase promissory notes issued by a commercial bank and invested some proceeds in their own businesses. LEAs froze assets belonging to the managers, including real estate, land, vehicles, and a ski resort valued at EUR 81.7 million. The bankers were convicted in June 2018 with participation in an OCG (Art. 210) and self-laundering (Art. 174.1). The directors of the board and executive board received 19 years in prison, the deputy CEO received 17.5 years, and head of securities, 16 years.

208. When an FI is raided, Russian authorities investigate the management, but it is not clear that complicit bankers or other financial sector actors are held accountable for facilitating ML by customers at their institutions. An in-depth examination of cases concerning well-known laundromat schemes confirmed that Russian authorities are taking some steps to confront this threat. However, additional steps should be taken to ensure that professional money launderers and their international networks—to the extent they are subject to the jurisdiction of Russia—are prosecuted for their facilitation of major ML.

209. Large laundromat schemes have been identified by journalists in recent years. Many of these were previously known to Russian authorities, who have in many cases already pursued criminal investigations into subparts of these operations, and, in several of them, have prosecuted the individuals involved. When information in the public domain reveals unknown schemes or targets—e.g. based on investigative journalism or leaked documents—additional investigations are usually opened.[32] Rosfinmonitoring and other authorities consider that media attention on laundromats has been helpful because it can increase pressure to

[32] The so-called Azerbaijani laundromat was alleged to be a system for laundering the proceeds of grand corruption and had reported financial links with Russia. Civil society informed the assessors that it requested Rosfinmonitoring to investigate this scheme; the outcome is unknown.

engage in international co-operation, which they concede has been challenging. Russia has initiated dozens of criminal investigations in connection with the matters below, resulting in arrests and convictions. Billions of euros have been traced, dozens of complicit Russian banks have been shuttered, and suspicious outflows from Russia into Estonia and Latvia reportedly have been reduced. The few associated ML prosecutions have not yet been resolved.

Table 3.12. Actions Taken by Russian Authorities in Response to Laundromats[33]

Moldovan Court Orders	• Active 2011-2014, ~696 billion RUB transferred ($18 billion) • Identified in Russia through Moldovan FIU, 45 financial investigations launched • Based on fake loans, creditors sued debtors in Moldovan courts, complicit judges ordered debts to "paid" by offshore shell companies, controlled by Russians, into accounts controlled by court's marshal; funds disbursed through Moldinconbank (Moldova) and Trasta Komercbanka (Latvia) to new set of shell companies controlled by Russians • Funds derived from embezzlement from Russian banks • All records of the main Russian bank involved destroyed by its owner, G, who also controlled other complicit Russian banks; investigators pieced together transactions to Latvia. • G was charged with participation an organised criminal group and ML, verdict expected summer 2019 • Other convictions obtained in 16 criminal proceedings, RUB 840 million frozen • BoR filed reports to LEAs and provided financial information that was used to open criminal cases • 9 bank licences revoked; supervisory measures taken by the BoR prevented involvement of other Russian banks in the scheme • Moldovan scheme was fully disrupted by mid-2014
Lithuanian/"Troika" Scheme	• Active 2005-2012, ~72 billion RUB transferred (EUR 0.99 billion) • Identified in Russia by Rosfinmonitoring strategic analysis • Shell companies used fictitious trade to send funds through Ukio Bankas (Lithuania) to beneficiaries around the globe, links to known criminal schemes • BoR filed reports on detected suspicious activity to Rosfinmonitoring and alerted GPO • T, a former banker, was the mastermind of one sub-scheme who transferred funds through insurance and reinsurance companies and ultimately through Ukio Bankas • ~19 Russian banks involved, 12 licences revoked • 3 financial investigations, 17 criminal proceedings, 1.23 billion RUB frozen • Convictions achieved in 5 out of 6 sub-schemes • T charged with illegal entrepreneurship, tax evasion, and ML; remains a fugitive
Estonian/Danske Bank Scheme	• Active 2007-2014, ~417 billion RUB transferred (EUR 5.7 billion) • Identified in Russia through Rosfinmonitoring strategic analysis • Simultaneously, BoR informed foreign supervisor about detected suspicious cross-border financial flows • 117 financial investigations launched, more than 7 000 Russian suspects • 3 criminal proceedings, convictions for fraud and illegal transfer of funds abroad • ~15 Russian banks involved, 9 licences revoked

210. A laundromat, as understood in Russia, is a stable, illicit financial network with a profit-making purpose that provides reliable, quick, and low-price cashing

[33] Russia considers its Estonian/Danske and Lithuanian investigations to be finished, but investigations into these schemes are ongoing in many jurisdictions. It is critical for Russian authorities to continue to examine additional information uncovered and respond to, and act on, foreign requests, if received, as well as new disclosures. In another laundromat-type matter, Rosfinmonitoring has recently joined a task force of FIUs looking into connectivity with the defunct Latvian bank, ABLV, which shows that some co-operation is ongoing.

services and diversion of funds abroad: it is fully or partly a ML service. Whether the laundromat consists of one large OCG or a combination of several groups, it does not discriminate among its customers. According to the authorities, laundromats use various FIs and businesses in other sectors—such as securities and insurance—which criminals manage or control or where they can exploit vulnerabilities. One laundromat may employ different typologies over time and may switch out shell companies and enabling institutions as the methods evolve. The assessors conclude that the approach of the authorities to break down laundromats into sub-investigations is achieving some results, however, ML convictions linked to such schemes have not been realised. The focus on sub-schemes may miss the bigger picture of professional ML that is occurring.

Other ML methods

211. Cases involving other high-risk methods for ML identified in the NRA are generally being pursued. Examples reviewed by assessors involved the misuse of domestic and foreign shell companies, cash, electronic means of payment, and (in a way) virtual assets. During the on-site visit, the Supreme Court issued an advisory order stating "that the subject matter of [the ML offences under the CrC] can constitute, inter alia, monetary funds transformed from virtual assets (crypto currencies), obtained as a result of committing a crime." While a positive step, this interpretation falls short of confirming that VA can itself be laundered. Even still, some cases related to VA, but not centred on VA transactions, have been pursued. One ML conviction involved the laundering of online drugs sales through bitcoin that was eventually cashed out, and another VA exchanger that served more than 300 clients in Russia and processed EUR 7.3 million was charged with illegal banking. However, the reported hundreds of billions of roubles in cash converted by traders at unlicenced, over-the-counter VA exchanges in shopping centres in Moscow deserve increased attention from LEAs as potential avenues for ML, per BoR.[34] Regarding trade-based ML, both the risk understanding and cases pursued by the authorities signal a concentration on fictitious invoicing schemes and fake trade documents used to justify money flows. Case examples did not usually involve the purchase of legitimate or counterfeit goods with proceeds for import/export into or out of Russia, or the exploitation of trade channels or supply chains for ML.

Types of ML cases pursued

212. Russia faces a significant ML threat: the GPO recorded 105 087 economic crimes in 2017. In the same year, there were 587 971 investigated predicate offences falling into the FATF's 21 categories. Domestic *damages* generated by crime (i.e., not including all types of *proceeds* from crimes without victims) are estimated at around RUB 210-230 billion or EUR 3.3-3.6 billion, per year. In addition to the significant domestic ML threat, officials met during the on-site visit explained that illicit funds from CIS countries and former Soviet republics are apt to transit the

[34] *The Central Bank Estimated the Shadow Turnover of the Moscow Markets at 600 Billion Roubles*, 12 April 2018, www.rbc.ru/finances/12/04/2018/5acf26f59a79471ae61bfbc9; *Moscow's Chinese Merchants Using OTC Cryptocurrency for Bank-Free Money Transfers*, 18 April 2018, www.ethnews.com/moscows-chinese-merchants-using-otc-cryptocurrency-for-bank-free-money-transfers.

Russian financial system, even though Russia is considered a source country and is not usually a final destination for criminal proceeds.

213. There has been an incremental increase in the number of core ML cases prosecuted, which, since 2014, has been consistently higher than 530 cases per year. On average, 557 people are charged with the two main ML offences annually. In the six years for which data was provided, Russia convicted an average of 323 individuals annually under Articles 174.1 and 174. This is adequate when combined with the fact that lower-level ML is prosecuted well under Article 175 (1 832 individuals convicted per year, on average). Compared to other jurisdictions, the 63% conviction rate is normal and shows that GPO is appropriately aggressive in charging.

Table 3.13. Prosecution of Core ML Offences (CrC Arts. 174 and 174.1)

	2013	2014	2015	2016	2017	2018
Number of Persons Charged	271	448	592	596	530	619
Convictions	164	248	311	412	379	426
Conviction Rate	61%	55%	52%	69%	72%	69%

Overall sophistication of ML cases

214. From 2013 through 2018, there were 15 729 total ML cases prosecuted. The majority of charges are for violations of CrC Article 175 (acquisition or sale of proceeds). Article 175 does not require proof of intent to conceal the nature or source of the funds or to make them appear legal; prosecutors need only show the perpetrator received or sold property obtained in a criminal manner. Inherently, Article 175 is reserved for less serious, lower-value offences, and 78% of all ML charges are for this basic type of crime.

215. The assessment team sees value in pursuing Article 175 cases, but remains concerned that the simple spending of criminal proceeds makes up such a large proportion of prosecutions as opposed to more sophisticated ML activity. The assessors' impressions of Article 175 as a lesser offence are proven by statistics showing that the overwhelming majority of offenders were convicted under paragraph 1 of Article 175—the lower level of this (lesser) offence. This means that the conduct did not involve either a substantial amount of money (not more than approximately EUR 19 960), a conspiracy or organised group, or misuse of official position. Assessors recognise that there are simply more low-value ML offences, and do not criticise the decision to pursue all ML regardless of value. It does not appear that low-level cases divert LEA's attention away from large-scale or complex ML. But the fact remains that the majority of cases are not for the type of ML considered more pernicious, i.e., the concealing and disguising of proceeds.

Third-party ML

216. The number of 3PML offences prosecuted in Russia is low, in absolute terms, and particularly in the context of a country with high levels of economic crime and a developed financial sector. It appears that authorities are not taking full advantage of opportunities to identify and prosecute third-party money launderers facilitating the movement of criminal assets through and out of Russia. This stems

at least in part from the low level of detection and investigation of 3PML noted above.

217. Most case examples reviewed by the assessment team and discussed on-site resulted in self-laundering charges. A few sophisticated 3PML cases involved an OCG working across borders, a true professional launderer with financial expertise, and a corporate embezzlement scheme. However, most of the case examples of 3PML were not particularly complex or of high-value. [35]

218. When the third-party offence is used, statistics show that it was mostly for basic ML (para. 1), for amounts laundered under the large-scale threshold of a mere RUB 1.5 million, or EUR 19 960.

Table 3.14. 3PML Cases (CrC Art. 174)

	2013	2014	2015	2016	2017	2018
Prosecutions	93	49	26	16	20	5
Convictions	67	51	20	9	11	22

219. The relatively low number of 3PML cases was notable prior to 2015—before significant numbers of non-compliant banks were remediated or shut down and when the environment for laundering was more permissive in the financial sector. But over the last three years, the prosecution rate for 3PML has decreased further, to only five cases in 2018. This minimal level of prosecution is also inconsistent with key vulnerabilities identified in the ML NRA, such as the provision of risky financial services by some FIs and the participation in ML schemes of associates of public officials. It would also be a useful legal tool for laundromat cases wherein the proceeds moved often belong to others.

220. There are some factors that partly mitigate the dearth of 3PML cases.

- First, certain third-party or even professional money launderers may be charged with other offences, such as CrC Article 210, which criminalises participation in an organised group established for the purpose of jointly committing crime. The authorities explain that large criminal groups prefer in-house ML services (although this understanding is not highlighted in the NRA). During the on-site visit, LEAs surmised that enforcement efforts have driven up the fees for outside ML, but this hypothesis is difficult to test and, therefore, to take into account. The assessors reviewed examples of individuals playing a distinct financial role within a group being charged as OCG participants, but there was no data available showing the frequency with which this provision is used to punish money launderers.
- Second, quasi third-party or professional launderers may be charged under the self-laundering offence because they were a member of a wider group committing predicate crimes. The defendant might be aware of the

[35] With the exception of the cases noted above, the 3PML case examples could be described as small in scope: two involved transactions with stolen cars, another involved the purchase of a car to promote drug trafficking; another involved laundering through a low-value fictitious contract; and one involved a loan made with proceeds which was repaid with trade in caviar.

predicate(s), but mainly be involved in the financial transactions in support of the group. This explanation may have some quantitative support, as at least between 2014 and 2018, the majority of self-laundering accusations were made pursuant to para. 4 of Article 174.1, which is ML committed by an organised criminal group *or* on an especially large scale (involving more than EUR 81 923). In 2016-2018, more than 100 prosecutions annually fell under the organised group sub-paragraph, which may or may not be a proxy for 3PML. Additionally, a defendant's status as a member of a group does not mean that he or she personally committed the predicate offences giving rise to the proceeds such that self-laundering would be the only available charge.

- Finally, as discussed in section 3.3.5, non-ML offences including illegal banking and illegally transferring funds into non-resident's accounts are used to capture some 3PML-like activity, but these are not conclusively ML cases for the purpose of core issue 7.3.[36]

Other types of ML

221. Additionally, in light of the numbers and examples of self-laundering cases supplied to the assessors, Russia is not prosecuting any or many stand-alone ML cases independently of predicate offences. Statistics for stand-alone ML were not available. LEAs stated that since ML methods are readily accessible (e.g. using cash or e-wallets), most criminals launder their own ill-gotten gains due to trust issues, such as a fear of theft by other criminals, and due to minimal special knowledge needed to launder. However, it is not clear why this should be unique to Russia or that the tools of ML are any more available in Russia than they are in other similar jurisdictions where stand-alone ML is routinely prosecuted.

222. Russian LEAs have capacity to pursue ML cases based on foreign predicate offences, but rarely do so in practice. Examples provided of ML cases based on foreign crime, often occurring in neighbouring countries, also tended to include domestic predicate activity. Examples proffered included one case pertaining to a multinational drug trafficking organisation where a kingpin was extradited and

[36] Russia prosecutes facilitators of the movement of funds out of Russia using CrC Article 193.1. This "outflow offence" punishes persons responsible only for one element of an illegal financial scheme: the transfer of funds to the accounts of non-residents under false pretences. While LEAs regard this activity as a specific type of illegal financial services, this is not equivalent to the pursuit of ML *per se* because it does not necessarily involve proceeds of crime. The offence may involve the transfer of proceeds, but it also may represent, among other things, capital flight, pure tax evasion, or clean money. Furthermore, the criminal conduct may involve the cross-border movement of funds, but the law does not require it (the pertinent element is a remittance to an account held by a non-resident, not an account held at a foreign bank). Thus, the outflow offence should not always be equated with international ML. For the purpose of assessing core issue 7.3, prosecution of the outflow offence does not categorically constitute a "type of ML." The same principle holds for violations of CrC Article 172. The illegal banking offence is proven by showing a lack of a licence plus (1) large-scale damage to individuals, organisations, or the state, or (2) profit-making on a large-scale. There is no way to know whether the illegal bank cases prosecuted always, often, or rarely move criminal proceeds, except when LEAs have worked backwards to uncover predicate criminality.

convicted on drug and ML charges in Russia. While the case had many international features and involved cross-border co-operation, there were clearly domestic predicates at issue in addition to foreign predicates. While this trend is generally in line with expectations because Russia is mostly a source country for proceeds, there is some risk of incoming proceeds deriving from CIS countries being placed in Russian banks or laundered through Russia. The authorities have opened ML investigations and conducted asset seizures in Russia based on foreign predicate conduct. Russia is capable to prosecute foreign predicate ML cases autonomously, but has not yet done so.

223. The assessment team discussed in detail several case examples of high-end ML, including linked to domestic and international OCGs. Task forces at the central and regional levels yielded quality ML prosecutions, to include the case study below. These cases are commendable. While the assessors have not weighted quantity over quality, the balance between these types of cases and the 78% of "basic" ML charges that predominate does present room for improvement.

Box 3.14. Sakhalin High-End ML Case

Rosfinmonitoring spontaneously disclosed information on the suspicious activities of certain government contractors in the Sakhalin region. LEAs happened also to be investigating a number of officials based on citizen complaints, including the Governor, KH, who created an OCG with the Agriculture Minister and his advisor. KH collected RUB 500 million or EUR 6.8 million in bribes from businesses in the construction, aviation, education, and energy industries in return for performing official duties. Bribes were transferred to offshore accounts and the advisor helped KH repatriate the funds to Russia for KH to use in cash. Bribes were also paid in rouble on bank cards held by nominees and converted into foreign currency. A multiagency task force led by IC investigated. Charges included bribery (Art. 290) and 3PML (Art. 174), and the officials' convictions were upheld by the Supreme Court. KH was sentenced to 13 years and a RUB 500-million fine; the advisor received 9.5 years and RUB 171 million fine. Notwithstanding the Governor's conviction, GPO filed an unexplained wealth lawsuit under Federal Law 230 and confiscated various assets worth more than EUR 10.4 million.

Effectiveness, proportionality and dissuasiveness of sanctions

224. *Based on statistics*, sanctions applied against natural persons convicted of ML appear partly effective, proportionate, and dissuasive, as terms of imprisonment for ML and fines are on the low end. The statistics on sanctions provided by Russian authorities related to cases in which ML was the primary offence, meaning the offence of highest gravity. Because ML is almost always prosecuted with a predicate offence that may qualify as the primary offence, the statistics are of limited utility in assessing the effectiveness of sanctions. Recidivism rates for ML convicts were not provided.

225. *Based on case examples*, it was often not possible to discern the ML sentence from the predicate sentence, due to the practice of cumulative sentencing and the fact that a significant portion of Russia's ML convictions are not for autonomous ML. Certain case examples included harsh prison sentences and large fines, however, it was challenging for the assessors to determine how much of an enhancement in punishment was achieved when a defendant was convicted of ML alongside a predicate offence. Furthermore, a number of the high-profile case examples presented to the assessment team on-site resulted in charges against missing defendants, some of whom were convicted in absentia. Figures on how many trials in absentia for ML have been conducted in recent years were not available, but sentences given to such persons may not, if ever, be fulfilled or effective in incapacitating specific offenders.[37]

226. Considering the statistics for ML (when it was the primary offence) and the difficulty of extrapolating from case examples, the assessors conclude that the penalties actually imposed present a mixed picture and that they are of moderate impact in punishing criminals and ultimately deterring proceeds-generating crimes and ML.

227. Fines have been the most frequently used penalty for ML in the six-year period between 2013 and 2018. The most common fine imposed on individuals for ML is minimal, at RUB 5 000-25 000 (up to EUR 340). In major cases, however, such as the corruption case detailed above in Box 3.12, fines may correlate to proceeds, as they did with the bribes demanded by the governor. Very minor ML cases are resolved solely through fines, without criminal charges. This tactic was used only six times in 2018, which is deemed by assessors an appropriate allocation of resources.

228. Between 2013 and 2018, on average, 392 defendants per year were given sentences of imprisonment when convicted of one of the three ML offences. Considering that 2 155 individuals are found guilty of these crimes on an annual basis, imprisonment is not a frequent sanction. This tends to confirm the lower-scale nature of many ML cases, particularly those under Article 175, as those which may not warrant custodial punishment. During the same period, a total of 1 940 individuals were convicted of self-laundering or third-party laundering (the two more serious ML offences). For those two crimes, *plus* the third, lesser ML offence, a total of 970 people were sentenced to incarceration for *any* ML offence. Thus, during the relevant timeframe, any given defendant had exactly a 50/50 probability of being sentenced to prison for ML. While the circumstances of each defendant differ and the punishment should fit the crime, the assessors conclude that the frequency of incarceration does not bring enough reliability or dissuasiveness. Even if it is assumed that the Article 175 offences did not warrant imprisonment at all, that would mean that only half of the defendants convicted of the more serious offences under Articles 174 and 174.1 were sentenced to imprisonment.

[37] Russian authorities note that trials in absentia proceed similarly to regular criminal trials in that the defendant is represented by an attorney and may appeal a verdict. If extradition of the defendant is sought, Russia provides assurances to the requested state that the defendant can seek a re-trial upon return. This is helpful, as trials for which a defendant is entirely absent may prompt procedural questions from foreign partners.

229. Under the CrC, basic ML is punished with a fine, and penalties escalate for the most serious ML to a maximum term of imprisonment of seven years. Conditional imprisonment and compulsory work are often ML penalties. In Russia, persons sentenced to prison for ML do not usually receive more than two years and the majority of ML cases have been punished with a term of imprisonment of less than one year. Between 2013 and 2018, two people were sentenced in the highest range for ML (more than five years).

230. The commonly used 1-2 year sentence is proportionate to penalties for some, but not all crimes in the financial sector, where the bulk of sentences are in the same range. The ML sentencing trends are disproportionate to penalties imposed on drug offenders and offenders in the budget spending and tax area. Drug crimes are most often punished with sentences in the 3-5 year range and fraud, embezzlement, and tax evasion frequently result in 3-5 year prison terms. These comparisons refer to the circumstances in which ML was the main crime of conviction, as ML is rarely prosecuted without associated predicates.

231. On-site discussions with a district judge and LEAs revealed that sentences for different crimes may be served concurrently, in full or in part. If all crimes are of light or medium gravity, then the less severe penalty will be subsumed within the more severe penalty. If the conviction includes an especially grave crime and sentences are concatenated, they cannot exceed by more than half the maximum penalty for the gravest crime committed. The judge emphasised that punishments must be fair and in line with the Supreme Court's Order No. 58 on the practice of sentencing and CrC Article 69 on cumulating. Judges also consider the situation of the defendant, including public danger posed, remorse, dependents, etc. However, even if a predicate and ML sentence run simultaneously, the ML sentences alone still appear to lack dissuasiveness.

232. Two drug-related ML cases were provided to demonstrate that ML adds value when combined with sanctions for the predicate offence.[38] In these examples, it is likely that the ML enhanced the sentences for those convicted of laundering and drug trafficking. But it is also likely that the conduct of the launderer was substantively different from the non-launderers such as to warrant differences in punishment (e.g. the defendants who were only sentenced for predicate crimes were accomplices). The assessors find that there is some sentencing augmentation provided by an ML conviction, but could not quantify the extent of this based on the information provided.

233. In six years, only six convicts were barred from holding a position as a result of a penalty imposed for ML. The assessors initially found this incongruous in light of the number of public officials and financial sector professionals featuring as ML defendants, but since ML is charged along with a predicate, those sentences will often prohibit such persons from holding positions. In fact, across criminal cases,

38 In the first case, the defendant was sentenced to 16 years in prison for drug trafficking and laundering EUR 198 000, and his accomplices were sentenced to 9-10 years for the trafficking crime only (ML differential: + 6-7). In the second case, the defendant was sentenced to 15 years in prison for preparation for the sale of 42 kilograms of heroin and laundering EUR 765 000, while his co-defendant was sentenced to 8 years in prison for the sale of 42 kilograms and preparation for the sale of 37 kilograms more (ML differential: + 8).

convicts were banned from holding positions more than 57 000 times in 2018. However, for financial sector offences, this penalty was not utilised frequently. This punishment is valuable in connection with ML and financial crime, as it can prevent opportunities for recidivism and ensure integrity in public service and the financial sector. Russian authorities state that even without formal debarment, felons convicted by a domestic court would not normally be able to work for government agencies or hold high positions in FIs due to strict requirements for candidates.

234. As noted in the TC Annex, Russia cannot prosecute legal persons, only sanction them administratively. The administrative offence for legal persons is available for use against obliged entities when negligent compliance results in ML, but no information has been provided on the number of such cases and so the effectiveness of non-criminal sanctions against legal persons has not been separately assessed. Competent authorities opt to prosecute owners and directors of companies or use the offences detailed below against natural persons who use companies to carry out ML.

Use of alternative measures

235. Russian authorities presented a suite of twelve alternative criminal justice measures that can be used for investigating, prosecuting, and punishing conduct that resembles, is indicative of, or may occur in connection with ML. Between 2013 and 2018, 156 527 alternative offences were identified and 81 836 individuals were convicted of these offences. Those discussed below were weighted by the assessors.

Illegal Banking

236. The offence that appears to have the most significant impact in combatting potential ML activity is banking conducted without a licence under CrC Article 172. LEAs noted that the charge of illegal banking is relied upon in 3PML situations when the suspect's knowledge of the nature of the proceeds is difficult to prove. The illegal banking cases shown to the assessment team presented facts typical of professional ML, as exemplified below.

Box 3.15. Large Illegal Banking Case

MoI, along with IC and Rosfinmonitoring, investigated Mr. M, the leader of a massive illegal banking scheme involving cash conversion and transfers abroad. This professional operation served clients for a fee. Generally, potential proceeds would be sent to the accounts of shell companies on the basis of fictitious trade. Eventually, highly liquid securities would be bought and sold (or simulated) through brokerages with profits sent to the foreign bank accounts of offshore companies. The scheme was complex, vertically integrated, and centrally controlled, involving more than 400 persons and six subgroups with unique functions. The defendants used nominees to buy shares in four Russian banks and all transactions flowed through shell company accounts therein. Billions of roubles went through this probable ML network and the group made over RUB 600 million / EUR

8 million in profits for their services. Numerous searches were conducted and the equivalent of EUR 6.8 million was seized. MLA requests were sent, but the bulk of the cash conversion took place in Russia. Rosfinmonitoring helped identify 123 shell companies and 273 accounts in 22 banks. Three bank licences were withdrawn, and 12 persons have been brought to justice, including Mr. M, who was a banker himself, and complicit brokers. So far, charges have included illegal banking (Art. 172), participation in an OCG (Art. 210), and registering fictitious companies (Art. 173.1). The clients of the system are being investigated to understand the criminal origin of their money, but no ML charges have been brought to date.

237. Illegal banking is being detected with increasing frequency. In 2017, the number of identified crimes doubled following updated guidance sent by the MoI to its territorial offices. To date, 60 criminal cases related to illegal banking were initiated with the use of information from Rosfinmonitoring. In 2016, 12 large-scale illegal banking schemes were disrupted and, in 2017, 22 were disrupted (large-scale here refers to cases involving hundreds of millions to tens of billions of rouble).

Table 3.15. Illegal Banking Cases (CrC Art. 172)

	2013	2014	2015	2016	2017	2018
Investigations	80	52	73	76	96	145
Prosecutions	70	47	66	71	91	133
Individuals Convicted	80	73	119	144	259	356

238. The illegal banking case examples bore the hallmarks of ML activity (e.g. use of multiple shell companies, forged payment documents, hierarchical structure, and fees for money transmitting). This offence may be applied outside of the formal sector, against completely unlicenced conduct, but can also be applied against actors within the financial sector, such as criminals who surreptitiously control FIs. But, as analysed earlier, the commission of this crime would not necessarily involve criminal proceeds. LEAs state that they investigate the underlying criminal predicate activity of the clients of the illegal bank, if possible. Illegal banking does not appear to be used by authorities as an impermissible substitute for ML, but may be helpful when proving the perpetrator's knowledge of proceeds becomes an obstacle to obtaining an ML conviction.

239. The assessment team commends Russia's use of the illegal banking offence to dismantle potential ML networks and infrastructure. At the same time, the team emphasises the primacy of securing ML convictions under IO.7 and the importance of working backwards, if necessary, to uncover the predicate criminality of the "clients" of illegal banks. Some examples of Russian LEAs uncovering the clients and the predicate proceeds funnelled through illegal banking schemes are highlighted in Box 3.15. Defendants are generally sentenced to 2-3 years for illegal banking. This is tough for what is essentially a licensing offence, particularly when compared to ML which does involve transactions conducted for malign purposes with proven criminal proceeds.

Other alternative measures

240. Another relevant alternative offence is CrC Article 193.1, which criminalises the transfer of Russian or foreign currency to the accounts of non-residents through the deliberate filing false of documentation with a bank to justify the transfer. This is used to target "outflow" schemes, such as the Moldovan laundromat (see Table 3.12) and potential trade-based ML. When the complexity of the scheme prevents LEAs from reaching a firm conclusion about the criminal source(s) of the funds or the defendant's knowledge of those source(s), this offence is a sound alternative that does not diminish or substitute for ML. The number of identified offences under Article 193.1 approached 200 in both 2016 and 2017. Authorities should ensure that reliance on this offence is justifiable. For both the illegal banking and outflow offence, there is no technical difference in penalties available as compared to ML; however, the possibility to charge ML should be vetted, as alternative offences may pose unanticipated challenges in international co-operation when dual criminality is required. Neither illegal banking nor the outflow offence necessarily involve criminal proceeds, which is why they are fully credited under core issue 7.5 and only noted in 7.3.

241. Several alternative measures are also employed to combat the misuse of legal persons. CrC Articles 173.1, 173.2, and 170.1 criminalise shell company behaviour. Providing deliberately false information to the USRLE, creating or reorganising a legal entity through nominees, and unlawfully using documents to create or reorganise a legal entity are prohibited. Case studies exemplified that these crimes can be used in conjunction with ML charges, or independently against perpetrators playing minor, non-financial roles that can facilitate larger schemes. These types of offences are still relatively rare among FATF jurisdictions. As less serious crimes, they do not carry penalties quite comparable to ML and, in practice, the sanction will be a monetary fine. In Table 3.16 below, Article 173.2 accounts for 1 334 of the total convictions. The number of persons sanctioned for this offence doubled from 2017 to 2018.

Table 3.16. Sampling of Alternative Criminal Justice Measures

CrC Art. 170.1 – Falsifying Information in the State Register of Legal Entities
CrC Art. 173.1 – Unlawful Establishment of a Legal Entity
CrC Art. 173.2 – Unlawful Use of Documents to Establish a Legal Entity

	2013	2014	2015	2016	2017	2018
Individuals Convicted as a Primary Offence	24	35	41	167	860	1 588
Individuals Convicted as an Additional Offence	11	21	26	29	55	67
Total No. of Individuals Convicted of Shell Company Offences	35	56	67	196	915	1 655

242. In a review of numerous case examples showing the deployment of alternative charges to ML, it was not always evident why the investigation did not

result in ML charges or whether an ML investigation had been initiated, but abandoned for justifiable reasons. The assessors understood that a wide range of offences can be used in Russia to prosecute crimes similar to, or accompanying ML, and encourages authorities to continue to ensure that these offences are not substituted for ML prosecutions.

3

Overall conclusions on IO.7

243. Most of the ML investigations and cases pursued in Russia are relatively simple and low-value. Authorities do not adequately detect, investigate and prosecute third-party ML or stand-alone ML, and the 3PML cases conducted are not especially complex. There is also a weakness in prosecuting financial sector professionals facilitating the laundering of proceeds out of Russia through Russian FIs (as compared to the cases against those who launder embezzled funds from banks they manage, which the assessors deem beneficial). Given Russia's ML risk environment, this, and the lack of cases of ML linked to bribery, represent a misalignment of enforcement resources in some key risk areas. There is also a lack of reliable dissuasiveness in the fairly modest sanctions against natural persons and a lack of administrative penalties against legal persons.

244. Assessors note numerous positive features, such as the good capability of investigators, the use of multiagency task forces to handle complex cases, the tight collaboration between LEAs and Rosfinmonitoring, the upward trend in overall ML cases brought to court, and the use of alternative measures—principally the illegal banking offence—as a tool to disrupt potential ML networks/shadow financial schemes. The assessment team has also carefully weighed items that mitigated shortcomings, for example, the ways 3PML can be combatted through other types of charges; the fact that the number of ML investigations linked to bribery as a form of corruption have recently improved; and that laundromats as a threat have been confronted, even if not through ML convictions to date.

245. Russia is rated as having a moderate level of effectiveness for IO.7.

Immediate Outcome 8 (Confiscation)

Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective

246. Russia pursues confiscation as a policy objective as demonstrated by recent national strategies, plans, and various interagency and intra-agency documents. These products oblige LEAs, prosecutors, and the judiciary to carry out confiscation, although some of them are relatively recent proclamations and detail future, not current, activity.

247. Confiscation is emphasised in the Concept for the Development of the National System to Combat ML and TF, signed by the President on 5 March 2018 (SD1). This overarching strategic document for the entirety of Russia's AML/CFT system defines national risks and objectives. Confiscation has been determined, at the head of state level, to be of the second highest priority in connection with reducing ML, corruption, TF, and PF. The main task for authorities is to improve "the mechanisms for confiscation and other forms of proceeds seizure from persons who have committed crimes, as well as compensation for damage caused by unlawful

acts to the state, organisations, and citizens." SD1, para. 10(b). International co-operation in confiscation and the conclusion of international agreements for the return of proceeds of crime are also declared policy objectives. SD1, para. 11(i). Confiscation is a policy objective in the National Anti-Corruption Plan 2018-2020 (SD378), which proposes the expansion of property of public officials subject to confiscation as unexplained wealth and a review of judicial practice regarding the use of CPC Article 115, a provisional measure. The previous anti-corruption strategy, in place since 2010, did not highlight confiscation as an objective. The Strategy for the National Anti-Drug Policy (2020) has as one of its goals disrupting the economic underpinnings of the drug trade, including by combatting drug ML and preventing TF accomplished with drug proceeds. The Concept of Combatting Terrorism does not specifically address confiscation.

248. The ML NRA Action Plan identifies, as a matter of first priority, a number of items related to confiscation. Although these are plans for the future, not policies in place as of the on-site visit, they reflect a stated commitment to improving the domestic confiscation regime. In particular, GPO and LEAs are directed to prepare a draft law addressing the confiscation of the proceeds of certain predicate offenses (see TC Annex, c.4.1). Additionally, MoI is instructed to consider the possibility of asset seizure at the pre-investigation stage in order to ensure successful confiscation. All agencies are to enhance statistics-keeping mechanisms related to ML and confiscation efforts.

249. Several documents provide more detailed guidance on conducting confiscation and using provisional measures. According to Supreme Court (SC) Order No. 32 (2015), all courts must resolve issues on the confiscation of property with respect to persons convicted of ML. The same is true for crimes of terrorism, including TF, by virtue of SC Order No. 1 (2012). SC Order No. 17 (2018) clarifies processes for confiscation in criminal cases and advises on the correct and consistent application of confiscation law and procedure. Other orders outline interagency co-ordination for the purpose of confiscation, such as Joint Order RFM No. 105 (2016). This requires LEAs to identify property subject to confiscation and to apply early and often to courts for provisional measures available under CPC Article 115. It also encourages LEAs to seek legal assistance under CPC Chapter 53 when assets are located abroad. Finally, GPO has issued a number of relevant documents, such as GPO Order No. 87 (2017), which requires that the most skilled and qualified prosecutors supervise criminal cases related to ML and TF and that, when justified, they recommend to the court the penalty of confiscation. This Order further states as a policy objective that illegally obtained funds and proceeds should be withdrawn from the economy through confiscation. Under CrC Article 61, rendering active assistance in the investigation of crime, exposing accomplices for prosecution, and aiding in the search for criminal proceeds are considered mitigating circumstances at sentencing, and voluntary compensation of financial damages caused by crime are can also result in leniency.

250. In addition to written policies, the heads of LEAs consider confiscation-related issues at yearly meetings and other interagency fora. For example, as a result of a meeting in 2014 between Rosfinmonitoring and the IC emphasising the importance of collaboration to trace assets that may be subject to seizure, confiscation, or restitution to victims, there was a demonstrable increase in requests sent by the IC to Rosfinmonitoring. This increase has been sustained (IC requests for

financial intelligence have nearly doubled to 2 600 in both 2016 and 2017). Russia has established an interagency working group on foreign asset recovery related to corruption and, inter alia, an ad hoc office for the purpose of recovering stolen funds from the Bank for Development and Foreign Economic Affairs.

251. Federal Law 144-FZ on Criminal Intelligence and Surveillance Operations (1995) provides that one of the four objectives of operational agents is identifying property subject to confiscation (Art. 2). This law permits measures at the criminal intelligence phase that enable the identification, tracing, and evaluation of assets, such as examination of items and documents, interrogation, making inquiries, and the examination of premises and means of transportation (Art. 6). To identify assets that may be subject to provisional measures and confiscation, LEAs use the whole range of criminal intelligence techniques available in Federal Law 144-FZ, as well as the powers granted in the CPC.[39] LEAs cited Rosfinmonitoring as a trusted source to identify and help trace criminal assets. Rosfinmonitoring has a wealth of information, accessible to it directly and upon request, that proves useful in locating criminal assets. This includes: the registry of bank accounts (FTS); registration and ownership of vehicles (MoI); the unified registry of real property (Russian State Register); tax liabilities (FTS); insurance information (Pension Fund, Social Insurance Fund); import/export revenue and customs declarations (FCS); cross-border cash/BNI declarations (FCS); notarised deals (Notary Chamber); USRLE (FTS); court records (Supreme Court Judicial Dept.); commercial databases; and open source websites such as marinetraffic.com.

252. Aside from LEAs and GPO, the Federal Bailiffs and FASPM contribute to the accomplishment of confiscation as a policy goal. Bailiffs execute court orders pertaining to confiscation, fines, and restitution. They forcibly implement monetary orders by tracking down defendants' property and effectuating seizure. LEAs manage and evaluate most assets seized in their own cases; upon confiscation, the FASPM takes possession, appraises, and auctions the property with the assistance of approved contractors. Complex assets and those requiring active management are dealt with efficiently, as when a defendant's confiscated factory equipment was sold to pay back-salaries of 510 employees in 2017-2018. Confiscated funds and the proceeds of liquidated tangible assets are transferred to the federal budget; tangible assets are not repurposed for LEA use. The MoF receives confiscated cash and funds from confiscated property that has been sold. The Gokhran receives precious metals, stones, jewellery, and bar.

[39] As discussed in IO.7, there are two phases of criminal investigation. The activities of criminal intelligence agents differ from those of investigators. There is continuity between the phases and both field operatives and investigators identify and trace assets. During criminal intelligence, authorities seize property as evidence or because it is the subject of the offence—e.g., a cash bribe—and take it into custody (mostly instrumentalities). During the public investigation, the investigator will formally seize those assets via court order, as well as additional property, using the CPC (mostly proceeds). Authorities confirmed and assessors verified through case examples that equivalent value is routinely seized.

Box 3.16. Asset Management

LEAs and Rosfinmonitoring investigated the executives of a group of companies, known as the S Group, whose business was residential real estate development. The executives were investigated for fraud (Art. 159), tax evasion (Art. 199), and non-payment of wages (Art. 145.1). During the course of the investigation, authorities seized the executives' shares in S Group, meaning that the State had to operate the significant, ongoing business activities of S Group. The shares were transferred to a state-owned bank, which established a special-purpose LLC to manage and rehabilitate the S Group. Loans from the bank provided financing, which were paid back with profits of S Group's business activities.

Confiscation of proceeds from foreign and domestic predicates, and proceeds located abroad

253. Competent authorities are achieving good results using various asset recovery mechanisms domestically and are intensifying nascent efforts to recover proceeds and instrumentalities abroad. Seizure, confiscation, and restitution trends have held steady or increased in recent years. Russian authorities, per legal mandates including CPC Article 6, focus on compensating victims of crime. Therefore, restitution figures are higher than criminal confiscation figures. Competent authorities do not confiscate assets to the State in order to distribute funds to victims at a later point—compensation is done upfront. The assessors find the balance between confiscation and restitution to be appropriate in the Russian context, where many crimes falling into the high-risk areas of budget spending and taxes (public funds) and the financial sector have identifiable victims, such as the State, citizens, or legal entities. Significant volumes of proceeds from crimes such as fraud, embezzlement, and misappropriation are often recovered through methods other than confiscation. Crimes in the risk-areas of budget spending and financial sector make up the majority of restitution amounts (namely, theft, fraud, misappropriation, tax crimes, and embezzlement). Thus, restitution is the priority in the Russian system and criminal confiscation is used when legal owners cannot be identified, or in the case of offences that create proceeds, but do not result in financial losses.

254. As noted in the TC Annex under Recommendation 4, Russia's legislation on confiscation, currently split between two Codes, has potential downsides in its complexity. Although Russian authorities view these arrangements as complementary and prioritising victims' claims, there is no corresponding reason for the main criminal confiscation authority to list some but not all predicate offences. Russian authorities have set out in their ML NRA Action Plan to fully expand confiscation under the CrC to include all offences, which should streamline law and practice. The assessment team does not view this TC issue as having a major impact on effectiveness, but it would be more efficient to have a consolidated confiscation regime.

255. Overall, between 2014 and 2018, criminals in Russia were deprived of RUB 318 437 127 000 or EUR 4 942 341 457 (EUR 988 million per year, on average) through the application of all legal mechanisms of confiscation, restitution, and civil claims.[40] These figures do not include fines.

Table 3.17. Total Deprivation of Criminal Proceeds & Instrumentalities – All Mechanisms

	2014	2015	2016	2017	2018
RUB	39,321,524,000	55,700,583,000	61,462,335,000	71,227,489,000	90,725,196,000
EUR	799,799,789	890,095,316	800,239,602	1,180,239,493	1,217,967,248

256. Approximately RUB 262 billion, or EUR 4 billion, has been restituted to victims of crime in the five-year timeframe captured below. On average, approximately RUB 52 billion, or EUR 816 million, is restituted on an annual basis.

Table 3.18. Voluntary Restitution of Criminal Assets to Victims

	2014	2015	2016	2017	2018
Amounts Recovered During Investigations (RUB)	26,189,232,000	34,647,600,000	43,113,581,000	44,349,289,000	63,484,719,000
EUR	532,688,979	553,668,648	561,338,825	734,867,719	890,055,760
Amounts Recovered in Court Proceedings (RUB)	9,015,909,000	11,587,808,000	8,474,222,000	10,145,157,000	11,506,038,000
EUR	183,383,589	185,173,172	110,334,370	168,105,250	161,314,653

257. Criminal confiscation amounts are relatively modest when compared to restitution. Approximately RUB 16 billion, or EUR 249 million, has been criminally confiscated in the five-year snapshot below. On average, approximately RUB 3.2 billion or EUR 50 million is confiscated on an annual basis. These sums encompass results achieved using all criminal confiscation provisions, including CrC Article 104.1, the main criminal confiscation law; CPC Article 81, which is the provision used for certain predicate offences instead of Article 104.1; and CrC Article 104.2, for equivalent value (statistics for which could not be counted separately).

40 The rouble to euro exchange rate varied significantly during the assessment period. Thus, for the purpose of IO.8, the MER used the official exchange rate from the European Central Bank as at the end of March (i.e. the end of the on-site visit) for each individual year between 2013 and 2018. All multi-year totals and averages also draw on these conversions. This more precisely represents the IO.8 picture in Russia than if one singular exchange rate, or one average exchange rate, had been applied to the entire assessment period.

Table 3.19. Value of All Assets Confiscated on a Conviction Basis

	2014	2015	2016	2017	2018
RUB	1,818,760,000	3,879,517,000	2,943,823,000	3,513,439,000	3,833,847,000
EUR	36,993,578	61,994,682	38,328,575	58,217,684	53,750,535

258. Another common mechanism of asset recovery used in the Russian system is the civil claimant process under CPC Article 44. Civil claims may be lodged by individuals or public entities when the crime has caused financial damage to the State or a citizen. LEAs inform the governmental authority that suffered the loss to file a civil claim. If the claim is not filed within ten days, the prosecutor does so directly. This process is tied to the criminal case—claims may be filed after the initiation of the criminal proceeding and up until the end of trial. When rendering the verdict and sentence, the judge also rules on which claims should be satisfied. For instance, in the first half of 2018, 2 242 claims were made by prosecutors to recover losses inflicted upon the State in the amount of approximately RUB 7.8 billion, or EUR 105 206 000.

Table 3.20. Damages Recovered through Prosecutors' or Victims' Civil Claims
(Within Criminal Cases)

Total in Years 2013-2018	RUB 41.7 billion or EUR 657 million
Annual Average, Years 2016-2018	RUB 10.7 billion or EUR 159 million

259. Russia has criminally confiscated RUB 2.2 billion or EUR 32 431 506 in laundered funds from 110 individuals convicted of ML over a six-year period. The assessors consider this to be low, but not necessarily problematic when evaluated in light of the fact that most ML in Russia is not prosecuted on a stand-alone basis and other methods of recovery may be used depending on the nature of the also-charged predicate (e.g. restitution when the underlying offence caused pecuniary loss).

260. A strength of the confiscation regime is the recent use of unexplained wealth orders concerning public officials whose expenditures exceed income. If a public official (or his or her spouse or minor child), spends a sum greater than the official's declared income over the most recent three years, GPO can file a motion that forces the official to justify such expenditures or face forfeiture.[41] This power, contained in Federal Law 230-FZ, is being used by GPO with increasing frequency and authorities stated that more significant discrepancies are being targeted. The list of public officials against whom this power can be employed appears extensive, reaching to federal legislators, managers of State-owned companies, and federal, regional, and municipal officials, members of the judiciary, and heads of agencies. Currently, there are limited types of assets that can be forfeited, including real estate, vehicles or vessels, and securities, but other assets such as cash, jewellery, or assets held in foreign trusts, are not covered. Separately, foreign bank accounts must be declared by officials, and high-level officials are technically prohibited from

41 If criminal or administrative offences are detected in the course of examining unjustified assets, an investigation and/or prosecution can be initiated. Dismissal from service is a consequence for the official's failure to provide information showing a legal source of funds.

holding foreign accounts or financial instruments. Another positive outcome is that from 2016 through the first half of 2018, nearly RUB 16 billion or EUR 213 659 000 was voluntarily restituted by individuals accused of corruption.

Table 3.21. Non-Conviction Based Confiscation (Unexplained Wealth of Public Officials)

	2012-2014	2016	2017
No. of Motions Filed	40	29	35
No. of Motions Satisfied by the Court	20	15	26
Total Amounts Confiscated	EUR 27.2 m	EUR 25.8 m	EUR 133.7 m

Box 3.17. Confiscation of Unexplained Wealth from Officials and Third Parties

- GPO sought to confiscate assets, which had already been subject to provisional measures, belonging to official Z and third parties. The Court granted the motion in December 2017, ordering the confiscation of twelve apartments, two Porsches, two Mercedes, various currencies, and a gold bar. The real property and vehicles were transferred to the FASPM for sale, and the cash and bullion were kept by the MoF and Gokhran, respectively.
- Property registered in the name of a public official's spouse and daughter, as well as the spouse's relatives and the family's driver, was confiscated for being largely undeclared and significantly exceeding the official's income. During the course of an IC investigation into the official for bribery, assets including apartments, shares in commercial property holdings, cars, trailers, a snowmobile, sporting guns, watches, and currency were identified. The court satisfied GPO's motion in full against assets held by third parties totalling RUB 140 million or approximately EUR 1.9 million

261. Authorities are pursuing provisional measures against a variety of assets—including funds, residential and commercial real estate, securities, vehicles, and luxury goods—to secure them for criminal confiscation, restitution, civil claims, or the collection of fines. Property of equivalent value can be seized to increase the odds of confiscation, and, as demonstrated through case examples, LEAs seize corresponding value frequently, especially in bribery cases where proceeds are quickly spent. Upon the motion of an investigator pursuant to CPC Articles 115, 115.1, or 116, property can be arrested during the public phase of a criminal investigation. Between 2013 and 2017, courts granted, on average, 30 949 motions per year, and denied 2 526 motions per year, for the restraint or seizure of assets in all criminal cases, with an uptick in restraints sought every year. Judges rule on applications for provisional measures within 24 hours. In urgent circumstances, investigators may arrest the property and approach the court within three days to

seek ratification of the action, a feature that helps close the gap between assets identified and ultimately recovered. There is a good correlation between amounts subject to provisional measures (a little over EUR 1 billion per year on average) and amounts subject to final deprivation pursuant to all modes of recovery (around EUR 988 million per year on average).

262. The arrest of a suspect's property by the court is based on the investigator's articulation of specific facts; the arrest of property belonging to anyone other than the suspect or the accused must be based on sufficient grounds to believe the property is proceeds or instrumentalities of crime (including property intended for use in terrorism/TF). A reasonably small ratio of applications for asset seizure are denied by the courts, demonstrating that LEAs are able to meet these legal standards in practice. The length of the arrest or conditions on use and disposal of assets held by third parties is at the discretion of the court. A pragmatic approach is taken: for example, both the MoI and FSB noted instances where prohibitions on title transfer were used instead of seizure as a provisional measure, such as when a property is a family's sole residence. The IC explained that courts would order seizure in lieu of restraint if the bank holding the targeted accounts was, for instance, under investigation.

263. In practice, the seizures described above cover mostly proceeds, e.g. funds in bank accounts, real property, and financial products. The average annual value of criminal assets seized is approximately RUB 71.6 billion or EUR 1.1 billion. However, assets can also be seized in the pre-investigation phase. Such seizures are conducted under CPC Article 81 and cover mostly instrumentalities or evidence taken into custody, e.g. cash seized from suspects, such as drug payments or bribes changing hands. The average annual value of instrumentalities and material evidence seized is approximately RUB 18.5 billion or EUR 294 million. The formal seizure of these assets, with court authorisation, occurs later (except if the property is held as evidence) and amounts seized during both phases are subsequently included in final judgments.

Table 3.22. Use of Provisional Measures

	2014	2015	2016	2017	2018
Criminal Assets Seized (Proceeds) CPC Art. 115	40,957,040,000	60,905,934,000	83,820,694,000	77,481,261,000	94,859,064,000
EUR	833 million	973 million	1.09 billion	1.28 billion	1.33 billion
Criminal Assets Seized (Instruments or Evidence) CPC Art. 81	16,522,411,000	25,404,612,000	17,570,364,000	13,475,510,000	19,685,701,000
EUR	336 million	406 million	229 million	223 million	276 million

264. These sums are impressive. However, the portion of assets seized in all criminal cases that relates specifically to investigations into the core ML offences is less than 1.5% of the total amount (note, however, that Russia does not generally pursue ML as an autonomous crime and so the seizures may be connected with the predicate offence). Additionally, the average amount of assets seized in third-party ML cases has not exceeded EUR 500 000 in any recent year. Authorities should make

certain to pursue restraint and seizure in the approximately 3 135 ML investigations conducted annually, whenever possible. There are approximately 665 655 investigated predicate offences in Russia per year falling into FATF's designated categories. If nearly 30 000 motions for seizure are filed per year, assuming, arguendo, they are filed on a one-per-investigation basis, then asset seizure is sought approximately 4.5% of the time in predicate investigations. It is easier to determine from statistics *how much* a country is seizing than it is to reach a conclusion on *how often* a country is seizing and in how many cases—such data was unavailable. Often, there are no assets to seize and, in Russia, not all seizures of instrumentalities require a court motion, at least not initially or when assets are held as evidence until resolution of the case. The assessors also recognize that the values provisionally seized in Russia are substantial. The number of motions for seizure has gone up incrementally every year, and the number of investigated predicates has gone down. Thus, Russia may be on a positive trajectory of seeking more seizures even in fewer predicate cases, but LEAs must explore the possibility of seizure during financial investigations in all appropriate cases, especially when ML is suspected.

Box 3.18. Illegal Banking Seizure in Krasnodar

The IC in the Krasnodar region conducted an investigation into an illegal banking operation. The defendant organised a group of five accomplices to register shell companies, accept cash from clients, and wire the money at their direction using false documents to justify the transfers. In two years, the group accumulated proceeds of RUB 66 million, or almost EUR 900 000. The main defendant and two accomplices were arrested and charged with illegal banking (Art. 172) and self-laundering (Art. 174.1). The equivalent of EUR 613 000 was seized during the investigation.

265. In the scope of all investigated criminal cases from 2014 through 2018, Russian authorities estimate the damages and losses inflicted exceed RUB 216 billion or EUR 3.3 billion per year. This obviously does not include latent criminality or indirect proceeds and may not capture proceeds that are not "damage" to a particular person. Even so, if RUB 64 billion or EUR 988 million per year is recovered annually through all mechanisms, then LEA actions are having a sizeable impact in depriving criminals of the fruits of their offences kept onshore.

266. However, the ML NRA concludes that in recent years, large amounts of funds, presumably of both licit and illicit origin, were moved offshore using non-resident legal persons and structures established abroad. The NRA notes that of the years studied, the high-water mark for money moved offshore, in 2011, was RUB 369 billion, or approximately EUR 8.83 billion. In 2013—the first year within this assessment period—the figure was estimated to be RUB 300 billion or EUR 6.66 billion.[42] The assessment team had the opportunity to meet the Chairman of the

[42] There are a diversity of views on the topic of Russian money moved offshore and estimates from different experts vary widely. The assessors have focused on the NRA and the

Russian Duma's Committee on Budget and Taxation. He estimated that in 2013, capital flight cost the Russian treasury USD 22 billion in lost tax revenue. Recently, reportedly as a result of measures taken by the Russian authorities, capital flight from Russia reduced significantly in 2015-2017 and the amount of assets moved offshore dropped by more than ten times (RUB 32 billion) by 2017. Still, feedback on risk from the FATF global network stated that criminal proceeds generated in Russia were often moved to, concealed in, or spent in regional and global financial centres. Enclaves of Russian-controlled wealth, especially in the form of real property, exist in London, New York, Miami, and Spain, among other places, some of which is thought to be of questionable origin.[43]

267. While there are some instances of the pursuit of assets moved abroad, including in large cases involving multiple countries discussed in depth during the on-site visit, this is an area where Russia should conduct and seek significantly more asset recovery.

Box 3.19. Pursuit of Assets Abroad

B was an associate of a public official who assisted in laundering the proceeds of various corruption offences. The criminal activity involved the assignment of creditor rights, embezzlement of state property, and undervaluation of state assets sold to private parties. Shell companies and fictitious deals were used to expatriate proceeds of more than EUR 190 million. The IC investigated the case and Rosfinmonitoring identified foreign financial connections – requests were sent to France, the U.S., Cyprus, and Switzerland. The suspects maintained a warehouse with more than 1 000 works of art in St. Petersburg as well as land plots, two apartments, and two vehicles belonging to the PEP in Moscow which were all seized. The PEP has been extradited, but B is still a fugitive. B was sentenced in absentia to 10 years in prison for misappropriation (Art. 160) and self-laundering (Art. 174.1) and assets controlled by her, including hotels in France valued at EUR 120 million and real estate and vehicles valued at CHF 10 million, were ordered confiscated. Multiple assets have been seized in Switzerland to date and additional requests are pending.

Chairman's statement, but note that, as additional background, some economists estimate that in the last 25 years, as much as USD 750 billion in Russian assets have moved offshore. See *Capital Flight from Russia Carries $750 Billion Price Tag*, Bloomberg Economics, 19 March 2019, www.bloomberg.com/news/articles/2019-03-12/capital-flight-from-russia-carries-750-billion-price-tag-chart. The Moscow Times put 2014's capital flight figure at USD 154.1 billion. See *Russia: Massive Capital Flight Continues*, 1 May 2015, www.themoscowtimes.com/2015/05/01/russia-massive-capital-flight-continues-a46263.

43 Considering the example of London, a Deutsche Bank report from 2015 posits that nearly £133 billion of hidden capital inflows from Russia have entered the UK since the mid-1990s. See https://assets.documentcloud.org/documents/3036316/Special-Report-9-Mar-2015-2.pdf.

Russia began instigating a large hashish trafficking case. This transnational OCG was composed of nationals from Russia, Spain, Belarus, and Moldova who delivered and sold drugs from North Africa, through the Mediterranean, and into CIS countries. The OCG conducted laundering operations out of Moldova, with proceeds exceeding EUR 1 million. On the basis of evidence from Russia, assets in Moldova have been seized and persons arrested. Russian LEAs identified real property in Spain that is currently sought for seizure in the context of a joint investigative team formed between Russian LEAs and Spain's Guardia Civil. Fifty people were arrested in Russia; some have been sentenced under Art. 210 (establishing/participating in OCG).

In 2010, a Russian court convicted and sentenced to life in prison a former member of the Federation Council on charges of management of an armed gang, organising two murders, organising a terrorist act, bribery, and other offences. Following on a Swiss ML investigation into the former official, Russia sent a request to Switzerland to seize funds, which was executed in 2014. CHF 200 000 were shared with the Russian Federal Bailiff's Service.

268. Requests sent to other countries for confiscation-related assistance have clearly increased starting from 2016. For example, the IC, which focuses in part on combatting corruption, reported seizures of assets outside of Russia between 2014 and 2016—including a yacht, funds, residential and commercial real estate, vehicles, and art—located in four different countries and valued at RUB 368 million or EUR 5.45 million. However, in the context of Russia, more productivity was expected in this area. There were simply not enough requests demonstrating the pursuit of proceeds moved to other countries in light of the amounts of suspicious offshorisation, especially in the earlier years reviewed. The CPC requires LEAs to send such requests for tracing and seizure when warranted, so the assessors have concerns about the breadth of investigations involving international components earlier in the assessment period, but the situation appears to be improving in recent years. There were case studies involving asset sharing, but no specific statistics were provided. Also, as discussed in IO.7, Russia occasionally tries and convicts defendants charged with ML and other financial crimes in absentia. This practice can hinder Russia's attempts to have confiscation judgments recognised abroad. In most countries, foreign confiscation orders must be final to be enforced and they cannot be truly final and non-appealable if there is a possibility of re-trial in Russia of a (former) fugitive.

Table 3.23. Outgoing MLA Requests Seeking Seizure of Assets in ML and Predicate Cases

(GPO and MoI, plus IC and FSB as of 2017)

2013	2014	2015	2016	2017	2018
Requests Sent					
2	5	1	12	31	17
Requests Executed					
0	0	1	2	15	11
Requests Pending					
7	9	6	14	29	32

269. While not especially common in light of Russia's status a source and occasional transit point for criminal proceeds rather than a destination, case examples concerning Uzbekistan and Brazil showed that Russian LEAs will seize assets in the course of ML investigations concerning foreign predicates.

270. In terms of tax recoveries, charges are dismissed against individuals accused of tax crimes if it is a first offence and the person voluntarily restitutes the damage, fines, and penalties before the court's verdict. Case examples regarding restitution of taxes evaded were reviewed, but the tax system is not generally used to recover criminal proceeds/instrumentalities.

Confiscation of falsely or undeclared cross-border movements of currency/BNI

271. Confiscation of falsely or non-declared cross-border movements of currency/BNI is pursued to a lesser extent, mainly due to the lack of declaration system in place at Russia's borders with Eurasian Economic Union (EAEU) countries. There are also contextual factors that influence this conclusion, such as the number and size of Russia's land borders with other jurisdictions and the prevalence of cash in the domestic economy. The use of cash in ML schemes is identified as high-risk in the NRA and the assessors concur that this is generally an internal risk, mostly relating to the common ML method of "cashing out" from bank accounts. However, once withdrawn, proceeds in the form of currency can be difficult to track and contain, and some of it may be crossing the border particularly in connection with goods trafficking conducted by organised, transnational groups. Conversely, Russian authorities rated the smuggling of cash and BNI as a moderate threat crime and ranked the cross-border transportation of currency and BNI for ML purposes as posing a moderate level of risk that is estimated to be decreasing. The assessment team agrees with this risk understanding, but the sheer volume of currency moved across Russian borders remains high (the equivalent of USD 1 billion was brought in during 2017 and USD 2.4 billion was brought out). China, Turkey, and UAE are deemed the riskiest countries for the illegal movement of cash into and out of Russia. Considering these factors, a relatively low percentage of illegally smuggled cash that is identified is confiscated and the amount of unidentified cash that moves across intra-EAEU lines is unknown. However, the modest cash seizure figures are partially offset by additional fines imposed as a sanction for smuggling.

272. Smuggling of cash or monetary instruments is a criminal offence under CrC Article 200.1. The law establishes criminal liability for the illegal movement of cash or monetary instruments across the customs border of the EAEU committed on a large scale (more than USD 20 000). The offence is punishable with a fine of three-times to ten-times the value smuggled, a fine in the amount of the defendant's income for a period of up to two years, or restriction of freedom or compulsory labour for up to two years. The sanctions increase in gravity if the offence is committed on an especially large scale (USD 50 000). Money, valuables, and other property that are the subject of this offence can be confiscated under CrC Article 104.1.

273. Lower level currency smuggling is an administrative infraction under CAO Article 16.4. This provision sanctions the failure to declare or false declaring of cash or monetary instruments by natural persons and applies to cash/BNI moved illegally across EAEU borders in amounts between USD 10 001 and USD 20 000. The penalty is a fine in the amount of under-declared cash or one-half to two-fold the amount of cash not declared, and/or the confiscation of the cash or monetary instruments pursuant to CAO Article 27.10.

274. Russia's cross-border currency and BNI declaration regime is only applicable at the outer borders of the EAEU, composed of Russia, Belarus, Armenia, Kazakhstan, and Kyrgyzstan. As a state party, Russia implements the EAEU Customs Code (EAEU CC). The movement of currency or BNI at land crossings or airports (for inter-EAEU flights) within the area covered by these countries is not considered to be cross-border. It is noteworthy that the land border between Russia and Kazakhstan is the second longest in the world, and there is no declaration system in place there. During on-site interviews, LEAs confirmed that there are no customs controls within the EAEU, so cash moves freely and largely without detection. When currency or BNI is moved over Russia's borders, it must be declared only when brought to or from the following countries (listed in order of length of land border with Russia): China, Mongolia, Ukraine, Finland, Georgia, Azerbaijan, Estonia, Latvia, Lithuania, Poland, Norway, and DPRK. Since no declarations are required within the EAEU, neither the crime nor administrative offence applies.

275. Within Russia and abutting its EAEU land borders, FCS may stop and inspect any motor vehicle, including those not engaged in the international transportation of goods, in order to verify compliance with customs law and regulation. Goods, currency, other similar instruments, and documents relating to the goods can be examined. Such a stop may take place in the border control zones, as well as in the territories next to Belarus and Kazakhstan (the only members of EAEU which share land borders with Russia). Use of this legal power under Federal Law 289-FZ could lead to the discovery of items such as contraband or counterfeit goods, illegal drugs, or cash suspected to be linked to ML, TF, or predicate offences. However, there would be no seizure without indicia of crime and there could be no currency smuggling violation (since there is no legal requirement to report the movement of currency except at a border that Russia deems to be international). Similar powers exist for stopping and inspecting watercraft and aircraft. Russian authorities state that even across EAEU borders, the flow of suspicious and criminal funds can be detected. However, no statistics were available to substantiate this.

276. At all external borders and airports, the FSB's Border Service can receive information from customs authorities on possible cross-border movement of suspicious cash and can take measures within its power and authority as a LEA to prevent its movement. Additionally, transport police are present in every Russian airport. At all airports, authorities scan checked luggage and use trained dogs to detect undeclared cash. Transport police officers can receive information from customs authorities and take action to detect and disrupt the movement of criminal cash and monetary instruments. There were no statistics on airport cash seized or confiscated, but case examples are mentioned in Box 3.21 below.

277. FCS has around 55 000 employees, including central staff in Moscow, regional units in federal districts, and officers at all border crossings. FCS implements measures for countering ML and TF when exerting control over currency, securities, currency valuables, or traveller's checks transported over the customs border of the EAEU. Under the EAEU CC, the FCS conducts inspections, examinations, checks of customs and other documents, interviews, and other actions necessary for enforcement. Risk mitigation systems and selection criteria (profiling) are employed. LEAs, including FCS, can suspend the movement of cash or BNI when a false declaration has been made (i.e., when inaccurate information provided in the declaration is discovered). If there is a suspicion that cash may be linked to ML, TF, or predicate offences, FCS sends the relevant information to Rosfinmonitoring, in paper copy, through the State Courier Service, which is not considered efficient by the assessors. FCS may detect currency and BNI smuggling independently, as a result of the above investigative actions and the FCS risk-management system, or on the basis of information provided by other LEAs or Rosfinmonitoring.

278. If an offence under CrC Article 200.1 is identified, FCS attempts to trace and confirm the licit or illicit source of the smuggled cash or BNI. All smuggling suspects are cross-checked through MoI's Main Informational Analytical Centre database to see if they have a criminal history. Relevant information is also requested from Rosfinmonitoring. Illicitly moved cash and BNIs are taken into custody after the examination of the crime scene. Detection of smuggled cash triggers the following process:

Box 3.20. Federal Customs Service Response to Detection of Smuggled Cash

- The FCS detecting official documents the elements of the offence and enters a potential violation in the customs registry.
- FCS operational agents (distinct from the detecting officials), conduct pre-investigative checks to determine, within three days, whether a crime has been committed.
- Seizures are carried out and a cash/BNI seizure protocol (i.e., a detailed report of the investigation) is completed.

- FCS determines whether to open a criminal case under CrC Article 200.1, decline to open a case, or refer the case to another LEA.
- If the amount of illegally moved currency/BNI does not exceed USD 20 000 (the large-scale cash threshold), then the FCS initiates an administrative offence under the CAO and the illegally moved currency or BNI is seized pursuant to CAO Article 27.10 (undeclared/falsely declared amounts between USD 10 001 and USD 20 000).

279. FCS is responsible for investigating violations of part 1 of CrC Article 200.1 (large-scale smuggling) and MoI and the FSB are responsible for investigating offences under part 2 of CrC Article 200.1 (especially large-scale). Potential links between smuggled currency/BNI and other crimes are investigated, as exemplified in the cases below. The FCS database includes up-to-date information on nationally designated terrorists and extremists so that listed individuals crossing borders can be identified and searched for cash/BNI. FCS has also developed and implemented profiles for travellers who may be linked to terrorist and extremist activity. As of 2017, FCS and border control officials have applied a joint co-operation plan at Moscow Domodedovo Airport to exchange information and carry out measures aimed at detecting crime, including currency smuggling. Twenty-five such joint operations have been conducted.

Box 3.21. Cross-border Currency and Instrument Confiscations

- In 2018, an investigation by FCS in the Rostov region led to a cash smuggling conviction (Art. 200.1). The penalty imposed was a fine in the amount of illegally transported cash (RUB 6.8 million or EUR 92 714) and confiscation of USD 40 000 USD and RUB 4 900.
- In 2017, an individual was convicted of smuggling BNI (Art. 200.1). FCS seized a promissory note worth RUB 2.8 million or EUR 31,060 from a passenger at Moscow Sheremetyevo Airport, which was later confiscated.
- In 2017, FCS referred a criminal cash smuggling case to MoI. The offence was found to be minor and was dealt with under the CPC Article 25.1 so the defendant was only fined; however, EUR 41 691 was confiscated.
- In 2016-2017, promissory notes worth RUB 2.8 billion (EUR 38.1 million) were illegally smuggled into Russia from France. Further investigation revealed a scheme involving the production of false documents, including the notes. A fraud investigation was opened as a result of the detection of the notes.

- In 2016, a multistate LEA operation was conducted under the auspices of the World Customs Organisation aimed at combatting arms trafficking and currency smuggling. FCS issued 35 alerts on individuals who declared significant amounts of cash when leaving Russia, leading to the interdiction of EUR 2.2 million and USD 58 900 in Greece and EUR 107 000 in Italy.
- Information from a foreign FIU lead to an investigation of individuals using cash transported from Russia to Estonia to buy large quantities of precious metals for importation back into Russia without declaration. Rosfinmonitoring identified the individuals engaged in currency exchange transactions and coin sales and disseminated information on the suspects to FCS. Seven months later, in 2014, FCS arrested one of the suspects on the border and recovered unpaid customs duties from the confiscation and liquidation of seized coins.
- Goods worth EUR 38.4 million in 161 containers were identified as smuggled from China to Vladivostok without payment of customs duties. Authorities brought several dozen administrative cases and effected seizures; ultimately, goods valued at RUB 3.3 billion, or EUR 44 million, were confiscated by the court. Although this example does not concern cash/BNI, it demonstrates that cargo can be screened.

280. FCS has standing coordination and information exchange agreements with a number of Russian competent authorities.[44] FCS also regularly exchanges information with foreign counterparts aimed at detecting, alerting, and intercepting or arresting persons involved in the illegal cross-border transportation of currency. Such requests and responses are sent via customs information exchange channels, through 21 FCS liaison officers abroad, and the channels of the FCS General Department of Anti-Smuggling. The Regional Communications Centre on Law Enforcement Matters of the World Customs Organisation in the CIS Region (RILO-Moscow) provides a forum for operational co-operation between the CIS countries. Exchanges are conducted via a technical platform known as CEN.comm, which contains information on major interceptions and arrests at the border. Since 2011, 1 216 offences related to currency smuggling have been reported in CEN.comm by CIS members. Target-specific information is exchanged on CEN.comm, but countries are not currently sharing information in bulk, such as all national declarations. Between EAEU members, customs authorities can exchange information upon request.

44 FCS MOUs include: Rosfinmonitoring (2007); MoI (electronic information sharing, 2013); MoI (co-operation, 2014); Federal Bailiffs Service (2015); IC (2012); GPO (2016 with 2017 addition); Judicial Department of the Supreme Court of Russia (responsible for court administration) (2017), and BoR (2016). With the exception of the agreement with Rosfinmonitoring, the rest of these coordination mechanisms have been put in place since Russia's 3rd round FATF on-site visit.

281. The tables below show that the vast majority of offenders are caught smuggling money *out* of Russia, which is consistent with the country's ML risk profile. There are more administrative than criminal violations, demonstrating that most smuggling detected involves smaller amounts of money. The number of administrative offences detected concerning cash smuggled out of Russia peaked in 2013 at slightly more than 5 000 violations, as did the values smuggled. The number of identified administrative offences stayed below 3 000 for a time, but rose in 2018 to exceed 4 000. The average number of large-scale criminal violations is 75 inbound and 59 outbound. Approximately EUR 368 million in smuggled currency was detected over the six-year period between 2013 and 2018. Of that amount, EUR 13.8 million has been confiscated. On average, EUR 61 million in smuggled cash is identified and EUR 2.3 million is confiscated every year. Overall, roughly 3.8% of undeclared or falsely declared cash/BNI that is found by Russian authorities is confiscated.[45]

Table 3.24. Small-Scale Currency/BNI Smuggling Violations & Confiscations

	2013	2014	2015	2016	2017	2018
CAO Offences, Outbound Cash/BNI	5008	3127	2151	1675	2990	4226
CAO Offences, Inbound Cash/BNI	528	837	1188	1107	1713	2326
Value of Illegally Moved Cash/BNI (RUB)	10,524,578,500	1,306,025,300	1,277,902,700	1,038,440,200	539,199,400	786,279,070
EUR	264,693,149	26,564,555	20,420,885	13,520,491	8,934,534	11,023,633
Value Confiscated (RUB)	84,225,000	186,042,000	131,343,000	69,091,000	24,425,000	17,658,000
EUR	2,118,259	3,784,094	2,098,861	899,565	404,722	247,565

[45] The percentage of values confiscated to values detected is higher for the large-scale criminal offences than for the small-scale administrative offences. Within those sets, there were significant changes year-to-year, from less than 1% to over 45%, and there were no discernable trends. This suggests to assessors that individual cases may have a large impact and also that targeted risk- or intelligence-driven FCS and LEA operations could make a significant dent in cash detected and confiscated.

Table 3.25. Large-Scale Currency/BNI Smuggling Violations & Confiscations

	2013	2014	2015	2016	2017	2018
Criminal Offences, Outbound Cash/BNI	53	92	51	38	68	52
Criminal Offences, Inbound Cash/BNI	89	80	80	60	59	81
Value of Illegally Moved Cash/BNI (RUB)	271,327,700	225,846,700	204,351,760	226,197,000	143,162,900	224,831,000
EUR	6,823,892	4,593,722	3,265,541	2,945,085	2,372,209	3,152,131
Value Confiscated (RUB)	1,385,000	53,284,000	36,315,000	47,211,000	65,568,000	63,373,000
EUR	34,833	1,083,797	580,314	614,687	1,086,462	888,489

282. Confiscation of only 3.8% of illegal, cross-border currency or BNI does not appear on its face to be an especially effective, proportionate, and dissuasive sanction. However, both the CrC and CAO permit fines to be imposed against offenders in addition to confiscation. The assessment team's view of effectiveness is slightly improved by considering fines alongside the confiscation numbers. Whether categorised as a fine or a confiscation, offenders are deprived of more cash than is apparent on first impression.

Table 3.26. Fines Imposed for Administrative and Criminal Currency/BNI Smuggling Violations

	2013	2014	2015	2016	2017	2018
Fines Under CAO Art. 164 (RUB)	59,202,459	185,759,470	182,952,431	161,414,830	198,128,501	309,006,534
EUR	1,488,942	3,778,348	2,923,580	2,101,621	3,282,989	4,332,272
Fines Under CrC Art. 200.1 (RUB)	9,303,814	4,661,365	9,120,644	11,593,697	28,529,446	51,984,000
EUR	233,991	94,812	145,748	150,950	472,733	728,816
Total Fines In EUR	1,722,933	3,873,160	3,069,328	2,252,571	3,755,722	5,061,087

283. Between 2013 and 2018, the total amount of imposed fines was EUR 19.7 million, including EUR 17.9 million for lower-level smuggling and EUR 1.8 million for criminal currency smuggling offences. The average annual amount of fines is EUR 3.29 million. Recalling that EUR 2.3 million in cross-border

cash is confiscated on a yearly basis, the fines actually outpace the confiscations significantly.

284. With fines factored in, Russia is taking away approximately EUR 5.5 million from individuals illegally moving cash and BNI across borders each year. Even though fines partly offset the lower confiscation figures, the sanctions for smuggling currency or bearer negotiable instruments are only somewhat effective. Furthermore, there is no significant confiscation of potential criminal proceeds at Russia's international borders within the EAEU, as described above, owing to the lack of declaration system in place.

Consistency of confiscation results with ML/TF risks and national AML/CFT policies and priorities

285. Russian authorities were able to breakdown useful statistics regarding criminal assets seized related to the areas of highest risk as identified in the NRAs, including budget spending and taxes (public funds), corruption, the financial sector, drug trafficking, and TF, as described below. Restitution statistics were available by risk area—which is illustrative in the Russian context—as well as dozens of case examples. Generally speaking, over a five year period, final confiscation amounts related to financial sector crimes and corruption were higher than those related to budget spending/tax crimes and drug crimes. Confiscation results, broadly defined, align with identified ML/TF risks and AML/CFT priorities, with some variations between and within the risk areas.

286. According to LEAs, misuse of virtual assets is an emerging risk especially in drug settlements and laundering, cyber-crime, and the theft of VA. There is currently no legal authority to seize or confiscate virtual assets, but there have been ML cases involving them. The stopgap approach of the authorities is to trace the virtual assets and seize them when they are exchanged into fiat currency. In one instance, authorities seized the instrumentalities of an unlicenced VA and e-money exchange network, including 151 bank cards and dozens of electronic devices including computers and data storage devices. Authorities are seizing hardware and access codes or keys, which may not be effective if criminals or their associates can still gain remote access to digital wallets. Legislative change is necessary to recognize VA as property so that it can be confiscated and so an asset management and liquidation infrastructure can be established.

287. Seizure numbers for drug trafficking are low and seemingly decreasing, and these facts are not mitigated by examining restitution or civil claims, as in other high-risk areas. Drug-related offences constituted around 40% of all ML predicates between 2014 and 2018, and the most, by far, out of any category of predicate giving rise to self-laundering and third-party laundering offences. With seizure amounts in drug trafficking cases averaging EUR 7.1 million annually, and confiscation amounts falling and not corresponding well to seizures, the assessors are persuaded that not enough has been done to confiscate drug money.

288. LEAs explained and assessors accept, to some degree, that opportunities for the seizure and confiscation of large values of drug proceeds are rare because MoI is interdicting wholesale drug shipments before they are sold in Russia and payments for such shipments are often made outside of the country. An example of this approach—to detect and seize major drug shipments and therefore reduce the

chances to generate proceeds in Russia—is recounted in the case mentioned in Box 3.22. The goal of preventing drug sales and, thus, the need to confiscate, is laudable, but the NRA states that there are still more than 200 000 drug crimes recorded in Russia annually which are expected to generate proceeds for at least some persons or groups present in Russia. According to a September 2013 Russian government report, there were an estimated 8.5 million drug users in Russia (almost 6% of the population), so the domestic consumer base is not insignificant. The NRA notes the popularity of darknet drug markets catering directly to consumers as well as these markets' reliance on virtual assets as a means of payment. This threat requires financial investigation and a greater focus on asset confiscation, as opposed to large-load confiscation, to combat the changing patterns of the domestic drug trade. Russia also notes that profits from drug sales in Russia are often transferred overseas for laundering and investment and that LEAs co-operate with foreign authorities to carry out seizures. In other cases, particularly when proceeds are transferred to Middle East financial centres and some Central Asian countries, co-operation attempts have not resulted in seizures. Nonetheless, this is one area where confiscation results are disconnected with ML risk and where legal recognition of VA will have an impact on confiscation outcomes.

Box 3.22. Confiscation of the Proceeds of Drug Offences

MoI investigated drug trafficking and ML by S and D. Rosfinmonitoring detected 510 financial transactions indicating the laundering of RUB 19.6 million or EUR 267 000. D was convicted of drug trafficking (Art. 228.1) and self-laundering (174.1) and sentenced to eight years in prison. RUB 4.6 million or EUR 62 665 was confiscated from assets provisionally seized.

289. In the area of TF, most seizures are of instrumentalities and small amounts of money, which is aligned with the risk in Russia. In a survey of 1 600 judicial decisions issued between 2013 and 2017 in terrorism cases, instrumentalities were confiscated most frequently. In 97 terrorism judgments dealing with 137 individuals, 14 vehicles and 110 electronic devices were ordered confiscated. In 10 TF judgments dealing with 13 individuals, one vehicle and 10 devices were confiscated. The equivalent of EUR 7 557 was confiscated in TF cases in 2017 and EUR 6 000 was confiscated in 2018. Illegal armed groups in the North Caucasus pose a diminishing, but still existent TF threat for Russia, and according to authorities, judges often find such defendants impoverished and confiscation impossible.

290. In the area of financial sector crime, solid results are achieved pertaining to assets stolen from Russian FIs, but more work is needed regarding assets sent abroad via FIs located in Russia. As discussed above, vast amounts of money have been moved out of Russia through the financial sector in recent years. In just one example, an EU-based financial institution was heavily fined by two countries for insufficient AML controls that permitted EUR 10 billion in suspect funds to be transferred out of Russia through mirror trades; associated confiscation results were not shown. Russian authorities assert that they have faced challenges tracing potential proceeds due to the passage of time and the complex methods used to

justify the flows, such as layering through legal structures and fictitious contracts. Primarily, Russian authorities assert that they have faced obstacles in receiving international co-operation in tracing, seizing, and recovering funds from certain jurisdictions. An increasing number of formal requests have been sent by Russia in connection with ML and predicate offences (31 in 2017 and 17 in 2018), but in spite of the apparent unresponsiveness of other countries, Russian authorities should persist and consult with partners about the use criminal confiscation as the basis for such requests.[46]

291. Russian authorities have been attempting to trace assets stolen and transferred out of domestic banks, and have identified, with the assistance of dozens of jurisdictions, more than EUR 179 million embezzled from 114 Russian credit institutions. For crimes in the financial sector, RUB 130 billion or EUR 1.7 billion, was seized between 2013 and 2018. On average during this timeframe, RUB 10 billion or EUR 139 million was restituted by individuals accused of crimes such as fraud, embezzlement, deliberate bankruptcy, and illegal banking, on an annual basis. Between 2013 and 2018, through seizure or voluntary restitution, Russia recovered EUR 38.9 million in illegal banking investigations. Although there were quality case examples of asset recovery related to fraudulent activity in the financial sector, additional confiscation results in this area, particularly for assets located abroad, were expected by the assessment team.

Box 3.23. Asset Recovery Related to Financial Sector Crime

- MoI and Rosfinmonitoring dismantled an OCG, operating under the control of M and R, which took over credit institutions through third-parties and numerous shell companies. M and R were charged with participating in an organised criminal group (Art. 210) and registering fictitious companies (Art. 173.1). RUB 120 billion, or EUR 1.6 billion, was cashed out through this network. Although the source of the funds was not entirely determined, the OCG made profits of approximately EUR 8.6 million. During the investigation, assets totalling RUB 420 million or EUR 5.7 million were seized, including funds held in shell company accounts. M, R, and others were convicted in 2016 and assets confiscated included the amounts seized as well as cash hidden in the residences of the defendants.
- During an investigation into PA and PS for causing intentional bankruptcy of a commercial bank shortly before its licence was withdrawn, MoI in the Keremovo Region seized a shopping centre belonging to the suspects worth RUB 3.3 billion or nearly EUR 45 million. PA and PS were charged with abuse of authority (Art. 201) and misappropriation (Art. 160). A civil claim brought by DIA was satisfied using the seized property.

[46] See also Ch. 8.2.2 and Recommended Action 2 within IO.2.

292. In the high-risk area of budget spending and taxes, Russian authorities, especially Rosfinmonitoring, take an innovative approach that emphasises the prevention of theft in procurement, particularly in infrastructure and defence contracts. This positive feature is noted by the assessment team, but it is not strictly speaking a matter of confiscation. However, case examples demonstrated that the authorities do seek to confiscate stolen public funds in Russia, and, increasingly, abroad, including through the enforcement of Russian court orders and confiscations initiated by third countries on the basis of Russian requests and evidence. For crimes in this key risk area, RUB 83.9 billion or EUR 1.15 billion, has been seized in the five-year period between 2014 and 2018. On average, RUB 24 billion or EUR 333 million was restituted by individuals accused of crimes concerning public funds on an annual basis.

Box 3.24. Confiscation of Misappropriated Public Funds

A joint-stock company and its managers embezzled budgetary funds allocated to the Ministry of Defence. Proceeds were laundered through real estate, luxury goods and vehicles, and stashed in bank safe-deposit boxes. The financial investigation, requested by military prosecutors, was carried out by FSB and Rosfinmonitoring, which sent FIU requests to three foreign FIUs. Assets valued at more than RUB 1 billion (EUR 13.6 million) were seized and the director and accountant of the joint-stock company were found guilty of fraud (Art. 159) and self-laundering (Art. 174.1). Seized assets were used to satisfy fines imposed and were converted into state ownership.

293. In the area of corruption, on average, nearly EUR 400 million worth of proceeds and instrumentalities are seized per year in cases concerning mainly bribery and abuse of office. From 2014 to the end of 2018, nearly RUB 25 billion or EUR 345 million was voluntarily restituted by individuals accused in corruption cases. Russia uses a multipronged approach to recover the proceeds of corruption and budget spending offences, to include conviction-based and NCB confiscation, restitution, and civil lawsuits filed by prosecutors on behalf of victims including state entities.

Box 3.25. Confiscation of Misappropriated Public Funds

FSB and Rosfinmonitoring investigated a former official of the Ministry of Defence (MoD), X, who conspired with executives of private companies and another MoD official to embezzle funds gained by selling off MoD property and laundering hundreds of millions of roubles through loans and the acquisition of real estate. Assets seized from the suspects included more than EUR 10.8 million worth of paintings, jewellery, watches, and other assets. In 2015, X was convicted, along with others, for fraud (Art. 159) and self-laundering (Art. 174.1) and damages were recovered from amounts seized.

294. Another EUR 159 500 000 was confiscated using unexplained wealth motions in 2016-2017, and GPO expects to use this tool in increasingly significant cases. With one LEA estimating the "cost of corruption" at over EUR 1.69 billion in the last seven years, these are sound results, but LEAs should be encouraged to continue undermining the profit motive for corruption through confiscation actions against corrupt public officials high and low, and those who facilitate them, in all vulnerable sectors.

Overall conclusions on IO.8

295. Russia pursues confiscation as a policy objective and LEAs use financial investigations to routinely trace the proceeds and instrumentalities of crime. Provisional measures are used vigorously, including against equivalent value. Authorities focus on compensating victims, so restitution figures are higher than criminal confiscation figures. Restitution is the priority under the Russian system, and criminal confiscation is used when legal owners cannot be identified or for offences that create proceeds, but do not cause pecuniary loss to victims. The statistical picture in terms of Russia's domestic asset recovery efforts is solid. The GPO is increasing its pursuit of the unexplained wealth of public officials. While authorities are pursuing criminal assets moved abroad with more frequency, cross-border confiscation is not yet a fully established practice for LEAs. Confiscation regarding falsely or non-declared cross-border movements of currency/BNI is pursued to a lesser extent, partly due to the lack of a declaration obligation within the EAEU, but fines imposed for cash smuggling help to bolster the dissuasiveness of this sanction. The seizure and confiscation of funds related to drug crimes, the most common ML predicate, are low and decreasing, although some contextual factors mitigate this in part.

296. Russia is rated as having a substantial level of effectiveness for IO.8.

CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 9

1. Russia has a strong understanding of its domestic and international terrorism threats and the TF risks associated with those threats.
2. Russia has a robust legal framework for combatting TF, which is largely in line with international standards.
3. On average, Russia pursues 52 TF prosecutions per year. Since 2013, Russia has convicted more than 300 individuals of TF, with the majority resulting in sentences of imprisonment ranging from 3-8 years.
4. LEAs and prosecutors must consider in the course of each criminal investigation whether there are indications of other crimes and whether property has been used or intended for use to finance terrorism or groups engaged in such activity. This requirement has the effect of ensuring that the investigation of the financial aspects of terrorist crimes is mandatory. In practice, LEAs systematically consider the financial component of terrorist activities, which has led to the detection, identification and investigation of TF. Russia is able to identify different methods of TF and the role played by financiers.
5. The investigation of TF is integrated with, and used to support, national counter-terrorism strategies and investigations. Agencies co-ordinate and co-operate well across jurisdictions. Counter-terrorism and CFT have been given top priority by the highest level of the Russian government.
6. Russia has several alternative measures to disrupt TF where it is not practicable to secure a TF conviction, which it actively applies in practice.

Immediate Outcome 10 and Immediate Outcome 11

7. Overall, Russia has an adequate system to implement TFS, but has gaps and weaknesses in some areas. Russia demonstrates an ability to implement TFS within the context of UN designations, national designations and in response to requests from third countries to take freezing actions pursuant

to UNSCR 1373. There is a shortcoming in relation to Russia's ability to implement UN designations without delay.

8. Rosfinmonitoring plays an important role communicating TFS obligations to FIs and DNFBPs and raising awareness in the private sector.
9. Russia's domestic TFS regime has both terrorism and extremism activity as potential grounds for designation. The process for accessing frozen funds differs between the "international" list (which relates to UN designations) and the domestic lists. As a result, the assessment team noted confusion among reporting entities met on-site regarding the various lists (UN lists, domestic terrorism lists, domestic extremism lists) and their respective procedures to seek special exemptions or access to frozen funds.
10. Russia makes extensive use of its domestic designation regime, with over 7 000 persons and groups domestically designated as terrorists (this does not include the significant additional number of extremist designations). Russia has also sent one freezing request containing over 400 names to third countries for consideration of designation pursuant to UNSCR 1373. Russia makes significantly fewer proposals for international designation at the UN (in the last five years, Russia proposed 21 persons, four groups, one delisting request, and an alias addition to a listed group).
11. While Russia identified the overall TF risk associated with NPOs as low, some parts of the sector were assessed as medium-risk and subject to additional controls. Russian authorities are conducting risk-based outreach to and supervision of NPOs.
12. Russia demonstrates that it deprives terrorists, terrorist organisations and terrorist financiers of assets and instrumentalities through various approaches, such as through terrorist designations, administrative freezes, court orders, and confiscation. While the total amount of assets and instrumentalities deprived is low, it is consistent with Russia's risk profile.
13. During the last five years, Russia has frozen accounts related to one person listed pursuant to DPRK sanctions pursuant to UNSCR 1718 and its successor resolutions.
14. Some of FIs and DNFBPs may face challenges in the effective implementation of PF TFS due to difficulties in identifying the ultimate BO of a customer or party to a transaction. At the same time, the supervisory authorities are working to clarify the AML/CFT obligations of FIs and DNFBPs.
15. The obligation to implement TF and PF TFS does not apply to all natural and legal persons. Although Russia's Constitution establishes an automatic incorporation of all UN Chapter VII decisions into domestic law, the relevant UNSCRs do not include all the elements required to be an enforceable mean under the FATF Standards and some requirements are incumbent upon member states to implement through domestic legally enforceable means. While the AML/CFT law contains penalties for TFS breaches by obliged entities, there are no explicit penalties for natural and legal persons who

contravene the TFS requirements. Instead, Russia would apply its TF offence for TF TFS violations by natural and legal persons, which does not cover the freezing requirement. There is no mechanism to punish natural or legal persons (beyond FIs and DNFBPs) for PF TFS violations.

16. Russia has a useful mechanism in place to administratively freeze accounts for five days, which can be extended to 35 days (i.e., the 5+30 day freeze) when there is a suspicion that a transaction relates to a designated person or group.

Recommended Actions

Immediate Outcome 9

1. Russia should continue its efforts to detect possible TF offences and, if detected, investigate and prosecute them. Furthermore, since the terrorist threat continues to evolve, Russia's CFT strategy should be updated to reflect the changing nature of the threat.
2. In addition to using Rosfinmonitoring and the Egmont channel, Russia should more actively communicate expulsions of TF suspects to third countries using a different authority, such as the MoI or the FSB.

Immediate Outcome 10 and Immediate Outcome 11

Russia should:

1. Take actions to implement TFS without delay, including the communication of the lists to reporting entities by Rosfinmonitoring.
2. Implement explicit measures to ensure that all natural and legal persons (beyond FIs and DNFBPs) have legally enforceable UN TFS freezing measures and are prohibited from making any funds, financial assets or economic resources available for the benefit of a UN designated persons or entities, whether directly or indirectly.
3. Proactively request jurisdictions other than EAG members to consider giving effect to Russia's domestic designations pursuant to UNSCR 1373.
4. Consider proposing additional designations to the relevant UNSC Committees.
5. Continue raising and maintaining awareness amongst FIs and DNFBPs on TF and PF TFS to ensure that sanctions obligations are understood and implemented, especially with respect to the various lists of terrorists and their scope, as well as the distinct regimes governing the access to frozen funds.
6. When access to frozen funds is granted to domestic designees under national law, consider whether disbursements should be made in a more traceable form than cash.
7. Ensure that the next update of the NPO TF risk assessment incorporates more granular information identifying the features and types of at-risk

NPOs within the legal forms rated as medium-risk, as well as the findings of supervision for different types of higher TF risk NPOs to enhance its utility for public and private users.

8. Carry out additional outreach and communication with the private sector in respect to the NPO sector analysis.
9. Enact and implement the additional draft measures to better protect the NPO sector from potential TF abuse.
10. Consider ways to strengthen obliged entities' ability to identify companies owned or controlled by sanctioned entities, in order to identify possible instances of PF sanctions evasion.

297. The relevant Immediate Outcomes considered and assessed in this chapter are IO.9-11. The Recommendations relevant for the assessment of effectiveness under this section are R. 1, 4, 5–8, 30, 31 and 39.

Immediate Outcome 9 (TF investigation and prosecution)

Prosecution/conviction of types of TF activity consistent with the country's risk-profile

298. As noted in the TC Annex, Russia has a robust legal framework for combatting TF, which is largely in line with international standards. Specialised units within the FSB are responsible for initiating/investigating terrorism and TF offences at the intelligence phase (i.e., pre-investigative phase). The IC has investigative units across Russia that specialise in terrorism and TF investigations and are responsible for leading public investigations into terrorism and TF (see IO.7 for the phases of investigations in Russia). Similarly, the GPO has dedicated anti-terrorism/extremist and TF units in each of the federal subjects of Russia who assist in the prosecution of these cases. Rosfinmonitoring plays an important role in the intelligence phase and during public investigations by initiating investigations through its tactical analysis or helping to establish the financial linkages in ongoing cases. Other LEAs, such as MoI and the FCS also participate in TF and terrorism cases, where appropriate. In complex cases, LEAs establish joint task forces to develop terrorism and TF cases. Military courts are responsible for hearing TF cases. Terrorism and TF appeals are heard by the four Military District Courts, and final appellate authority rests with the military chamber of the Supreme Court. The Military Courts follow the same procedures as civilian courts.

299. Russia has a strong understanding of its domestic and international terrorism threats and the TF risks associated with those threats. The assessment team based its conclusions on a variety of elements, including discussions with relevant LEAs during the on-site visit. The team also reviewed numerous case studies and statistics, which demonstrate Russia's active investigation, prosecution and conviction of individuals and groups involved in TF, consistent with its TF risk profile.

300. As noted in IO.1, the TF NRA states that Russia's primary terrorism threat relates to: illegal armed groups operating in the North Caucasus; cells of international terrorist organisations operating in Russia; Russian FTFs traveling to/returning from

conflict zones; foreign terrorist fighters transiting through Russia to travel to/return from conflict zones; and perpetrators recruiting Russian nationals for terrorism through the use of internet. Risks are considered in view of the vulnerabilities in the three stages of TF (i.e. raising, moving and using funds).

301. The TF NRA states that the highest risk methods for TF are: soliciting funds via the internet; cash transfers; transfers of funds using bank accounts and bankcards; and the movement of funds via money transfers (without opening bank accounts). The TF NRA considers these TF methods are common to all terrorist individuals and groups.

302. As a public document, the analysis contained the TF NRA is written at a general level and does not provide granular information about Russia's specific TF threats. For example, the TF NRA does not outline which of the aforementioned TF methods illegal armed groups in the North Caucasus or Russian FTFs most often employ. Nevertheless, this public document is supplemented by more granular and specific knowledge of precise groups, cells and regions on the part of the LEAs who specialise in terrorism and TF. Indeed, LEAs met by the assessment team demonstrated a strong understanding of the financial activities of specific terrorist organisations and cells operating in Russia and abroad.

303. In the last five years, Russia's terrorist threat environment has corresponded to the activities of Islamist terrorist organisations, with most domestic terrorist activity occurring in Chechnya and Dagestan. As a result of enhanced counter-terrorism efforts, terrorism and TF threats emanating from these regions has steadily decreased in recent years. Most recent terrorism and TF activity relates to FTFs departing Russia to participate in terrorist activity in conflict zones, or the provision of funds to persons or groups operating in these areas. Between 2013-2018, approximately 4 000 FTFs have departed Russia to conflict zones. Given the recent reduction of ISIL-held territory, FTFs re-entering or transiting through Russia are a heightened area of focus for LEAs.

304. Various types of TF cases are investigated and offenders are successfully prosecuted, consistent with Russia's TF risk profile and reflective of the methods and channels of TF activities described above. LEAs across the country share a common strategy of pursuing the most serious terrorism-related offence and this often results in a more serious charge (i.e. CrC Article 208, the creation of a terrorist organisation and participation therein) instead of a TF-specific charge (Article 205.1 CrC). On average, Russia pursues 52 TF prosecutions per year (based on data from 2013-2018), with the highest number of prosecutions occurring in 2017 (83 in total). This peak in terrorism and TF prosecutions is attributable to ISIL-related activities and FTFs. Since 2013, Russia has convicted 333 individuals of TF.

Table 4.1. Terrorism/TF Investigations, Prosecutions and Convictions

	2013	2014	2015	2016	2017	2018
Detected Terrorist crimes	661	1128	1538	2227	1871	1679
Detected TF	74	124	127	109	236	364
Terrorism prosecutions	265	367	436	555	607	567
TF prosecutions	29	48	45	35	83	69
Persons convicted for terrorism crimes	247	342	360	556	647	574
Persons convicted for TF crimes	30	35	41	48	89	90

305. Charges and final verdicts may not occur in the same year. As a result, there are more convictions than prosecutions in some years (see Table 4.1). Nevertheless, the GPO states that there have been no acquittals and that all TF prosecutions have resulted in conviction. As mentioned above, TF is an offence dealt with exclusively in military district courts. By virtue of Federal Law 321-FZ (2008), TF is not a charge for which a jury trial can be requested—all TF cases are heard by three-judge panels. A 100% conviction rate on TF, quite unusual amongst the FATF Global Network, could confirm the thorough work of LEAs in gathering evidence and of prosecutors in presenting persuasive cases. The assessment team could not determine any substantive reasons for the difference between the ML and TF conviction rates.

306. Through multiple case examples, Russia demonstrated that it actively prosecutes and convicts different types of terrorist activity. The most prevalent activities prosecuted are money transfers between individuals, and moving funds using accounts in FIs. There were no TF prosecutions of natural persons that involved NPOs or the use of legal persons.

Table 4.2. Statistics on Methods and Types of TF

Type of TF	2014	2015	2016	2017	2018
Collection and/or accumulations of funds	8	11	12	13	51
Provision of funds for needs to terrorists	13	8	23	41	68
Moving funds through online transfers	2	6	13	39	38
Moving funds using FIs	7	12	15	55	151
Direct provision of funds to terrorists	2	3	9	28	21
Providing terrorists with instruments and means to commit terrorism-related crimes	n/a	n/a	5	3	18
Money transfers between individuals	11	17	44	84	103
Moving cash	4	6	9	27	18

307. The following cases demonstrate Russia's pursuit of various types of TF, including the collection, movement and use of funds.

Box 4.1. TF Case Involving Online Fundraising and Bank Cards

During the activities aimed at countering terrorism, Mr. B was detected by the FSB. According to operational information, in February 2014, Mr. B arrived in Syria to participate in the armed group "Jamaat Seifullakh Shishani" structurally associated with the Jabhat-al-Nusra. Mr. B then created propaganda sites on Vkontakte and Facebook to organise the collection of funds for TF. The collected funds were provided to Jabhat-al-Nusra, including for the purchase of weapons, uniforms, food and travel expenses for FTFs to travel Syria. In order to establish TF conduct by Mr. B, the FSB sent a request to the Interregional Department of Rosfinmonitoring. In the course of the financial investigation, it was established that Ms. H provided Mr. B with the following financial instruments registered in her name: the virtual wallet "Q" and the bankcard issued to this wallet for collecting money in the interests of Mr. B. The total amount of incoming funds on the virtual wallet Q in the period from October 2015 to March 2016 amounted to RUB 284 646.99 (EUR 4 000). In the same period, the total amount of outgoing transactions amounted to RUB 164 962.12 (EUR 2 262). At the same time, Ms. H under the pseudonym "Muslim Abdullaeva" was a subscriber of a closed group in the social network created by Mr. B, where she introduced herself as his wife. It was found that, in 2015, Mr. N provided financial support to Jabhat-al-Nusra by transferring money from his bank card issued by bank S to the bank card owned by Ms. H using the information published by Mr. B online. In the period from November 2015 to December 2015, Mr. N made four transactions totalling RUB 5 200 (EUR 71) to the bankcard. The GPO prosecuted Mr. N for TF (art. 205.1), Ms. H for TF crimes and for publically appealing to commit extremist activity (art.205.1 and 208) and Mr. B for the same two offences, as well as organising the activities of terrorist organisations (art. 205.5).

The criminal case against Mr B and Ms. H was suspended due to the lack of information about his whereabouts. Subsequently, the defendant was included on the Federal wanted list.

On 26 April 2017, Mr. N was found guilty of TF pursuant to art. 205.1 CrC and was sentenced to five years of imprisonment.

Box 4.2. TF Case Involving Bank Accounts and Bank Cards

The IC found that from June to October 2014, Mr. R knowingly made money transfers (totalling RUB 152 000, or EUR 2 084), through ATMs, to the bankcards of ISIL members with the intent that it be used for terrorism purposes. Mr. R was found guilty of committing three instances of TF (art.205.1) and on 18 December 2017, was sentenced to eight years imprisonment.

Box 4.3. TF Cases Involving Cash

- In January 2017, criminal cases were brought to the court on charges of Mr. U and Mr. S in crimes under Part 5 of Art. 33, Part 1 of Art. 208, Part 1 of Art. 222, Part 1 of Art. 222.1 of the Criminal Code. It is established that Mr. U, in order to provide financial services to support the activities of Khasavyurt Sector, transferred to Mr. S EUR 55 to the purchase a vehicle. Mr. S, in his turn, while collecting funds, invested his money in the amount of EUR 233 and bought a car. Later he gave to the participant of the illegal armed formation Mr. A the car and EUR 69 intended to support the activities of this illegal armed group. In June 2017, the court found Mr. U and Mr. S guilty and sentenced to imprisonment for 13 years and 13 years 6 months, respectively.
- In September 2013, Mr. V requested from his friend Mr. S for funds to travel to Syria to join ISIL. Thus, Mr. V intended to commit a crime under Part 2 of Art. 208 CrC. On 20 September 2013, Mr. S gave Mr. V EUR 350 knowing that this money was intended to ensure the participation of Mr. V in an illegal armed group. In January 2016, Mr. S was found guilty and sentenced to six years imprisonment.

Box 4.4. TF Cases Involving Fund Transfers

- In August 2017, the Military Court found Mr. S guilty of TF. Mr. S was involved in terrorist activities online. Mr. S transferred EUR 137 through Western Union to a member of the subdivision of the terrorist organisation "Imarat Kavkaz", in Turkey. Mr. S was sentenced to six years imprisonment, and a fine of RUB 2 331 (EUR 32).
- In 2015, Mr. A, while in prison, created an online terrorist community to collected funds for terrorism. Acting on the instructions of Mr. A, Mr. K, Mr. Z, and Mr. D murdered two persons combined with robbery. The victim's stolen money and

car, totalling RUB 428 000 (EUR 5 868), were sent to finance ISIL. On July 2016, the Military Court found Mr. A guilty and sentenced him to 30 years imprisonment for accumulative offences. Partners in the crime and perpetrators of the robbery-related murder, Mr. D, Mr. K and Mr. Z were sentenced to 27.5, 27 and 26.5 years imprisonment, respectively.

- In July 2017, the Military Court convicted Mr. J of TF, and sentenced him to four years and six months imprisonment. In 2014, Mr. J transferred RUB 4 000 (EUR 55) through bank S to purchase a ticket for an ISIL recruit, and transferred another RUB 3 500 (EUR 48) to the same person after he joined ISIL in 2015.

TF identification and investigation

308. In line with the TF NRA, Russia has successfully identified instances of TF, including through its sophisticated and extensive use of financial intelligence in the course of terrorism investigations (see IO.6). Similar to the process followed in predicate offence investigations, all terrorism investigations consider the financial dimensions of a case. Indeed, this requirement is established in law (i.e. the CPC) and it is the responsibility of the GPO to verify that LEAs conducted financial analysis in the course of their investigative work. As a result, LEAs systematically consider the potential or actual financial aspects of all identified terrorist activities, which has resulted in nearly 300 TF charges laid in the last five years (see Table 4.1 above). When appropriate, TF is also pursued as a distinct criminal activity, resulting in the initiation of TF investigations even in the absence of other suspected terrorism offences.

309. TF is typically detected through "operational investigative measures", which refers to law enforcement investigative activity as outlined in R.30-31 in the TC Annex and includes the full range of routine and special investigative techniques. LEAs also analyse records obtained from FIs and DNFBPs, employ the assistance of specialists as needed, and review tax information, if required. Information is also obtained through international co-operation, including from foreign LEAs (and intelligence agencies). For example, relevant requests for legal assistance were sent to the competent authorities of the Republic of Azerbaijan, the Kyrgyz Republic, the Republic of Kazakhstan, the Republic of Tajikistan, the Republic of Turkey, and the USA. The below cases exemplify TF investigations that required foreign legal assistance.

Box 4.5. Cross-border TF Cases

Azerbaijan: The FSB identified the offence of TF through a criminal case against Mr. G through wiretapping. In addition, the phones and laptop of Mr. G were seized. The result of its inspection discovered Mr. G spoke with his brother through Skype. It was determined that the brother of Mr. G headed one of the units of the terrorist organisation, "Jund al-sham". Moreover, the testimony of witnesses (friends and relatives of the accused) confirmed the radical views of Mr. G. During the investigation, Mr. G was found to be involved in TF between 2013 and 2014 in the

amount of USD 7 000 through money transfers to "Junsh al-sham," which were cashed in Turkey. In the criminal case against Mr. G, a request for legal assistance was sent to the Republic of Azerbaijan, the results of the response confirmed the involvement of the accused's brother in terrorist activities and his departure to Syria. Mr. G was found guilty TF and was sentenced to five years imprisonment, with a fine of RUB 200 000 (EUR 2 744). The car owned by Mr. G was seized in order to ensure payment of the fine.

Belgium: In September 2018, LEAs extradited a Russian citizen from Belgium, Mr. G, who engaged in the provision of financial support to ISIL. Since 2015, he lived in Belgium, from where he sent money to ISIL fighters in Syria. In 2016, LEAs opened a TF case against Mr. G. In May 2017, the defendant was detained in Brussels and placed under pre-extradition arrest. On September 2018, Mr. G was extradited to Russia. This case is ongoing.

310. Russian authorities consider that one of the defining characteristics of CFT investigations conducted by LEAs is their constant and ongoing interaction with Rosfinmonitoring throughout the process. As outlined in IO.6, Rosfinmonitoring provides disseminations to LEAs on possible occurrences of terrorism and TF on request and spontaneously. When Rosfinmonitoring disseminates spontaneously, LEAs verify the information and, when applicable, use the information to initiate cases or use the information to support ongoing work. According to discussions with LEAs, as demonstrated through case studies, Rosfinmonitoring's financial intelligence is primarily used to provide ongoing support to investigations, and LEAs systematically make requests for information from Rosfinmonitoring. In some occasions, Rosfinmonitoring also provides LEAs with information on new suspects to initiate investigations. The FIU, in practice, responds to TF-related requests from LEAs within hours and one case example demonstrated that financial leads were provided to the FSB within 24 hours.

Box 4.6. Information on TF Received from Rosfinmonitoring

Upon request: The IC, in co-operation with Rosfinmonitoring, Mr. N (a Russian citizen) reliably knew that his brother Mr. M was a participant of ISIL in Syria. In the period from 4 to 9 December 2013, Mr. N knowingly provided a bankcard with RUB 200 000 (EUR 2 744) to a friend of Mr. M. In 2013 and 2014, the intermediary provided the cashed out fund to Mr. M, in Turkey. As well as during 2014, Mr. N purchased tickets for members of illegal armed groups to travel to Turkey and then to Syria to join ISIL. Rosfinmonitoring provided data on the specified financial transactions.

Spontaneous: In the course of financial investigations in respect of persons intended to take part in armed conflict on the side of ISIL (according to LEA information), Mr. A was detected by Rosfinmonitoring. On arrival to Turkey, Mr. A organised the collection of funds through

social networks for ISIL. Between April 2013-August 2014, approximately RUB 1 million (EUR 13 720) from individuals from various regions of Russia were transferred to the bank card of Mr. A. Mr. A cashed these funds in Turkey. Based on this information, the financial investigation was proactively sent to LEAs by Rosfinmonitoring. Surveillance activities found that the funds collected using the bankcard were used by Mr. A to support the activities of ISIL. In addition, it was discovered that a hotel located on the Turkish-Syrian border was rented by Mr. A at the direction of the leadership of ISIL. From the beginning of 2014 to September 2015, Mr. A organised financial and material support for ISIL in this hotel and also used it for recruits travelling to Syria to join ISIL. In April 2018, Mr. A was accused for various terrorism offences, including TF. Mr. A was domestically designated and his assets frozen. Mr. A is also currently internationally wanted.

311. Russian LEAs also take active steps to enhance their knowledge in order to improve the detection of TF offences. For instance, in 2017, the FSB issued letters to LEAs that included typologies of TF. The FSB also prepared a review of the implementation of countering terrorism and extremism.

312. With assistance from Rosfinmonitoring, the IC also prepared a handbook on how to use financial intelligence in the course of TF investigations. In particular, the IC reviewed TF cases and from October to November 2017, distributed letters to investigative authorities that called for the need to take additional measures to identify TF cases, as well as their effective investigation. In addition, TF typologies were described, and case examples included.

313. In 2017, the MoI prepared guidelines for the organisation of operational activities to identify and suppress TF and extremist activities, and distributed a confidential training manual on the organisation and tactics of LEAs to identify and suppress TF channels and extremist activities.

314. LEAs and Rosfinmonitoring have adequate human, financial and technical resources and ability to identify and initiate TF cases. For example, services, departments, offices, divisions and other units of the FSB have been formed in the field of combating terrorism and its financing. This has resulted in a specialisation of FSB investigators for conducting investigations into terrorism and TF.

315. In the MoI, the functions of CFT are assigned to specialised departments in the Main Directorate for combating economic crimes, as well as in the Main Directorate for combating extremism, and has specialised units in each local body of the MoI.

316. In Rosfinmonitoring, CFT is assigned to a separate department, and similar CFT units are defined in each regional branch of Rosfinmonitoring.

317. The structure of the investigative bodies of the IC is based on the territorial principle. The powers of the Main Investigation Department include the investigation of the most difficult, complex and dangerous crimes, including inter-regional and inter-state nature; the office includes several specialised investigative units, including the First Office for the Investigation of Crimes Against the Person and Public Security which specialises in the investigation of terrorism and TF.

318. The GPO also has a specialized unit for the prosecution of terrorism and TF. Specialised prosecutors work in each of the federal subjects of Russia.

TF investigation integrated with, and supportive of, national strategies

319. The investigation of TF is integrated with, and used to support, national counter-terrorism strategies and investigations. The TF NRA and its conclusions serve as basis for determining national CFT priorities. National strategies have been approved at the highest level of the government, forming the principles of Russia policy in combating terrorism and its financing. This includes the designation of terrorist and terrorist organisations.

320. The main strategic-level document is "The Concept of Combatting Terrorism," which was signed by the President in 2009, and notes that one of the principal conditions for enhancing the efficiency of CT activities is to better understand and attack the sources and channels of financing. TF investigations and prosecutions are in line with these overall objectives and are consistent with the TF threat identified in the NRA. For example, there has been an increase in the identification of TF related to the movement of funds through bank transfers. The Concept for the Development of the National AML/CFT System, approved on 30 May 2018, defines the main risks for ML and TF. It specifically mentions the risk posed by the use of new financial instruments and technologies to finance terrorist activity, including those allowing for the anonymity of participants in a financial transaction and the phenomenon of crowdfunding. This Concept also outlines the overarching goal of combatting TF, including, inter alia, (1) developing methods for identifying, investigating and detection of crimes related to terrorism financing, (2) specialising investigators, judges, and prosecutors to consider TF cases and building their capacity, (3) focusing on prevention of TF, and (4) expanding law enforcement's timely detection and blocking of assets intended for TF.

321. National co-ordination in the area of CT and CFT is handled by the National Anti-Terrorism Committee (NAC), the federal operational headquarters of the LEAs, and the headquarters of the same in the constituent entities of Russia. Since 2010 and at three-year intervals since then, the NAC has drawn up the interagency CT/CFT plans, the execution of which is mandatory for all participating agencies. While these plans are confidential, the assessment team received briefings on their content during the onsite visit. The plan in effect from 2013 through 2015, for example, resulted in the amendment of the AML/CFT Law to improve the legal mechanism for freezing terrorist assets pursuant to the national designation regime. The plan in effect from 2016 through 2018 resulted in improvements of the TFS freezing mechanism, criminalisation of the financing of international terrorism, and strengthened the penalties for TF (i.e. added the possibility of life in prison). A CFT- expert advisory group within the NAC is also tasked to, inter alia, increase the effectiveness of measures taken in this field. It is chaired by the Director of Rosfinmonitoring and includes members from LEAs, MoJ, MFA, FCS and the FTS.

322. The FSB and the NAC monitor the alignment of operational activity and results with the NRA TF on an ongoing basis. Threats and potential threats are identified, mitigating measures are implemented, strategies and laws are revised, and tactical-level documents are developed, as needed. The FSB and its units have operational performance plans that fully assimilate the results of the TF NRA (e.g.

terrorist fundraising online, through cash movements, using bank accounts, and through MVTS) although these documents were confidential and not provided to the assessment team.

323. Consistent with the high-level strategies and coordination arrangements, financial intelligence and financial disruption are used effectively at the operational level to support counter-terrorism objectives. Counter-terrorism investigators of the FSB and other LEAs use financial intelligence to map and understand terrorist networks and their connections, working in close co-operation with Rosfinmonitoring in the context of TF investigations. Parallel financial investigations are routinely conducted as part of every counter-terrorism investigation. Financial tools are used to disrupt (non-financial) terrorist activity by terrorists, particularly the 5+30 day administrative freeze when there is an urgent need to freeze an account of a suspected terrorist. While the LEAs interviewed on-site appreciated the utility of this tool, they emphasised that its use is a last resort and that preventive investigation and disruption should preclude its need, except in exceptional circumstances.

Box 4.7. Financial Intelligence Used to Counter Terrorism

In April 2014, Mr. S came to the attention of Rosfinmonitoring during the financial investigation of FTFs departing Russia to join ISIL. In November 2015, LEAs initiated a criminal case against Mr. S under part 2 of article 208 of the Criminal CodeCC.

Upon arriving in Turkey, Mr. S organised the collection of funds to support ISIL activities. Between May and December 2014, Mr. S received about RUB 5 million on his card from individuals from Russia. These funds were cashed by Mr. S in Turkey. A large number of persons identified as financial counterparties were previously known byknown by LEAs for possible involvement in terrorism activities.

In the course of financial investigations, it was determined that the bank card was being used tocarry out the collection of funds on behalfof ISIL. Part of the collected funds were withdrawn from the bank card belonging to Mr. S, the other part was used to ensure the departure of the newly recruited militants to Syria. In July 2017, LEAs initiated a TF case against Mr. S. Moreover, as a result of search and surveillance activities in respect of the financial counterparties of Mr. S, 13 criminal cases were initiated (seven for TF and six for the participation in the ISIL activities).

Effectiveness, proportionality and dissuasiveness of sanctions

324. As noted in the TC Annex (c.5.6), TF is punishable by a term of imprisonment of eight to twenty years (depending on TF activities) and the possibility of a fine up to RUB 700 000 (approximately EUR 9 640) or two to four years' salary. A maximum sentence of life in prison is also possible for TF in the most severe cases (e.g., financing an act of international terrorism, and financing an illegal armed group). The sanctions applied against natural persons are effective, proportionate, and dissuasive. As noted in the below table, natural persons convicted of TF were sentenced to imprisonment

for a term of three to five years (36% of cases) or for a term of five to eight years (33% of cases).

Table 4.3. Sentences of Imprisonment for TF Convictions

TF Sentences	2013	2014	2015	2016	2017	2018
Up to 1 year	0	0	4	1	0	0
Over 1 or 2 years	4	0	2	2	9	0
Over 2 to 3 years	5	7	6	4	13	6
Over 3 to 5 years	7	9	7	11	21	28
Over 5 to 8 years	2	8	4	12	19	31
Over 8 to 10 years	0	1	0	0	1	4
Over 10 to 15 years	0	0	0	0	2	0
Over 15 to 20 years	0	0	0	0	0	0
Total	18	25	23	30	65	69

325. In comparing TF penalties to penalties imposed for other terrorism-related offences, some crimes of terrorism have garnered sentences in the ten to twenty-year range, especially in 2017 and 2018; however, most sentences fall within a similar median range (most terrorism offenders receive between one and five-year sentences).

326. To further demonstrate the efficacy of TF sanctions, Russia provided statistics related to terrorism and TF recidivism rates (data was only available for 2017 and 2018). The recidivism rate for TF was 5.6 % in 2017, and 4.4% in 2018. For context, the total recidivism rate for all criminal offences in Russia in 2017 was 33%, and 36% in 2018.

327. While Russia does not allow for corporate criminal liability, legal persons may bear administrative or civil liability for TF. However, as noted above, LEAs have not identified any instances of TF involving legal persons (including NPOs). As a result, the effectiveness of administrative sanctions for legal persons liable for TF could not be assessed.

328. In summary, Russia applies dissuasive, proportionate and effective criminal sanctions for TF.

Alternative measures used where TF conviction is not possible (disruption)

329. Russian authorities indicate that their preference is to prosecute terrorists, and situations where prosecution for TF is not possible arise infrequently. Nevertheless, Russia has several alternative measures to disrupt TF where it is not practicable to secure a TF conviction, which it actively uses in practice. These measures are predominantly applied when the accused is located outside of Russia, and international legal assistance has failed or is not possible (e.g., the location of the accused is unknown).

330. The most common form of alternative measure is the use of the domestic listing process (i.e., the IAC CFT list), which results in: public identification of the person as a terrorist; freezing actions if accounts exist in Russia; and prohibitions of financial transactions and services. Russia makes very extensive use of this process,

both to supplement all terrorism convictions and as a freestanding sanction in some cases. The domestic listing process and total number of designated terrorist persons and groups is discussed in IO.10. In other instances where it is not practicable to secure a TF conviction, the GPO may advise for the application of other terrorism-related charges, such as aiding terrorists and the participation in the activities of a terrorist organisation. Every year, approximately 60 people are convicted under alternative articles (in total, 290 persons between 2014 and 2018).

331. Russia also uses deportation as an alternative measure based on a decision proclaiming the "undesirability of the stay of the foreign citizen" in Russia. This is determined by Rosfinmonitoring after consulting relevant domestic authorities. This measure has been used against three individuals since 2016. In these cases, Rosfinmonitoring communicated via the Egmont channel to the home country of the individuals to inform them of the deportation order and the relevant information on the case. In these three cases, the persons were under prosecution of TF in their home countries.

332. In urgent situations, where there is an imminent threat to life or danger of flight of persons or funds, LEAs may seek to disrupt TF rather pursue criminal charges. For example, an additional legal tool may be used by LEAs in the pre-investigative phase, which is referred to as the 5+30 day administrative freeze. This freeze can be triggered by LEAs, Rosfinmonitoring or FIs/DNFBPs themselves upon suspicion of a natural or legal person acting on behalf of a domestic or internationally designated person or group. In these cases, Rosfinmonitoring sends a request to the FI via the Personal Account to freeze accounts of a customer for five days (which can result in a tip-off to the target and disrupt the illicit activity). During this five-day period, LEAs and Rosfinmonitoring conduct a pre-investigation into the target. This freeze can be extended to a maximum of 30 days. After 35 days, LEAs must seek judicial approval to extend the freeze. If TF charges cannot be applied in these cases, LEAs seek to apply other terrorism-related charges (i.e., participation in a terrorist organisation or acting on its behalf).

333. Russia is also able to seize passports of suspected FTFs prior to their departure to conflict zones, as well as anyone suspected of a crime. However, Russia does not maintain statistics on the number of passports seized.

334. The last measure used is the prohibition of entry of certain foreign or stateless persons, as determined by Rosfinmonitoring. Four such bans on entry have been imposed on persons since 2017. An example of this measure is provided below.

Box 4.8. Prohibition of Entry

According to the FSB, a citizen of Azerbaijan, Mr. U, through online messaging applications, carried out calls for participation in the activities of ISIL in Syria. Ms. S came under the ideological influence of Mr. U, went to Turkey with the aim of joining and participating in ISIL. While in Turkey, she gave him her bank card, which Mr. U used to organize the collection of funds for the needs of ISIL members. An analysis of money flows on Ms. S revealed multiple money inflows and further cash withdrawals in Turkey for over EUR 600. With the money received, Mr. U

brought weapons, ammunition, foodstuffs, personal hygiene products, and clothing for members of ISIL. The IAC CFT received sufficient grounds to suspect the involvement of Mr. U in terrorist activities, and a decision was made to freeze money and other property of Mr. U. After that, based on the available information, Rosfinmonitoring decided to prohibit the entry of Mr. U to Russia for a period of 30 years.

Overall conclusions on IO.9

335. In summary, Russia has a strong understanding of its domestic and international terrorism threats and the TF risks associated with those threats. Russia also has a robust legal framework and combatting TF is assigned a high priority by the Russian government. LEAs systematically consider the financial component of terrorist activities, which had led to the detection, investigation and prosecution of TF. On average, Russia charges 52 TF cases per year. Since 2013, Russia has convicted more than 300 individuals of TF, with the majority resulting in sentences of imprisonment ranging from three to eight years. Moreover, Russia is able to identify different methods of TF and the role played by financiers.

336. Russia is rated as having a high level of effectiveness for IO.9.

Immediate Outcome 10 (TF Preventive Measures and Financial Sanctions)

Implementation of targeted financial sanctions for TF without delay

337. Overall, Russia has an adequate system to implement TF TFS, although there are some specific gaps and areas where these measures could be implemented more effectively.

338. Russia demonstrates its ability to implement TFS within the context of UN designations, national designations and in response to requests from third countries to take freezing actions pursuant to UNSCR 1373 and its successor resolutions (see R.6). The assessment team based its conclusions on a variety of elements including discussions with relevant authorities (Rosfinmonitoring, MFA, FSB, and the GPO), financial supervisors and a wide range of entities from the private and NPO sectors. The team also reviewed case studies and statistics on assets frozen.

339. Russia implements TF TFS through the adoption of two lists. One list consists of two parts: (a) all designated persons and groups listed pursuant to UNSCRs 1267/1989/2253 and 1988 (also referred to as the international list); and (b) persons and groups identified and designated by Russian authorities (Russia's domestic list established pursuant to UNSCR 1373).

340. The second list is composed of persons and groups identified and designated by the Interagency CFT Commission (IAC CFT), including persons listed upon third country requests or persons who have not been criminally prosecuted for terrorism, which also corresponds to the Russia's implementation of UNSCR 1373. Russia's

domestic designation regime refers to both terrorism[47] and extremism[48] activity as potential grounds for designation.

UN Designations

341. Russia employs an inter-agency approach to designating persons and groups with respect to UNSCRs 1267/1989/2253 and 1988 (and their successor resolutions), with the MFA leading the process. An internal classified regulation, which was reviewed by the assessment team while onsite, establishes how relevant authorities must co-operate prior to the submission of a designation by the MFA to the relevant UN Committee via Russia's Permanent Representative to the UN. Prior to submitting a designation proposal to the UN, the MFA holds a round of consultations with relevant authorities—including Rosfinmonitoring, LEAs and the FSB—to corroborate details of the case, ensure that the proposal conforms with the rules of the UN sanctions committees (i.e. templates, terms of reference, etc.), and requests additional information where necessary.

342. Russian LEAs and the FSB primarily identify targets for referral to the UN based on ongoing criminal investigations. In most instances, international designations occur in tandem with, or after, a domestic designation (see Box 4.9 below). Most persons referred for designation to the UN are located abroad (e.g. FTFs in Syria). The decision to propose designations to the relevant committees of the UN occur simultaneously with a request to Interpol to issue a Red Notice.

343. During the last five years, Russia has proposed 21 persons and 4 groups for designation, and one de-listing request to the relevant the UN Security Council Committee 1267/1989/2253. Most recently, in June 2018, Russia submitted an alias request for Jabhat al-Nusra. Nine designation proposals are still under consideration by the Security Council Committee 1267/1989/2253, the others have been approved (12 persons, four groups, one de-listing request, and alias addition).

344. Russia has frozen the assets of one UN-designated person. This individual was proposed by Russia to the UN 1267/1989/2253 Committee. The details of this case are summarised below.

Box 4.9. Russian UN Proposal and Assets Frozen in Russia

Mr. B was domestically designated in Russia on 19 March 2015, resulting in freezing measures. In September 2016, Mr. B joined ISIL and departed to Syria to participate in its activities. In 2017, the MFA submitted a designation request for Mr. B to the UN 1267 Committee. Taking into account all information included in Russia's designation submission, Mr. B was added on 20 July 2017 to the UN 1267 list [as Barkhanoev Malik

47 This relates to the provisions of the CrC dealing with terrorism (arts. 205, 205.1, 205.2, 205.3, 205.4, 205.5, 206, 208, 211, 220, 221, 277, 278, 279, 360, 361.

48 This relates to the provisions of the CrC dealing with extremism (280, 280.1, 282, 282.1, 282.2, 282.3).

Ruslanovich (QDi.405)], and included on 14 June 2018 in Russia's international list.

The criminal case against Mr. B is suspended due to the lack of information about his whereabouts. Mr. B is included in Russia's and international wanted lists. The accounts of Mr. B were frozen on 19 March 2015. The total amount frozen at the end of 2018 was approximately RUB 400 000 (EUR 5 560).

In 2017, Mr. B was placed on the Interpol watch list due to the initiation of a criminal case (related to the participation of an illegal armed group and TF) by Russian LEAs

345. While Russia has proposed 21 designations over the last five years, the assessment team notes that the number of proposals made to the UN is low in proportion to the large number of Russian domesc designations, and bilaterally proposals pursuant to UNSCR 1373 (see below). Russian authorities attribute this difference to the differing legal requirements for designation at the UN level and domestically (e.g. UN requires unclassified justifications for a potential designation). In addition, Russia reports that a large proportion of those individuals domestically designated are imprisoned in Russia, and therefore do ot pose a threat to the international community thereby rendering an international designation proposal unnecessary. The assessment team notes that Russia could consider designation proposals of individuals in prison, as the resulting freezing measures would apply to persons acting on behalf or at the direction of the imprisoned person.

Domestic Designations

346. Russia has four triggers for domestic designation pursuant to UNSCR 1373: (1) the existence of a criminal prosecution for terrorism; (2) a court decision or conviction (both domestic and foreign) related to terrorism; (3) a designation decision by the IAC in the absence of a criminal prosecution; and (4) requests from third countries. The below table outlines the number of domestically designated terrorist persons and listed in Russia each year for the last five years. On average, Russia domestically designates approximately 1 200 persons and groups per year for terrorist activity. As of the end of December 2018, Russia designated 7 419 terrorists and 1 379 extremists in total.

Table 4.4. Domestic Designations of Terrorists and Terrorist Groups (added/year)

	2014	2015	2016	2017	2018
Number of terrorist persons	723	1303	2013	1126	948
Number of terrorist groups	0	3	3	1	0

347. Russia also designates a significant number of persons and groups for extremism, resulting in the same consequences as domestic terrorist designations (i.e. freezing of assets). While these designations fall outside the scope of this assessment, the below table is included to provide context as Russia is unable to separate the statistics on frozen assets corresponding to these two domestic designation regimes. Russia designates approximately 600 persons and groups as extremists each year.

Table 4.5. Designations of Extremists and Extremist Groups (added/year)

	2014	2015	2016	2017	2018
Number of extremist persons	432	540	570	565	574
Number of extremist groups	9	6	10	398	8

348. In regard to foreign requests made pursuant to UNSCR 1373, the IAC CFT is responsible for considering potential designations proposed by third countries, and Rosfinmonitoring sends Russian requests to third countries. The IAC CFT is comprised of high-level representatives of Rosfinmonitoring, the MoI, FSB and MFA and is chaired by the deputy head of Rosfinmonitoring. Through this mechanism, over the last three years, Russia has given effect to more than 1 200 freezing requests from third countries (the IAC CFT received requests from Tajikistan, Kyrgyzstan, Kazakhstan and Uzbekistan).

349. The total amount of frozen funds related to these incoming foreign requests as of December 2018 was approximately EUR 5 500.

350. The majority of these third-country requests are a result of a May 2017 project led by the EAG Plenary. Most incoming requests were decided by IAC CFT within two days upon referral from the third country, and relate to FTFs or persons engaging in TF. Each country below submitted one request containing multiple names.

Table 4.6. Number of Persons Specified in Incoming UNSCR 1373 Requests

	2016	2017	2018
Tajikistan			995
Kyrgyzstan	76		
Kazakhstan		122	
Uzbekistan			20

351. In terms of outgoing requests to third countries, from August to September 2017, Rosfinmonitoring sent to the eight other EAG member countries, as well as to the FIUs of Turkey, France and Belgium, one proposal for potential domestic designation of 419 Russian citizens who have committed acts of terrorism and TF or suspected in such activities

352. Russia does not systematically propose designations pursuant to UNSCR 1373 to third countries. The aforementioned requests appear to be a standalone occurrence.

De-listing

353. In addition to the one aforementioned delisting request to the UN, Russia has delisted a number of persons and groups from its two domestic terrorist lists, 36% of which relate to persons designated for terrorism-related reasons (see table below).

Table 4.7. Domestically De-listed Persons and Groups

	2014	2015	2016	2017	2018
Terrorists	186	95	243	151	242
Extremists	195	281	307	388	434
Terrorist groups	0	0	0	0	0
Extremist groups	0	0	0	1	0

Implementation of sanctions

354. Under the Constitution of the Russian Federation, international treaties (including UNSCRs) are a component of the legal system without the need for a separate act of implementation. However, the relevant UNSCRs do not include all the elements required to be enforceable means under the FATF Standards. The AML/CFT Law, while requiring immediate freezing, does not indicate the moment when such an obligation arises. Instead, it sets the deadline for the implementation of the relevant UNSCR requirements to the publication of UN decisions on Rosfinmonitoring's website. This gives rise to a risk of delayed implementation of freezing obligations, which is not in line with FATF requirements. Under such interpretation of the law, the enforceable obligation for FIs and DNFBPs to implement TF TFS occurs when Rosfinmonitoring publishes UN and domestic listing decisions on its official website (www.fedsfm.ru/documents/terrorists-catalog-portal-act). The requisite freezing obligations by all FIs and DNFBPs enter into force within 24 hours of this publication taking place. As a result, funds could be frozen within two days after a decision is taken by the UN, or Russian authorities in the case of domestic designations.

355. As calculated in the table below, on average, Russia publishes UN designations to its official website within two days. This publication, for reasons explained above, is more than merely a communication, but rather is the moment when the enforceable requirement for freezing, with corresponding penalties for violations of these requirements, arises. So in practice obliged entities must comply with the freezing obligation within 24 hours after the publication occurs. Considering that the average transposition time is two days, plus an additional 24 hours is allotted for the legal requirement to take effect, the assessment team does not consider that the implementation of TF TFS is occurring without delay.

356. Indeed, the usual publication period (and therefore the enforceable implementation of TFS) exceeds the standard of within a matter of hours, which has been interpreted by the FATF as within 24 hours. As noted in the table below, on average, it takes Rosfinmonitoring two days to publish UN designations. The assessment team notes that Russia holds a permanent position on the UN Security Council and is therefore aware of upcoming UN designations. This position should allow Russia to reduce its publication delay in practice, enabling Rosfinmonitoring to publish the new decisions as soon as officially adopted at the UN.

Table 4.8. Russian Publications of Recent UN Designations (UNSCRs 1267/1989/2253/1988)

UNSCR List	Date listed by UN	Decision Taken by UN	RFM Publication	Days
1267/2253	29/03/2019	Changes regarding six persons	01/04/2019	3
1267/2253	22/03/2019	One organisation listed	25/03/2019	3
1267/2253	13/03/2019	Changes regarding one person	14/03/2019	1
1267/2253	28/02/2019	One person is listed	01/03/2019	1
1267/2253	08/02/2019	Four persons listed	11/02/2019	3
1988	30/01/2019	Changes regarding two persons	31/01/2019	1

357. Rosfinmonitoring plays an important role in the communication of TFS obligations and raising awareness to FIs and DNFBPs. Reporting entities are proactively alerted of any changes to the UN and domestic TFS lists via their Personal Account, which also includes updated lists available for download. For those 1-2% of DNFBPs who do not yet hold a Personal Account, the publication on Rosfinmonitoring's website serves as notification.

358. The obligation to freeze as well as the prohibition from making any funds or other assets available to or for the benefit of designated persons or entities applies to FIs and DNFBPs, but does not apply to all natural and legal persons in Russia since there are no provisions that explicitly provide for liability for infringing the prohibition by all natural and legal persons (other than FIs and DNFBPs). Russia asserts that its Constitution establishes an automatic incorporation and a direct applicability of the UNSC decisions. While the assessment accepts this argument to some degree, relevant UNSCRs do not include all the elements required to be enforceable means under the FATF Standards but rather require member states to implement specific domestic legal requirements.

359. In practice, Russia uses its TF offence to punish the conduct of making funds or other assets, economic resources, or financial or other related services available to or for the benefit of designated persons or entities (see c.6.5 in the TC Annex). Russia provided cases where persons were prosecuted and convicted by the Court for making funds available to ISIL, including one case initiated after the onsite visit. Russia states that although the Judge needs to verify the commission of the criminal conduct (i.e. make funds available), the fact that an UN-listed person/entity is a terrorist is not challenged. Therefore, while there is a technical compliance deficiency for the TFS requirement of making funds available to or for the benefit of designated persons or entities by natural and legal persons (other than FIs and DNFBPs), the assessment team finds that the application of the TF offence mitigates it in practice.

360. To enhance the understanding of TFS by reporting entities, Rosfinmonitoring clarifies Russian legislative measures on its website. For example, on 16 January 2014, Rosfinmonitoring published an Information Note related to questions about the application of freezing and unfreezing measures. An additional note issued on 3 October 2013 explains the legal aspects of forming a list and the role of Rosfinmonitoring. The latest Information Note dated 1 March 2019, outlines the

recommendations for TFS implementation by the newly obliged DNFBPs, lawyers, notaries and accountants.

361. As noted above, numerous accounts have been frozen in relation to Russia's domestic TFS lists, and one account belonging to a UNSCR 1267-desginated person is frozen (see Box 4.9 above). During the onsite visit, Russia amended L115 to introduce an explicit freezing obligation for lawyers, notaries and accountants. Although this is a new legal obligation, the assessment team confirmed with a sample of the sector that they were indeed implementing TFS prior to this explicit legal obligation entering into force.

362. As noted in IO.4, reporting entities met by the assessment team demonstrated a good understanding of their TFS obligations. However, differences in status between the two lists of designations appear to create misunderstandings amongst the private sector, particularly the procedures for granting access to basic expenditure for designated individuals and the management of frozen funds.

363. Larger FIs and DNFBPs have a deeper understanding of their TFS obligations and have effective controls in place with respect to sanctions implementation. They rely on communication through the Personal Account and also receive alerts through commercial screening databases. Some smaller FIs and DNFBPs manually screen their client base.

364. All private sector entities met during the onsite were aware of their TF TFS obligations as well as the possibility, in the case of suspicion, to suspend a transaction for up to 35 days (5+30 mechanism), in order to request Rosfinmonitoring to conduct financial analysis and confirm or deny the grounds or suspicion. On several occasions, Russia blocked or rejected transactions, and identified individuals acting on behalf of domestically listed persons.

365. One challenge to effective implementation of TF TFS is whether FIs/DNFBPs properly identify the BO of a customer or party to a transaction. As noted in IO.4, the understanding regarding the identification of BO amongst reporting entities is uneven. Most reporting entities heavily rely on the ownership criterion (i.e., equity or shareholding) and, if doubts arise whether or not these owners are the true BOs, reporting entities may disregard the person that, through other means, may control the legal entity. This weakness may impact TFS implementation, and may result in instances of sanctions evasions through legal persons and arrangements.

366. As mentioned in IO.3, supervisors, including the BoR and Rosfinmonitoring, conduct offsite and onsite examinations for TFS. Some violations of the requirements were identified during such examinations (see IO.3 for breakdown). The majority of these violations relate to non-compliance with the requirement to report to Rosfinmonitoring on customer screening for list matches.

Targeted approach, outreach and oversight of at-risk non-profit organisations

Understanding of the risk and mitigating measures

367. According to the 2018 TF NRA, the majority of Russian NPOs pose a low TF risk. One relevant TF vulnerability identified is when funds collected by NPOs are not

credited to accounts, but kept in cash or credited to bankcards or other means of payment (e.g. electronic wallets, mobile phone accounts).

368. A sectorial NPO risk assessment, conducted in 2018 by Rosfinmonitoring in collaboration with LEAs and the MoJ, identifies the subset of organisations that fall within the FATF definition of NPOs as: NPOs (autonomous NPOs, foundations, private establishment, associations, Cossack society, minority communities), public associations (public organisations and social movements), and religious organisations and charitable organisations. This sectorial risk assessment confirms the overall low level of TF risk faced by the NPO sector, but notes that the NPOs most vulnerable of TF abuse are foundations, public organisations and religious organisations, as their activities are more associated with fundraising. Some vulnerabilities faced by the sector were also identified, including the collection of funds other than through bank accounts (e.g. personal bankcards, e-wallets). Moreover, the sectoral risk assessment specifically noted that charities pose a medium risk for TF as they often collect funds in cash or using e-wallets, not bank accounts, and because there is currently no guidance related to collecting cash through donation boxes.

369. Russia applies uniform TF risk mitigation measures on all NPOs, with additional measures applied to charitable organisations. Specifically, Russia's 212 000 NPOs are obliged to register with the MoJ. Documents required to establish an NPO are also sent to the government registration authority for inclusion in the USRLE. Information included in the register is publicly available through the FTS website, as well as the MoJ's NPO Information Portal, where information on the content of NPO annual reports is also available. Russian NPOs must also maintain accounting and statistical records, and keep records of transactions with funds received from foreign sources. All NPOs are also required to report on activities conducted, members of their management board and purposes for which funds are spent. This data is all publicly available.

370. Regarding charitable organisations, which are considered as posing a medium-level of risk, different requirements apply. In addition to the above general requirements for all NPOs, charitable organisations must submit annual reports on their financial and economic activities, confirming compliance with the requirements on the use of property and expenditure of funds; the composition of the highest governing body; the composition and content of charitable programs; the content and results of the activities; any violations of the legal requirements identified as a result of inspections carried out by tax authorities and measures taken to eliminate them. This report is submitted to the MoJ in the same period as the annual report on financial and economic activities submitted to the tax authorities. Additionally, information about the size and structure of incomes of charitable organisations, as well as information about the size of their property, expenses, number of employees, their remuneration and the involvement of volunteers are publicly available.

371. While not in effect at the time of the on-site visit, Russia is considering additional safeguards to protect NPOs from potential TF abuse. This includes establishing a register of payment details that public associations, religious organisations and other NPOs use to collect money; a new federal law to consolidate the prohibition for designated persons by the IAC CFT to act as founders directors, participants and members of NPO; and a specific procedure for collecting cash using donation boxes.

372. However, the NPO TF risk assessment needs to incorporate more granular information identifying the features and types of at-risk NPOs within the legal forms rated as medium-risk [i.e., information on the parameters of risk-assessment, such as the number and types of registered entities, data on the founders, members and participants (including the BO), amount of assets under control, number and amount of significant financial transactions, sources of donations and directions of expenditures], as well as the findings of supervision for different types of higher TF risk NPOs to enhance its utility for public and private users".

Outreach to the sector and its understanding of the risk

373. Russia has conducted outreach to enhance the sector's understanding of TF risks and vulnerabilities. After the publication of the NPO sectoral risk assessment, events were held in different regions of Russia to highlight current trends, risks, and ways to prevent the abuse of NPOs for TF purposes. The NPOs interviewed during the on-site visit were aware of the NRA's findings and confirmed regular and constructive dialogue with Rosfinmonitoring, the MoJ and within the sector itself. The NPOs met by the assessment team participated in the NRA and agreed with its results.

374. Rosfinmonitoring also compiled a document, entitled "CFT Recommendations for NPOs", which is publically available to all NPOs. This document includes relevant FATF reports on how NPOs can protect themselves from potential TF abuse. The sector also organises annual workshops, roundtables and meetings where authorities engage directly with NPOs. The topics of seminars and other events held for NPOs addressed a wide range of issues. For example, in September 2018, the MoJ office in one of the federal districts held a seminar on CFT with leaders and representatives of NPOs registered and operating in this region. Recommendations were provided to the attendees in order to raise awareness of the TF risks faced by the sector.

Oversight and actions taken

375. The MoJ supervises the sector for the requirements outlined above. Supervision occurs at the regional level by MoJ regional offices, and includes risk-based inspections. Inspections occur on a scheduled and ad hoc basis, with the schedule for regular examinations published online and endorsed by the GPO. Ad hoc inspections are prioritised over scheduled inspections.

376. Risk indicators for ad hoc (i.e. unscheduled examinations) are based on publicly available information about a particular NPO, as well as information provided to MoJ from Rosfinmonitoring, the GPO and LEAs. This information contains information about potential violations of legal requirements by NPOs. The information may include data on the financial and economic activities of NPOs, its employees and managers, events held, published literature, as well as incompleteness and/or inaccuracy of information on financial transactions.

377. The below table outlines the number of ad hoc and scheduled inspection over the last five year. Nearly 10% of all recent inspections took place on an ad hoc basis.

Table 4.9. Number of NPO Inspections

	2013	2014	2015	2016	2017	2018
Ad hoc inspections	164	621	380	359	429	304
Scheduled inspections	6229	5740	5741	5182	4636	4323

378. While conducting inspections, MoJ employees verify that the founders/members/employees of the NPO are not included in Russia's domestic or international lists; that the stated objectives of the NPO corresponds with its activities; and, the true beneficiaries of the NPO's activities are as stated.

379. Between 2015 and 2018, while conducting inspections of NPOs, the MoJ identified 22 persons (in 21 NPOs) who were domestically designated as terrorists and were employees of NPOs. Most NPOs excluded the designated person from the board of directors when it was revealed that they were a listed person. Based on these inspections, 5 individuals were removed from 5 NPOs, and 16 NPOs were dissolved as a result of the ad hoc inspections conducted by the MoJ and for failing to comply with the MoJ's warning to remove the designated persons from their position within the NPO. In such cases, the MoJ has petitioned the court for the dissolution of the NPO (see case study below).

Box 4.10. LEA Referral Leading to Action Against NPO

In 2016, LEAs identified individuals involved in the activities of terrorist organisations, including persons suspected of participating in ISIL.

Rosfinmonitoring provided financial and other information on these individuals to LEAs, which resulted in a TF case in 2017. The person involved was the head of a regional NPO. Rosfinmonitoring provided information to the MoJ to organise an unscheduled inspection. As a result of this inspection, the NPO was ordered to remove this person from the management of the NPO.

Due to persistent non-compliance with this requirement (i.e. two notifications sent to the NPO), the MoJ appealed to the court to dissolve the NPO. In August 2018, the NPO was dissolved.

Deprivation of TF assets and instrumentalities

380. Russia deprives terrorists of their assets and instrumentalities as a policy objective as demonstrated by recent national strategies, plans, and various interagency and intra-agency documents. These products oblige LEAs, prosecutors, and the judiciary to carry out seizure and confiscation for ML, TF and predicate offences (see IO.8)

381. Russia has demonstrated to a large extent that it deprives terrorists, terrorist organisations and terrorist financiers of assets and instrumentalities through various approaches, such as through terrorist designations, administrative freezes, court orders, and confiscation. While the total amount and value of assets and

instrumentalities deprived is low, it is consistent with Russia's risk profile, since the majority of terrorists and financiers/facilitators subject to deprivation measures are self-financing FTFs from relatively poor backgrounds and with limited funds available. Russian authorities explained that the measures used have an important disruptive effect, even when the amount of funds deprived is small.

382. As noted above, Russia actively uses its domestic terrorism designation powers to deprive terrorists, extremists and terrorist organisations of funds. In total, Russia has frozen over RUB 36 000 000 (EUR 491 000) worth of assets within 4 000 accounts belonging to domestic terrorists, extremists and their organisations. Russia is unable to disaggregate statistics on assets frozen for their connection to terrorists and extremists. As a result, it is unclear to the assessment team how much is frozen precisely in relation to those designated pursuant to UNSCR 1373, versus those related to extremism. That said, the below case example illustrates a domestic terrorism designation that resulted in a freeze of approximately EUR 18 240 in four accounts.

Box 4.11. Domestic Designation Instead of TF Prosecution

In 2012, Mr. S was prosecuted for committing crimes of terrorist nature, in particular for public calls for terrorist activities, public justification of terrorism and propaganda of terrorism as editor of a paper "Radical politics". As a result, in 2012, Mr. S was added to Russia's domestic list, resulting in freezing obligations. In April 2014, Mr. S was sentenced to imprisonment for seven years, including a restriction to carry out journalistic activity for five years. As of September 2018, about RUB 1.3 million (EUR 18 240) were frozen in four accounts

383. Russia has only frozen one account belonging to a UN-designated person, totalling RUB 400 000 (EUR 5 560) in 2018 (see Box 4.11). The annual increase to this one account, relates to incoming pension payments, the funds in this account are not accessible. The affected person has not sought an exemption to access these funds.

384. The breakdown of amounts frozen under Russia's domestic designation regime is below. This data includes assets frozen in relation to those designated for extremism, in addition to terrorism.

Table 4.10. Amount Frozen Related to UNSCRs 1267/1988/1373 (per year)

Assets frozen (RUB)	2013	2014	2015	2016	2017	2018
National list designation	14 mln.	25 mln.	33 mln.	24 mln.	15 mln.	26.4 mln.
IAC* domestic designations	n/a-	n/a-	n/a-	4.2 mln.	5 mln.	10 mln.
Total Frozen (EUR)	196 000	349 000	461 000	394 000	279 000	509 000
International list (i.e. UN list) (EUR)	0	0	1 700	4 000	5 500	5 600
Total	196 000	349 000	462 700	398 000	284 500	514 600

Note: The IAC was established in November 2015 and began operating in January 2016.

385. Russia has also frozen assets through the mechanisms, referred to as the 5+30 day administrative freeze (see IO.9). As noted above, assets of a person or group may be temporarily frozen by Rosfinmonitoring, LEAs and FIs when there is a suspicion that the entity is acting on behalf or under control of a designated person or group. The freeze initially lasts for 5 days but may be extended up to 35 days in order for LEAs to conduct investigations. If the grounds for suspicion are confirmed, LEAs may apply for a court order for the indefinite continuation of the freeze (or, potentially, IAC CFT designation may be sought).

Box 4.12. 5+30 Day Administrative Freeze

In October 2017, Rosfinmonitoring received a report from bank A on suspending a transaction of RUB 46 000 for five days. The transaction related to the cash withdrawal from the bank account of LLP "NS" whose director/founder was a domestically designated person for terrorist activity.

Within this five-day period, Rosfinmonitoring verified this information in co-operation with LEAs and issued a decision to suspend the transaction for an additional 30 days.

Within this 30-day period, LEAs carried out intelligence activity in order to establish the ultimate goal of this transaction, including the possibility of the use of the funds by designated persons. No signs of illicit activity was discovered, so the bank was informed to carry out the transaction.

386. From 2016 to 2019, this 5+30 days administrative freeze was applied by Rosfinmonitoring 13 times with respect to 19 individuals. This resulted in three persons being domestically listed, with a total amount of frozen funds of approximately EUR 5 600. In addition, the assets of 13 individuals were frozen by IAC CFT decision (total amount of frozen funds approximately EUR 5 600); and a transaction of one person was suspended upon court decision. Finally, suspicions were not confirmed with regard to two individuals

387. As noted under IO.8 and IO.9, Russia demonstrates that it seizes and confiscates small amounts of money and instrumentalities in TF cases. In a survey of 1

600 judicial decisions issued between 2013 and 2017 in terrorism cases, instrumentalities were confiscated frequently. In 97 terrorism judgments dealing with 137 individuals, 14 vehicles and 110 electronic devices were confiscated. In 10 TF judgments dealing with 13 individuals, 1 vehicle and 10 devices were confiscated. The equivalent of EUR 7 557 was confiscated in TF cases in 2017 and approximately EUR 6 000 was confiscated in 2018.

Box 4.13. TF Seizure and Conviction

In 2017, credit institutions filed a report to Rosfinmonitoring on an attempted transaction to the amount of RUB 300 000 by a legal entity under control of a designated person. This person was the only founder, director and employee of the legal entity used for shadow cashing-out schemes. The FSB established that he transferred part of his income to his brother who was fighting in Syria and purchased on airline tickets for those who travelled to the territory under ISIL control. As a result, the legal entity's accounts were frozen for 35 days.

During the suspension period, other legal entities under his control or under the control of his family members were established as participants of a shadow scheme. As a result of this work, all transactions including of legal entities were frozen.

Consistency of measures with overall TF risk profile

388. The measures undertaken by Russia are mostly consistent with its overall TF risk profile. As evidenced above, Russia actively domestically designates terrorist persons and groups pursuant to UNSCR 1373. However, in comparison, Russian proposes only a small number of designations to the UN, which would extend freezing requirements to all member states. Russia states that when considering the preparation of a request to the relevant UN Security Council committees, competent authorities conduct an analysis of possible routes for the movement of persons and possible channels for their financing. If there is information about specific countries whose territories or financial system are used by terrorists, requests for mutual freezing are sent to these countries, while in other cases, requests are sent to the relevant UN Security Council committee. However, based on the statistics on outgoing UNSCR 1373 requests, Russia has only made one request (containing over 400 names) to several countries. Thus, the assessment team believes that Russia should have more outgoing bilateral requests for designations and/or more proposals to the UN given the size of its domestic terrorist list. Indeed, this would have more significant international effects.

389. While the vast majority of Russian NPOs pose little to no TF risk, Russia has identified the subsector of those charities as most vulnerable to TF abuse, and places additional requirements on these entities. Appropriate action is taken to engage the most vulnerable NPOs and an outreach and inspection program is in place.

390. Based on the terrorism and TF cases reviewed, it is evident that Russia freezes, seizes, and confiscates terrorist assets and instrumentalities as a policy objective and in line with its risks. For example, as recognised by the NRA, one of the

main threats in Russia comes from illegal armed groups operating in the North Caucasus, which pose a diminishing, but still existent TF threat for Russia. A relatively small amount of proceeds have been seized and confiscated in relation to these groups. However, based on interviews with authorities, the assessment team discovered that judges often find such defendants impoverished and confiscation impossible. As a result, although the total value is low, it appears that confiscation in this area is in line with the overall TF risk profile. Moreover, Russia demonstrated that it was actively depriving terrorists and terrorist groups of assets based on the other TF risks noted in the NRA, notably FTFs travelling/returning to and from conflict zones, or terrorists raising and moving funds via the internet.

Overall conclusions on IO.10

391. Russia demonstrates its ability to implement TFS within the context of UN designations, national designations and in response to requests from third countries to take freezing actions pursuant to UNSCR 1373. However, an important deficiency exists regarding the timeliness of UN TFS implementation, through enforceable means. Furthermore, the obligation to implement TF TFS does not apply to all natural and legal persons. The AML/CFT law does not contain any specific penalties for natural and legal persons who contravene the TFS requirements. Russia would apply its TF offence that, however, does not cover the obligation to freeze. Obliged entities require additional outreach to clarify the different terrorist/extremist lists and related exemption requirements since confusion was observed during the onsite. Moreover, given the high number of FTFs travelling from and through the country, Russia has so far submitted relatively few proposals to the relevant UN Committees and third countries for listing consideration. In regard to NPOs, Russia has not completed a detailed analysis to identify the features and types of at-risk NPOs within those legal forms rated as medium-risk.

392. Russia is rated as having a moderate level of effectiveness for IO.10.

Immediate Outcome 11 (PF Financial Sanctions)

393. In terms of context for PF, Russia shares a border with the DPRK, and the two countries share a long-standing bilateral relationship focused on trade. In previous years, over 30 000 workers from the DPRK resided in Russia. As of March 2019, less than 4 000 DPRK workers continued to be employed in Russia and are expected to be repatriated in due course.

394. Russia and Iran share a long-standing bilateral relationship and trade relations. Russia is not an international financial centre or a trade and transhipment hub, nor is it a significant centre for the formation of international companies.

395. Russia has a significant high-technology manufacturing sector, producing proliferation-sensitive goods and materials. Nevertheless, although outside the scope of this assessment, Russia applies an export and technical control regime for trade in relevant goods and to ensure compliance with UN sanctions, and applies measures for control of the underlying financial transactions related to possible proliferation-related activities.

Implementation of targeted financial sanctions related to proliferation financing without delay

396. The mechanisms in place for the implementation of PF TFS are the same as those outlined in IO.10, related to the UN TFS regime for TF. However, Russia introduced PF TFS obligations for FIs and DNFBPs by amending the AML/CFT Law on 23 April 2018 (entered into force in July 2018), whereas the TF TFS requirements are more established given that they were introduced on 8 June 2013.

397. Russia has an inter-agency policy to consider designating persons and groups with respect to UNSCRs 1718 (related to the DPRK) and 1737/2231 (related to Iran) and their successor resolutions, with the MFA leading the process. An internal (classified) regulation, which was reviewed by the assessment team while onsite, establishes how relevant authorities cooperate prior to the submission of a designation by the MFA to the relevant UN Committee via Russia's Permanent Representative to the UN. According to this regulation, prior to submitting a designation proposal to the UN, the MFA holds a round of consultations with relevant authorities—including Rosfinmonitoring, LEAs and the Ministry of Defence—to corroborate details of the case, ensure that the proposal conforms with the rules of the sanctions committees (i.e. templates, terms of reference, etc.), and requests additional information where necessary. Classified intelligence may also be used in this process, when appropriate.

398. While this procedure for referring PF designations to the UN exists and is understood by authorities met by the assessment team, it has never been used in practice. Indeed, Russia has yet to propose a designation to the relevant UN Committees related to PF TFS.

399. As outlined in the TC Annex, under the Constitution of the Russian Federation, international treaties (including UNSCRs) are a component of the legal system without the need for a separate act of implementation. However, the relevant UNSCRs do not include all the elements required to be enforceable means under the FATF Standards. The AML/CFT Law, while requiring immediate freezing, does not indicate the moment when such an obligation arises. Instead, it sets the deadline for the implementation of the relevant UNSCR requirements to the publication of UN decisions on the Rosfinmonitoring's website. This gives rise to a risk of delayed implementation of freezing obligations which is not in line with FATF requirements. Under such interpretation of the law, the enforceable obligation to implement PF TFS occurs as a result of Rosfinmonitoring publishing UN listing decisions on its official website (www.fedsfm.ru/documents/omu-list). The requisite freezing obligations by all FIs and DNFBPs enter into force within 24 hours of this publication. As a result, funds could be frozen two days after a decision is taken by the UN. However, as illustrated in the table below, Russia published all of the relevant UN PF TFS designations to its list on 7 November 2018, which is four months after Russia's PF TFS legal requirements entered into force (July 2018) and three months after the latest update of the 1718 Committee in August 2018. This assessment team is concerned by the significant delay in the publication of the UN PF TFS lists, and notes that, in practice, PF TFS is not occurring without delay. The assessment team also notes that Russia holds a permanent position on the UN Security Council and is therefore aware of upcoming UN designations. This position should allow Russia to reduce its publication delay, in practice, enabling Rosfinmonitoring to publish the new decisions as soon as they are officially adopted at the UN.

Table 4.11. Russian Publications of UN Designations (UNSCRs 1718/2231)

UNSCR List	Date listed by UN	RFM Publication	Delays
1718	08/08/2018	7/11/2018	93 days
1718	09/07/2018	7/11/2018	Approx. 4 months
1718	23/05/2018	7/11/2018	Approx. 5 months
1718	30/03/2018	7/11/2018	Approx. 7 months
2231	17/01/2016	7/11/2018	Approx. 3 years

400. Rosfinmonitoring plays an important role in the communication of TFS obligations and raising awareness to FIs and DNFBPs. Reporting entities are proactively alerted of any changes to the UN and domestic TFS lists via their Personal Account, which also includes updated lists available for download. For DNFBPs who do not yet hold a Personal Account, the publication on Rosfinmonitoring's website serves as notification. Furthermore, once a month, any changes decided at the UN are published in the Official Gazette (Rossiyskaya Gazeta).

401. As noted in R.7, the obligation to implement PF TFS does not apply to all natural and legal persons, but only reporting entities since there are no provisions that explicitly provide for liability for infringing the prohibition by all natural and legal persons (other than FIs and DNFBPs). Russia asserts that its Constitution establishes an automatic incorporation of all UN Chapter VII decisions into domestic law by virtue of article 15(4).[49] However, this article is not considered as legally enforceable by the assessment team (see R.7 TC Annex). In terms of demonstrating effectiveness, Russia has no cases which could demonstrate the ability to penalise a natural or legal person who violated the TFS measures under UNSCRs 1718 or 2231, through the use of the relevant article of the Constitution or any other law.

402. In addition to the aforementioned measures related to PF TFS, Russia implements import/export obligations for dual use goods through a whole-of-government approach, via a working group on CPF (includes representation from Rosfinmonitoring, FCS, Federal Service for Technical and Export Control, MoI and the BoR). This Group meets to discuss operational issues related to possible instances of sanctions evasion. The group meets on an ad hoc basis, when deemed necessary. Since its establishment in 2018, the working group met two times. Items discussed are confidential and were not provided to the assessment team. Russia provided the assessment team with numerous cases studies in relation to violations of the import/export regime. While this demonstrates coordination amongst authorities to identify and disrupt non-financial sanctions evasion, it falls outside the scope of the FATF Standards.

[49] Article 15(4) of the Constitution states: "The universally recognised norms of international law and international treaties and agreements of Russia shall be a component part of its legal system. If an international treaty or agreement of Russia establishes other rules than those envisaged by law, the rules of the international agreement shall be applied."

Identification of assets and funds held by designated persons/entities and prohibitions

403. Since July 2018, FIs and DNFBPs are required to report to Rosfinmonitoring if they hold funds of individuals or entities designated under PF TFS authorities. During the last five years, Russia has frozen accounts related to one person listed pursuant to UNSCR 1718 and its successor resolutions (DPRK). However, since this freeze occurred prior to the entry into force of the legal requirements, the FI that took freezing measures did not notify any Russian authorities (MFA, BoR, or Rosfinmonitoring). The details of this case are presented in the box below.

Box 4.14. Assets Frozen Related to UNSCR 1718 (DPRK)

Mr. Han Jang Su was listed pursuant to UNSCR 1718 by the UNSC on 5 August 2017. Russia states that at this time Mr. Su was employed as a diplomat at the DPRK Embassy in Moscow.

Russia states that on the same day of the UN designation, a Russian FI identified three accounts, totalling RUB 2.2 million (approx. EUR 30 700), belonging to a Mr. Han Jang Su, and took immediate action to freeze these accounts. Given that there was no requirement to notify Russian authorities of the freeze at that time, the assessment team could not review any notifications by the FI to verify that this freeze occurred on the same day as the UN designation.

On 20 February 2018, Mr. Su attempted to access his frozen accounts but was rejected.

On 25 April 2018, upon request of Mr. Su, the MFA applied to the UN 1718 Committee for an exemption to access some the frozen funds for basic living expenses. The exemption was not granted by the UN 1718 Committee.

These funds are currently still frozen. Russia states that Mr. Su does not have any other bank accounts in Russia, and is still employed at the DPRK Embassy in Russia.

404. As noted in IO.6, STRs may be classified by reporting entities based on the nature of the underlying suspicion, which is assigned a particular classification code. In 2018, PF TFS was attributed a code by Rosfinmonitoring that indicates a possible PF TFS evasion. As of the end of the on-site visit in March 2019, no reporting entity has assigned this code to a STR. Rosfinmonitoring also monitors STRs received from FIs and DNFBPs related to the FATF's call for countermeasures.

405. As noted in IO.10, Russia has a mechanism in place to administratively freeze accounts for five days, which can be extended to a total of 35 days (i.e. the 5+30 day freeze), when there is a suspicion that a transaction relates to a designated person or group. While this mechanism equally applies to PF TFS, it has not yet been used in relation to PF TFS by Rosfinmonitoring, LEAs, FIs or DNFBPs. Moreover, the FCS reviews all cross-border transactions in relation to the movement of goods across the

border of the Russia and can use the 5+30 administrative freeze when there is a suspicion that a transaction relates to a designated person. The FCS has also never used this mechanism.

FIs and DNFBPs' understanding of and compliance with obligations

406. Similar to IO.10 and IO.4 in relation to TF TFS, larger FIs and DNFBPs have a good understanding of their PF TFS obligations in general and have effective controls in place with respect to sanctions implementation, relying on communication through the Personal Account and commercial screening databases. Smaller FIs and DNFBPs, on the other hand, have less mature controls in place and may need to manually screen their client base.

407. All private sector entities met during the on-site visit were aware of their PF TFS obligations as well as the possibility, in the case of suspicion, to suspend a transaction for up to 35 days in order to request Rosfinmonitoring to conduct financial analysis and verify the ground for suspicion. Obliged entities were also aware of their obligations to screen new clients during on-boarding and existing clients every three months.

408. During the on-site visit, Russia amended L115 to introduce an explicit freezing obligation for lawyers, notaries and accountants. Although this is a new measure, the assessment team confirmed with a sample of the sector that it was indeed implementing TFS (both TF and PF TFS) prior to this explicit legal obligation entering into force.

409. One challenge to effective implementation of PF TFS is whether FIs/DNFBPs properly identify the ultimate BO of a customer or party to a transaction. As noted in IO.4, the understanding regarding the identification of BO amongst reporting entities is uneven. Most entities heavily rely on the controlling ownership criterion and, if doubts arise whether this criterion is sufficient to determine BO, disregard the person that, through other means, may control the legal entity. This deficiency impacts TFS implementation, and could result in instances of sanctions evasions through legal persons and arrangements. Legal persons feature more often as targets for designation under UNSCRs 1718 or 2231 than under TFS related to terrorism, and this issue is therefore a more significant obstacle to effective implementation of TFS in the context of IO.11 than it is in the context of IO.10.

Competent authorities' monitoring and ensuring compliance

410. The BoR issues information letters to clarify PF TFS obligations to their reporting entities. Over the last five years, the BoR issued 11 letters to FIs, which were also published on its website. For example, a letter issued in May 2017, informs reporting entities of their obligations pursuant to UNSCR 2231. Specifically, this letter states that each diplomatic mission and consular office of the DPRK, as well as each accredited DPRK diplomat and employee, are prohibited from opening more than one bank account. Moreover, the FATF 2018 guidance on implementation of PF TFS was translated into Russian and provided to relevant stakeholders via Rosfinmonitoring's website.

411. In addition to publishing the relevant UN lists on PF TFS, Rosfinmonitoring communicates information to reporting entities about TFS via the Personal Account.

For example, on 1 March 2019, Rosfinmonitoring published an information letter on TFS obligations for lawyers, notaries and accountants, which included PF TFS. The assessment team notes that this letter merely reiterates the legal provision set out in the AML/CFT law, and does not provide detailed guidance.

412. Rosfinmonitoring also provides clarifications to reporting entities on the legal requirements and practical implementation of PF TFS. Over the last five years, Rosfinmonitoring processed more than 50 inquiries from reporting entities regarding PF TFS, the majority of which concerned clarifications of the obligations and legislation. Some inquiries related to translation of the list into Cyrillic, and requests by the private sector for Rosfinmonitoring to communicate the whole PF TFS list with comprehensive basic information. These inquiries were used by the Russian authorities to develop and implement the 2018 PF legislative regime for PF TFS.

413. The assessment team is of the view that reporting entities' awareness of their PF TFS obligations could be improved through the introduction of more detailed guidance on the practical implementation of the PF TFS requirements.

414. While supervisors consider PF TFS during the course of their offsite and onsite inspections, no PF TFS-related violations have been identified. The lack of identified violations could be attributed to the relative recentness of Russia's PF TFS regime.

Overall conclusions on IO.11

415. Given that Russia's PF TFS regime under the AML/CFT Law is relatively new (entered into force in July 2018), Russia has demonstrated a moderate level of effectiveness. The practical mechanisms in place for implementation of PF TFS are the same as those related for UN-related TF TFS. The assessment team notes that major improvements are needed, especially in light of the delays to publish the PF TFS lists after Russia's legal requirement entered into force, and three months after the latest 1718 Committee publication; and the fact that there are no explicit penalties for natural and legal persons (beyond FIs and DNFBPs) who contravene the PF-related TFS requirements. Nevertheless, Russia has frozen assets in relation to one person listed on UNSCR 1718, and its successor resolutions, thereby achieving this IO to some extent.

416. Russia is rated as having a moderate level of effectiveness for IO.11.

CHAPTER 5. PREVENTIVE MEASURES

Key Findings and Recommended Actions

Key Findings

Financial institutions

1. The understanding of ML risks is generally good among the financial sector's institutions interviewed, especially larger banks, including those belonging to international groups, securities market participants and insurance companies. Regional banks and MVTS providers have an uneven understanding of risk. Consumer credit co-operatives risk understanding is not considered to be in line with the risk identified in the ML NRA. TF risk is understood to a lesser extent, to which the NRA contributes only to a limited extent, given its high-level nature.
2. FIs met have procedures in place to identify, assess, understand and document their individual risks, including a periodic risk assessment exercise.
3. FIs met seem to have implemented adequate mitigation measures, by profiling customers based on ML/TF risk and applying adequate measures for CDD, record-keeping and monitoring.
4. On the identification of BO, overall there is a fair level of implementation of the requirements among FIs, but some seem to apply a rules-based definition of BO (i.e. identifying senior management officials as soon as no natural person is identified as owning 25% or more of legal persons), which may be a consequence of a superficial understanding of the definition of BO, in particular regarding complex structures.
5. FIs have an adequate understanding of specific high-risk situations through publicly available information, and take additional measures, particularly in relation to PEPs and higher risk countries. However, there are moderate technical deficiencies in R.12, in a matter of high risk in light of the NRA, which may not ensure a consistent application of mitigating measures across the sector.
6. Large banks are aware of legal requirements relating to TFS, and implement these without delay. However, there may be confusion among some sectors due to the mix of UN and domestic lists, which actually hinder prompt asset freezing.

7. STR requirements are generally understood by FIs. However, the STR system involves a low level of suspicion, based on a list of predefined set of indicators (see IO.6) and the high figure of indicator-based STRs. Given the system in place, the number of STRs filed is in accordance with the risk level of CIs, particularly banks.
8. CIs seem to prefer to file STRs at an early stage, generally without conducting a thorough and deep analysis of the transaction prior to such filing. This may impede the system from benefiting from the added value of the knowledge FIs hold of their customers.
9. Entities met demonstrated that adequate internal control policies and procedures are in place.
10. Until the on-site visit, Russian FIs pertaining to international groups could not share information within the same group for AML/CFT purposes relating to customers, accounts, transactions, analysis of transactions or activities which appear unusual and related STRs.
11. Under the relevant period of assessment, non-compliance by the overall sector – as opposed to the entities met during the on-site – worries the assessment team, particularly the organisation of internal controls, CDD and record-keeping obligations, although compliance has been improving in recent years.

Designated Non-Financial Businesses and Professions

1. The understanding of risks by DNFBPs met, as a whole, is fair. Certain sectors have a good understanding (e.g. accountants and auditors). Others have a less developed (casinos, real estate agents) or superficial (lawyers and notaries) risk understanding. DPMS risk understanding is not considered to be in line with the risk identified in the ML NRA.
2. DNFBPs rate customers based on ML/TF criteria and apply CDD and EDD measures accordingly.
3. All DNFBPs the assessment team met were aware of the obligation to identify and verify the identity of the BO, but their understanding of how to comply with this obligation is uneven and superficial.
4. While DNFBPs are aware of their obligation to report suspicious transactions, only some of them are filing an adequate amount of STRs (DPMS and real estate agents).

Recommended Actions

1. Russia should ensure that DNFBPs periodically (re-)assess their individual ML/TF risk.
2. Russia should enhance the understanding of ML/TF risks and ensure adequate implementation of AML/CFT obligations of those obliged entities not adequately supervised for AML/CFT purposes, including legal professionals.

3. Russia should enhance the understanding and implementation of BO requirements, particularly with regards to medium and small size banks and other FIs, as well as DNFBPs.
4. Given Russia's risk profile, it should continue to actively interact with obliged entities regarding the identification of domestic and foreign PEPs, their close associates and family members as well as implementation of AML/CFT obligations, such as EDD, STR filing and refusal to conduct transactions or establish business relationships.
5. Russia should further raise awareness amongst non-bank institutions and DNFBPs of the STR filing obligation and its implementation in line with the identified ML/TF risks, trends and typologies. Russia should also ensure that FIs, notably credit institutions, enhance the thoroughness and depth of analysis of non-indicator based STRs in order to ensure good quality.
6. Rosfinmonitoring should adjust its internal systems to allow FIs and DNFBPs to classify an STR as urgent and requiring immediate attention by Rosfinmonitoring analysts, thereby distinguishing it from the significant number of STRs automatically reported to Rosfinmonitoring each day. Rosfinmonitoring should provide additional feedback to reporting institutions regarding the basis or the level of suspicion associated with each STR or group of STRs.
7. Russia should ensure that obliged entities implement TFS and freeze assets without delay, including by actively engaging with them and further clarifying the distinct requirements under UN and domestic lists.
8. Russia should further enhance its legal framework regarding intra-group information sharing.

417. The relevant Immediate Outcome considered and assessed in this chapter is IO.4. The Recommendations relevant for the assessment of effectiveness under this section are R.9-23.

Immediate Outcome 4 (Preventive Measures)

418. The assessment team weighted the implementation of preventive measures most heavily for credit institutions, highly for consumer credit cooperatives and microfinance companies and DPMS, moderately for the securities, real estate, MVTS services, payment acceptance services sectors; and less heavily for the remaining sectors (lawyers, notaries, legal professionals, accountants, and TCSP services, insurance sector, private pension funds, mutual insurance companies, casinos, mutual investment funds, investment fund management companies), based on the relative materiality and risk in the Russian context.

419. The assessment team's findings on IO.4 are based on interviews with a range of private sector representatives; review of internal procedures and documents; data and statistics from supervisory activities; discussions with supervisors; data on STRs and discussions with the FIU.

420. The assessment team was able to meet only a small number of supervised entities from each of the relevant sectors – e.g. assessors interviewed five banks out of a total of more than 484 active in Russia on 1 January 2019. While every effort was made to include a range of different entities (e.g. international and domestic, national and regional, large and medium), it is impossible to fully reflect the diversity of the sector in the context of the evaluation. Thus, information on breaches was also relied upon in order to better convey the level of compliance of each sector as a whole. For instance, the BoR informed the assessment team that, in 2017 and 2018, 40% and 14% of the total number of breaches committed by CIs, respectively, were found in high-risk institutions, around 30% of those considered to be major breaches by Russian authorities in both years.

421. In addition, the findings in IO.3 regarding supervision of the financial sector have significant implications for the analysis of IO.4, since weaknesses in supervision will affect the extent to which the BoR and other supervisors are identifying all breaches to the AML/CFT requirements.

Understanding of ML/TF risks and AML/CFT obligations

FIs and DNFBPs

422. Large banks show a good understanding of their ML risks, in particular those which are part of international financial groups. Large securities, insurance and microfinance companies were also able to demonstrate a good level of risk understanding. These obliged entities have a track record of risk assessment and understanding which is not confined to the assessment at a national level conducted in 2017-2018. This understanding derives from internal procedures that mandate entity-wide risk assessment on regular basis. Banks that are part of international groups primarily focus on group-wide risks, although they show a good knowledge of Russian-specific risks as well. Understanding of risk demonstrated by other FIs, namely regional banks and MVTS is uneven and not as advanced as that of major players in the sector. However, it is considered to be generally commensurate with their risk exposure. Consumer credit co-operatives risk understanding is not considered to be commensurate with the risks identified in the ML NRA.

423. DNFBPs met demonstrate a fair, although uneven, level of understanding of the ML/TF risks, which mostly derives from the findings of the 2018 NRAs and not primarily based on the consideration of their specific exposure through their customer-base or business lines. DNFBPs consider the findings of the national exercises to be useful and accurate in relation to the different sectors, albeit relatively high-level. Certain sectors have a more advanced understanding (e.g. accountants and auditors), while others have it less developed (casinos, DPMS, and real estate agents). Lawyers, legal professionals and notaries presented only a superficial understanding of the ML/TF risks to which they are exposed. The DPMS sector risk understanding is not considered to be commensurate with the risks identified in the ML NRA, while its level and granularity needs to be improved.

424. The main risks and typologies identified by the FIs and DNFBPs interviewed are consistent with the ML NRA (e.g. use of fictitious companies, corruption, cash transactions and electronic means of payment). The ML NRA is considered a useful exercise, having benefited from broad inclusion of the private sector and is well known,

although some entities with more advanced understanding indicated that its conclusions only confirmed what they already knew about ML risks. This may indicate that the NRA may have limited added value in increasing the ML risk understanding of some reporting entities.

425. All FIs and most DNFBPs have a risk-classification of their individual customers based on various risk factors related to customers, products, geographical location and distribution channels. The authorities have provided instructions[50] as to how to classify the ML/TF risk of customers and transactions. For example, reporting entities would consider as high risk customers or BO who are PEPs, legal persons registered at the same address where other legal persons are registered, customer and (or) the BO included in the list of organisations and individuals in respect of which there is information about their involvement in extremist activities or terrorism. Moreover, different from DNFBPs, FIs determine risk mitigation measures for identified inherent risks and periodically re-assess the adequacy of controls implemented to mitigate risks.

426. TF risk understanding varies widely across the private sector. Similar to the ML NRA, there was broad inclusion of the private sector in the TF NRA. FIs and DNFBPs have been made aware of results of the TF NRA through the Compliance Council and its publication. Nevertheless, the published NRA is high-level and does not provide granular information about specific threats in each sector. Among the activities which private sector firms are instructed to consider higher risk are charities, which is not in line with the TF NRA findings that charities are at moderate risk for TF (with the whole NPO sector considered low risk). The authorities explain this with the intention of closely monitoring charities due to their inherently high TF risk exposure. It should be noted that the level of risk understanding (and level of engagement with authorities) is significantly higher among the largest banks: Rosfinmonitoring has developed detailed typologies to identify possible TF-related transactions in co-operation with 11 large banks, and plans to expand the use of these typologies to other FIs, as set out in the analysis of IO.6.

427. Russia established the Compliance Council in 2016, a body composed at national level by the representatives of the largest FIs and DNFBPs (over 100 members) and with regional sub-groups operating in all federal districts. It is intended to increase risk understanding and awareness across sectors, share new ML/TF typologies and develop new signs of suspicious transactions in order to provide guidance to FIs. This is the principal forum for dialogue between authorities and the private sector, which is found to be a useful platform by all stakeholders.

428. All reporting entities interviewed have a satisfactory understanding of their AML/CFT obligations. FIs have shown a good understanding of their obligations and seem to have developed a mature state of implementation. FIs are particularly aware of CDD, EDD, and of their STR filing obligations (following frequent and significant fines in cases of non-compliance). DNFBPs also demonstrate a fair understanding of their AML/CFT obligations, although not as well developed as FIs.

[50] By way of the following instructions: BR 375 in 2012; BR 445 in 2014; RFM 103 in 2002, all in force

Application of risk mitigating measures

429. FIs have established internal controls and systems in order to mitigate risks. These systems allow them to conduct customer and transaction risk assessment based on different criteria (generally risks related to the product, geography and type of customer) and attribute different risk scoring-grades. There are generally three grades (high, medium and low), which allows FIs to apply targeted mitigating measures entailing different approaches to scrutiny and different degrees of intensity. Customers rated higher risk generally require approval from more senior personnel in the compliance department and closer on-going monitoring in the back office. Breaches in this regard are mostly related to technical violations (i.e. the untimely updating of risk assessment programs in internal control rules) and are not significant in the financial sector. DPMS and real estate agents stand out as less compliant sectors although the trend of non-compliance is decreasing.

430. In order to mitigate certain identified risks, Rosfinmonitoring and BoR communicate typologies of behaviour to obliged entities, either by circulating methodological recommendations or by updating typology codes in regulations.

431. The number of customers who were refused accounts or transactions by FIs and DNFBPs has been declining in the period of 2015-2017. Russian authorities state that this could be an indication that entities are effectively mitigating ML/TF risks and, consequently, do not resort to termination of business relationships or refuse to conduct transactions due to ML/TF concerns. However, this assertion does not seem consistent with the fact that the number of STRs is increasing very rapidly (almost doubling from 2015 to 2017, as shown in Table 5.1; see also title 5.1.5). Since Russian AML/CFT legislation does not mandatorily trigger a refusal due to ML/TF concerns (see c.10.19), FIs may have chosen to shift their approach towards carrying on with the business relation or transaction and file an STR, instead of exercising the refusal.

432. There was no indication during the on-site visit that the technical deficiencies noted in c.10.19 on the duty to refuse due to the inability to conclude CDD either at the on-boarding stage or before conducting an occasional transaction has hindered effectiveness.

Application of CDD and record-keeping requirements

433. Interviews with private sector representatives suggested that FIs and DNFBPs generally understand and implement CDD and record-keeping requirements.

Financial institutions

434. FIs met obtain the required CDD information and refuse business relationships or transactions if the CDD process cannot be completed. They have also demonstrated that they take measures to monitor and verify information obtained and conduct periodic reviews of customer identification data, such as permanent monitoring of source and destination of funds, online monitoring of transactions and periodic reassessment of PEPs' status. FIs update available information at least once a year. Where doubts on the accuracy and reliability arise, updates takes up to seven working days.

435. However, the number of breaches identified by the BoR regarding identification of customers indicates a weaker level of compliance, particularly among

CIs, microfinance organisations and consumer credit cooperatives, which are identified in the ML NRA as heightened risk. Table 5.1 shows a diverse development of the compliance pattern. Apart from 2018, where the team acknowledges the efforts and the improvement of FIs, the three sectors seem to be underperforming. The BoR is also currently enhancing its supervisory procedures and practice (which the assessment team commends and encourages – see IO.3), and states that this may be the cause of the increased number of identified breaches. Assessors also appraise this statement as problematic for the following reasons: first, it is not in line with the figures of 2015 (which is the most prominent year of non-compliance); second, it implies that the current breach landscape may be understated since improvements in the present and for the future mean that procedures and practice – and, thus, the ability to detect violations – were not as developed in the past.

Table 5.1. Number of breaches on CDD for FIs

	2014	2015	2016	2017	2018	Total
Found in credit institutions	952	1 247	225	467	96	2 987
Number of on-site inspections[51]	404	275	244	217	123	1 263
Breaches per inspection ratio	2.4	4.5	0.9	2.1	0.8	2.3
Found in microfinance organisations	210	222	481	393	45	1351
Number of on-site inspections	1	5	14	12	4	36
Breaches per inspection ratio	210	44.4	34.3	32.8	11.3	38
Found in credit consumer cooperative	174	147	415	615	39	1 390
Number of on-site inspections	6	8	8	43	10	75
Breaches per inspection ratio	29	18.4	51.8	14.3	3.9	19

436. On identification of the BO, there is an uneven understanding of obligations, although FIs seemed more solid than DNFBPs. Most entities met rely on the 'controlling ownership' criterion only and are not aware of other ways to identify the BO. If doubts arise whether this criterion is sufficient to determine the BO, they disregard persons that may control the legal entity through other means. Customers are obliged to indicate the BO when establishing a business relationship; however, verification of the BO proved challenging, especially regarding complex structures (e.g. multi-layered legal entities and foreign trusts) or strawmen (informal nominee). The Compliance Council issued guidance to identify BOs in June 2018, which has some examples and case studies. Rosfinmonitoring and the BoR circulated explanatory notes on this matter; however, they seem a superficial explanation of the legal requirements and less of a detailed guidance on how to identify the BOs in unusual or complex structures.

437. Apart from larger FIs, who have the resources to conduct verification from external sources, the national central registry of legal entities is the primary source of information used to determine and verify information on BOs, with deficiencies identified in IO.5 regarding legal entities. Legal ownership information held in the USRLE may coincide with BO information only for entities with simple structures.

438. One FI met mentioned two cases where, following on-going monitoring, the BO information was found not to be consistent with the information provided and the

[51] These figures include planned and ad hoc inspections (both including an AML/CFT component and exclusively on AML/CFT – see IO3).

FI would keep both the BO information provided by the customer and the BO identified. Nevertheless, with few exceptions, FIs and DNFBPs seem to have a tendency to identify as the BO the natural person owning 25% or more of the legal person and in the absence of a person controlling the legal person through ownership interest, they would immediately identify the senior management as the BO (i.e. without trying to identify the BO as the natural person who exercises control through other means).

439. Russian authorities assert that the effectiveness of implementation of CDD obligations is connected to supervisory action undertaken by the BoR and the downward trend of non-compliance in this regard. While this is true regarding the identification of the BO in general, there has been an increase in detected breaches in 2017 by micro-finance organisations and consumer credit cooperatives,[52] which are both considered to be of heightened risk (see also previous paragraph), due to a (i) change in supervisory focus and methods (see IO.3) which enabled the BoR to detect breaches from that moment onwards that went unspotted in the past and, possibly, (ii) amendments to the AML/CFT Law which established new requirements for legal entities to disclose their BOs, as well as the publication of the BoR guidance on BO identification. While this shows an increased attention by the authorities to the micro-finance and consumer co-operative sectors, it also shows that CDD requirements in these sectors may be fairly deficient.

440. Record-keeping requirements were well understood and implemented by the firms interviewed. Nevertheless, between 2014 and 2018 the BoR identified 29 347 breaches in credit institutions (breaches in other sub-sectors are very few). From Table 5.2, CIs experienced significant non-compliance in the 2014-2016 period, having improved in recent years.

Table 5.2. Number of breaches on record-keeping requirements detected in FIs

	2014	2015	2016	2017	2018	Total
Found in credit institutions	4 310	5 023	17 661	688	1 665	29 347
Number of on-site inspections[53]	404	275	244	217	123	1 263
Breaches per inspection ratio	10.7	18.3	72.4	3.1	13.5	23.2

DNFBPs

441. DNFBPs met during the on-site implement adequate CDD and record keeping requirements in general. They are also aware that they are expected to refuse or terminate business relationships if the CDD process cannot be completed and then consider filing an STR. The figure above illustrates that DNFBPs apply it in practice. Available information is updated at least once a year, up to seven working days when doubts about the accuracy and reliability arise.

442. DNFBPs met demonstrated a fair understanding of BO requirements and a less developed level of implementation when compared with FIs.

52 Microfinance organisations committed 33 breaches in 2017, up from only 2 in 2016. Similarly, Consumer Credit Cooperatives committed 60 breaches in 2017, up from only 1 in 2016.

53 These figures include planned and ad hoc inspections (both including an AML/CFT component and exclusively on AML/CFT).

443. However, statistics on identified violations showed a significant level of non-compliance across DNFBPs, particularly in the DPMS sector, regarding the implementation of CDD measures, including the identification of the BO.

444. Real estate agents have been found in violation of record-keeping requirements in very few circumstances.

Application of EDD measures

Politically Exposed Persons (PEPs)

445. According to the ML NRA, Russia faces a high level of risk of participation of PEPs and their associates in ML schemes, mainly due to the large number of crimes in the public sector (linked to budgetary spending and taxation) and corruption.

446. Identification of PEPs seemed to be good in the financial sector. FIs met have shown a good level of implementation of EDD to PEPs, family members and close associates. There was no indication that technical compliance issues (see R. 12) hindered effectiveness of obliged entities met to identify foreign and domestic PEPs, including close associates, and to apply commensurate enhanced measures. One DNFBP mentioned difficulties in identifying foreign PEPs. A reduced number of breaches was identified in the financial and DNFBP sectors. However, there are major technical shortcomings and these may not ensure a consistent application of mitigating measures across both sectors or enable supervisors to find breaches regarding all the elements of the Standard.

447. In order to establish if a customer is a PEP, a family member or close associate, obliged entities rely on a number of sources, namely commercial databases as well as public information provided by domestic (in particular a list of Russian public officials)[54] and foreign competent authorities (essentially information published on official websites). However, it may be more challenging to identify if a PEP is a BO, given the deficiencies in BO identification stated above.

448. In practice, FIs and DNFBPs monitor PEPs' transactions more intensively. These types of customers are always considered as high risk and a set of EDD measures is applied, such as requiring senior management to approve a business relation or occasional transaction, requiring the source of funds and wealth as well as the nature of the relationship. Where additional information and documentation are not provided, FIs and DNFBPs refuse to carry out the transaction.

Correspondent banking

449. When establishing a correspondent banking relation, FIs carry out CDD on their respondents. This enables FIs to ascertain the nature of business and reputation although it is unclear whether (i) the respondents' AML/CFT controls are properly checked, (ii) there is an understanding of the AML/CFT responsibilities of each

[54] This list is determined by Presidential Decree No. 32 and includes job titles without names. Information on PEPs and other officials is also available on the official websites of government bodies on the Internet. According to Law 273, PEPs are subject to the obligation to publish information about their yearly income and expenses on the Internet (for example, www.declarator.org) as well as assets belonging to them or to close relatives.

institution in the context of the relationship and (iii) FIs assess the quality of supervision to which their respondents are subject. One bank stated that respondent's AML/CFT controls are checked. FIs examine the type of customers the respondent intends to offer services to, volume and amount of transactions. Correspondent institutions monitor the respondents' transactions effectively.

New technologies

450. FIs and DNFBPs met always consider new financial products and new or emerging technologies, as well as changes in the provision of existing products or services, to be high risk and apply commensurate mitigating measures. Many FIs met consider the risk to be so high that they prefer not to on-board customers – or to continue business relationship with existing customers – that provide new products or technologies rather than to manage the risk. However, credit institutions have offered electronic means of payments (such as "e-wallet" and pre-paid cards) without fully mitigating[55] the existing vulnerability of their anonymity (the issue of anonymity was identified as a vulnerability by the ML NRA).

451. Obliged entities also provide a fair amount of STRs concerning the use of new technologies, which indicates that their monitoring and risk awareness is satisfactory. Virtual assets are considered by the NRA as an increasing risk (particularly for drug-related offences) and STRs on the use of virtual assets by FIs grew exponentially in 2017, with 3646 reports filed to RFM (up from 18 in 2016, 25 in 2015 and 2 in 2014).

452. Russia recently passed new legislation concerning the use and oversight of virtual assets, but these remain prohibited, and practical steps to licence or register service providers or to apply AML/CFT controls to the sector have not yet been applied.

Wire transfers

453. FIs apply wire transfer rules in Russia. Despite legislation not fully in line with the standards (see R. 16), the meetings with FIs suggest that the technical compliance gaps do not affect the application of wire transfer rules, which are effectively applied. In addition, the BoR has not found a significant amount of breaches in the implementation of those wire transfer rules.

Targeted financial sanctions

454. FIs and DNFBPs met are aware of their obligations in relation to TFS and have measures in place to timely comply. All CIs have automated systems to screen for potential hits both before conducting a transaction and the establishment of a business relationship as well as during its course. Smaller FIs and DNFBPs conduct the screening with less sophisticated systems or manually. Nevertheless, there is some confusion with regard to the relevant obligations relating to domestic lists (which include both designated terrorists and extremists) as opposed to UN lists (see IO.10). FIs and DNFBPs appear to know better their obligations in relation to domestic lists, for example on disbursing certain funds to listed persons. Similar to PEPs, implementation

55 Regarding e-money institutions, transfers performed without conducting CDD are limited to around EUR 200 by the AML/CFT Law. Nevertheless, CDD needs to be conducted if, for instance, a ML/TF suspicion arises. Russian authorities are working to further reduce the referred amount.

of TFS requirements may be hindered given the deficiencies in BO identification stated above.

455. Competent authorities assert that their efforts in improving the effectiveness of the system regarding implementation of TFS are seen in the small amount of breaches found. In 2018[56], failure to freeze funds was detected twice in CIs and once in pawnshops. On failure to implement measures to freeze funds or other assets without delay, a continuous improvement is registered in all sectors (see Table 5.3) despite the sharp, isolated, increase in 2017 for CIs.

Table 5.3. Number of breaches on TFS obligations.

	2014	2015	2016	2017	2018	Total
Found in credit institutions	13	48	12	77	2	152
Number of on-site inspections[57]	404	275	244	217	123	1 263
Breaches per inspection ratio	0.03	0.2	0.1	0.4	0.02	0.1
Found in microfinance organisations	49	37	40	3	0	129
Number of on-site inspections	1	5	14	12	4	36
Breaches per inspection ratio	49	7.4	2.9	0.23	0	3.6
Found in credit consumer cooperatives	35	17	22	2	0	76
Number of on-site inspections	6	8	8	43	10	75
Breaches per inspection ratio	5.8	2.1	2.8	0.04	0	1

Higher risk countries

456. FIs and DNFBPs met are aware of the FATF public statements concerning higher risk countries, which they receive through the personal account. They must rank as "high-risk" any customer, including the BO, from a jurisdiction that fails to comply with the FATF Standards. They must also submit a mandatory report in case of any transactions of RUB 600 000 (around EUR 8 000) or above to or from a person who is from or resident in such a jurisdiction.

Reporting obligations and tipping-off

457. FIs and DNFBPs met during the on-site visit generally understand and implement their reporting obligations. However, it is not clear whether this understanding applies equally across all sectors and firms, as the number of STRs filed is relatively low (expect for credit institutions) (see Table 5.5).

458. In Russia, the level of suspicion involving each STR is low in general, which results in a large volume of STRs filed by CIs (more than 74 million for the period of 2014-2018 – see Table 5.5; and 41 million "mandatory reports" over the same period). The system is largely based on the risk indicators provided and updated on a regular basis by Rosfinmonitoring in co-ordination with the BoR, with scarce human intervention. As a result, all entities met during the on-site have few staff dedicated to verifying suspicious transactions relative to the amount of STRs filed each year (for

56 The BoR did not maintain statistics on the failure to freeze funds or other assets prior to 2018 having changed their statistical methodology in 2017 in order to provide them.

57 These figures include planned and ad hoc inspections (both including an AML/CFT component and exclusively on AML/CFT – see IO3).

example, each dedicated staff in a credit institution would have to deal with around 40 STRs per day). Russian authorities assert that these indicators are non-exhaustive and that obliged entities file STRs based on different grounds. However, statistics show (see Table 5.4) that non indicator-based STRs are filed to a lesser extent.

Table 5.4. Share of STRs submitted by CIs based on pre-determined indicators

	2013	2014	2015	2016	2017
Indicator-based STR (%)	65	72	76	81	80
Non-indicator-based STR (%)	35	28	24	19	20

459. Despite large amount of raw STRs, this system has proven to be a good source of financial information to Rosfinmonitoring, which uses big-data tools to automatically screen and filter raw STRs and generate leads for analysts (see IO.6). As such, the reporting system is tailored primarily to suit Rosfinmonitoring's data processing needs and less so on attaining a high degree of suspicion and high quality of STRs. Moreover, the assessment team finds the indicators in force to be comprehensive and regularly updated, which can justify a high proportion of red flags being automatically generated and resulting in the submission of an STR. However, this occurs without there being a thorough and in-depth analysis conducted by FIs prior to the filing of STRs which may impede the system from benefiting from the knowledge FIs hold of their customers. While STRs based on other patterns of behaviour (non-indicator based STRs) do occur, the added value may be reduced, given their significant amount (around 14 million during 2014-2018) and few staff of FIs dedicated to this matter to conduct analysis.

460. The STR reporting system does not allow Rosfinmonitoring to detect at all times when a specific report exceeds the threshold of suspicion required to trigger an STR (e.g. those cases which have been investigated by FIs and where they have a high degree of confidence that a crime has been committed), or where there is a high degree of urgency. Similarly, the internal systems used by Rosfinmonitoring do not include any means for such high-priority STRs to be prioritised for special or urgent attention by FIU analysts. Rather, all STRs are entered into the database and reviewed only if part of a pattern is identified by automated analysis tools. This may be inappropriate for some types of reporting entities – particularly those such as lawyers and accountants who have few customers and a more in-depth knowledge of each customer, and are therefore able to submit STRs containing more relevant and descriptive information, based on a higher degree of suspicion. Russia's reporting system has no way to gather and make use of the greater degree of customer knowledge in these sectors.

461. The rest of the financial sector (including non-CIs supervised by the BoR, which entails micro-finance and consumer credit cooperatives, considered to be heightened risk in the ML NRA) show a very diverse dynamic and significant disparity in STR filing, even taking into account differences that would necessarily exist due to firms' uneven asset-size and risk exposure. Overall, in the financial sector, apart from CIs, STR filing is much lower and should be improved.

462. DNFBPs show a trend of underreporting, which could be a concern since the nature of their customer relationships and the low volume of reporting mean that they are not such appropriate subjects for a big-data analysis approach, as set out above.

Table 5.5. Number of STRs (including attempted transactions) by sector

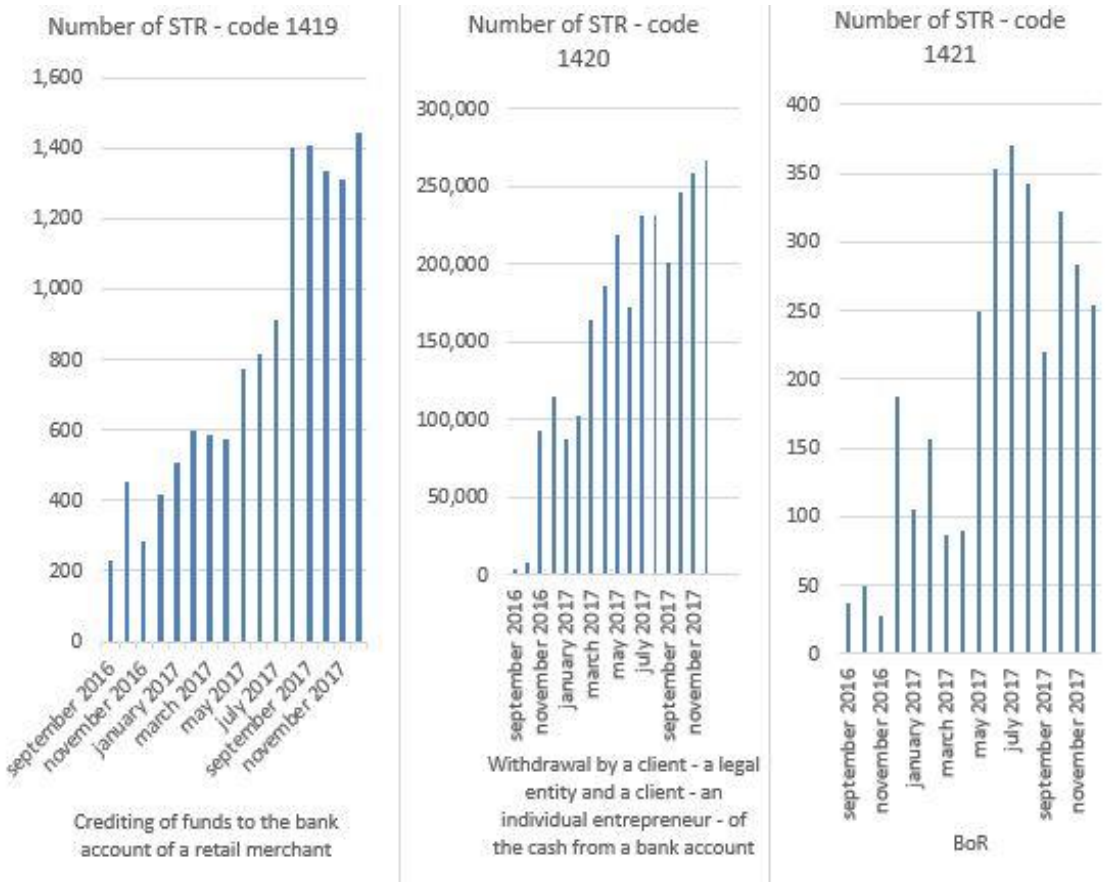
	2014	2015	2016	2017	2018	Total
Credit Institutions	4 500 000	11 800 000	18 800 000	21 400 000	17 700 000	74 200 000
Non-credit FIs supervised by BoR	74 000	101 000	162 000	107 000	105 000	549 000
Precious Stones and Metals Sector	3 500	4 000	4 700	4 100	4 200	20 500
Real Estate Agents	5 300	3 700	2 800	2 400	2 300	16 500
Payment Service Operators	44 000	65 000	64 000	69 000	60 000	302 000
Leasing Companies	4 900	4 700	5 300	12 500	13 000	40 400
Factoring Companies	800	400	1 000	100	100	2 400
Organisations of Post Communication	12 000	14 000	1 400	8 700	8 000	44 100
Communication Service Providers	12 000	14 000	1 400	2 000	3 000	32 400
Gambling Sector	100	1 500	400	100	400	2 500
Notaries	10	31	56	141	583	821
Lawyers	11	20	23	31	17	102
Accountants (auditors)	5	21	12	17	20	75
Legal professionals	3	11	10	27	23	74
Total	4 656 629	12 008 383	19 043 101	21 606 116	17 896 643	75 210 872

463. To identify transactions and produce reports, since 2009 CIs have been using a centralised automated solution, established by regulations issued by the BoR in coordination with Rosfinmonitoring. The continuous improvement of the automated software which CIs have introduced partly explains the sharp increase in the number of STRs. The increase is also explained by the more refined typologies/indicators given by Rosfinmonitoring and introduced into the software maintained by banks. Identification of transactions is carried out on the basis of algorithms developed on the basis of criteria internally established and typologies brought to their attention by competent authorities or independently identified by the financial institution. The identification algorithm can be changed depending on the frequency of trends. From discussions held with private sector representatives, it was clear that they heavily rely on input on trends and methods provided by Rosfinmonitoring and only marginally develop their own typologies.

464. The work developed by the Compliance Council led to an increase in STRs in certain areas. The majority of STRs filed by FIs (around 80% for the period of 2013-2018, according to Russian authorities) pertain to areas of high ML/TF risk, which could lead one to conclude that obliged entities are becoming more knowledgeable and focused on their ML/TF risks. However, this is more of a result of the Compliance Council's work, which is commendable, and less of that of reporting entities. Also, as already explained, since the threshold of suspicion for each STR is low the assessment team casts doubts as to whether this increase is not more of a result of automation and less of risk understanding.

465. In 2016, the Compliance Council identified risks of conducting suspicious transactions. Rosfinmonitoring has sent such information to the BoR with a proposal to amend the classifier of suspicious transactions indicators. As a result, three new indicators were introduced (code 1419, on the possible sale of cash by the client in violation of existing legal restrictions on cash turnover; code 1420, on suspicious cash transactions through legal entities; and code 1421, on signs of transactions with residents of offshore jurisdictions) (see Figure 5.1).

Figure 5.1. Number of STRs by code



466. Due to the STR-filing system being largely based on automation the quality of STRs is generally measured against many fields (250) that reporting entities must fill out before submitting an STR.

467. The quality of reporting is also addressed by Rosfinmonitoring by providing feedback on STRs to FIs and DNFBPs. Improvements to STRs are identified through ongoing monitoring of received STRs, which could result in modifications to indicators or the STR template. Rosfinmonitoring frequently issues new indicators, instructions and typologies to the private sector to better identify suspicious activity. More than 100 indicators and typologies have been distributed over the last five years. Feedback is provided via targeted outreach by supervisors, or outreach on filed STRs via engagement through the Compliance Councils (both federal and regional), with over 100 representatives of FIs and DNFBPs. The Compliance Council has monthly meetings dedicated to the quality of STRs. However, entities met referred that feedback provided by Rosfinmonitoring was made by way of messaging through the personal account and at the Compliance Council meetings. However, the content of feedback seemed very generic and with little added value for reporting entities. Most entities referred that they receive a message thanking them for having filed the STR and that in few cases they receive information on the added value or the consequence given to the STR.

468. Breaches of reporting obligations do not seem significant in the DNFBP sector. However, for the financial sector, the number is not negligent and most of them were found in heightened risk entities.

Table 5.6. Number of breaches of reporting duties

	2014	2015	2016	2017	2018
FIs					
Credit organisations	n/a	n/a	n/a	n/a	1665
Professional securities market participants	n/a	n/a	n/a	n/a	6
Asset Management Companies	n/a	n/a	n/a	n/a	24
Insurance	n/a	n/a	n/a	n/a	27
Non-state pension funds	n/a	n/a	n/a	n/a	4
Microfinance organisations	n/a	n/a	n/a	n/a	6
Consumer credit cooperatives	n/a	n/a	n/a	n/a	46
Pawnshops	n/a	n/a	n/a	n/a	174
DNFBPs					
Accountants (auditors)	0	0	0	0	0
Lawyers	1	1	0	0	0
Notaries	7	4	5	2	2
Legal professions	2	3	1	0	0
Gambling sector	-	-	-	0	0
Precious Stones and Metals Sector	21	13	14	10	7
Real Estate Agents	15	17	12	11	8

469. Regarding tipping-off, the obliged entities met demonstrated good internal controls and procedures for maintaining confidentiality of filed STRs, and no breaches have been detected.

Internal controls and legal/regulatory requirements impeding implementation

470. Firms met during the on-site visit demonstrated good internal control procedures and group-wide policies in place. FIs that belong to international groups or have branches outside Russia reported that data protection rules (seen as bank secrecy rules) prevented intra-group information sharing, thus creating a potentially negative impact on group-wide risk management. The assessment team was able to confirm that no information regarding customers, accounts, transactions, analysis of transactions or activities which appear unusual and STRs filed could be shared with the parent company or other subsidiaries or branches outside Russia. FIU-to-FIU channels were used instead in case of suspicious activity, although the number of voluntary disseminations by Rosfinmonitoring to foreign FIUs appears relatively low (see IO.2), which indicates that adverse information about Russian customers of groups is simply not sent outside Russia through either public or private sector routes. This shortcoming was partly addressed (see R. 18) only at the end of the on-site visit and, thus, is considered to be major for assessing effectiveness, especially given Russia's risk profile as a source country of criminal proceeds.

471. Moreover, supervision conducted by competent authorities, suggests that while there is a trend of improving compliance in recent years, some weaknesses persist, particularly the number of breaches in organising internal controls.

472. In fact, this practice seems to be widespread in Russia, whether regarding breaches of internal control rules or lack of timely update. For instance, for the period of 2014-2017, there were more than 17 000 cases where FIs were found not to comply with their internal control duties (of which 3 660 cases for CIs). Other heightened risk FIs also present a worrying picture (for the same period, 4 584 cases for microfinance companies and 3746 cases for consumer credit cooperatives). However, compliance seems to have been improving since 2016.

Table 5.7. Number of internal control breaches for FIs

	2014	2015	2016	2017
Found in credit institutions	679	1541	924	516
Number of on-site inspections[58]	404	275	244	217
Breaches per inspection ratio	1.6	5.6	3.7	2.3
Found in microfinance organisations	803	1527	1611	643
Number of on-site inspections	1	5	14	12
Breaches per inspection ratio	803	305.4	115	53.6
Found in credit consumer cooperative	524	973	1371	878
Number of on-site inspections	6	8	8	43
Breaches per inspection ratio	87.3	121.6	171.4	20.4

473. Supervisors find a large number of non-compliant entities regarding the provision of training for staff in AML/CFT issues. This seems relatively widespread among financial (especially CIs) and DNFBP sectors (especially DPMS and real estate agents) which is qualified as a significant shortcoming, since robust and effective preventive measures can only be applied by obliged entities if their staff has proper training and is alert to suspicious situations. Nevertheless, the entities met did state that AML/CFT training was provided.

Overall conclusions on IO.4

474. Overall, the understanding of ML/TF risks and the implementation of AML/CFT preventive measures on a risk basis by FIs is satisfactory in Russia, despite concerns on the identification of BOs. For the DNFBP sector, there is a mixed and uneven level of awareness and understanding of ML/TF risks, which is insufficient for some sectors. There is widespread and persistent trend of non-compliance with preventive duties, although decreasing in recent years. There is increasingly more reports being made using Rosfinmonitoring's pre-established indicators, which do not include the in-depth analysis by FIs, which could impact their added value. It is also unclear whether the increase in suspicious transactions should not be leading to more termination of business relations and refusals to conduct transactions for ML/TF concerns. Intra-group information sharing was not possible in Russia until the on-site visit took place.

475. Russia is rated as having a moderate level of effectiveness for IO.4.

58 These figures include planned and ad hoc inspections (both including an AML/CFT component and exclusively on AML/CFT).

CHAPTER 6. . SUPERVISION

Key Findings and Recommended Actions

Key Findings

1. The banking sector is exposed to a high level of threat from criminals. Since 2013, the number of credit institutions licenced to operate in Russia has been halved as a result of licence revocations (including for serious violations of AML/CFT provisions). The licensing requirements for FIs have improved since 2013. However, measures to ensure that criminals and their associates are not BOs of FIs could be stronger, and the BoR could expand the data sources used to screen applicants.
2. The BoR has developed a good understanding of the ML/TF risks in sectors it supervises. Its understanding of ML/TF risks before 2016/2017 was largely based on the analysis of suspicious transactions, but since then the BoR has improved its risk assessment methodology and conducted its first ML/TF sectorial risk assessment in November 2018 with the main objective of risk-ranking the supervised sectors. The BoR's understanding of risks at sector-level is now reasonable and fairly detailed but its understanding of risks at an institution-level requires additional attention taking into account factors such as product characteristics, client base, and potential non-compliance.
3. Planning of AML/CFT on-site inspections is not separate from prudential supervision. Planned on-site inspections follow a time-bound cycle based on prudential considerations (every two years for CIs, every three years for other FIs) and AML/CFT components can be added to planned inspections based on the information available on the institution.
4. Since 2013, the BoR has put in place an intense bank supervisory programme informed by AML/CFT risks. The BoR has shifted its supervisory strategy from on-site inspections to remote supervision, which uses algorithms to identify possible involvement in suspicious transactions and detect potential AML/CFT breaches. Where remote supervision identifies a higher risk of non-compliance by an institution and the institution does not remedy this, the BoR may organise a targeted (ad hoc) inspection solely focused on AML/CFT.
5. However, assessors are concerned about the insufficient number of on-site inspections of AML/CFT issues, and are particularly concerned about the declining number of such inspections as the BoR shifts its focus to off-site

AML/CFT supervision. Assessors consider that the BoR overrelies on remote forms of supervision, and has insufficient flexibility to schedule on-site inspections based on AML/CFT risks (as opposed to prudential risks).

6. AML/CFT supervision of non-credit FIs has only recently moved to a risk-based approach and the resource allocation to sectors is not fully in line with sector-specific risks.
7. Rosfinmonitoring has a robust understanding of the sectoral ML/TF risks in the sectors it supervises, and has conducted AML/CFT specific on-site and off-site inspections using a risk-based approach. Roscomnadzor and DNFBPs supervisors have their own risk assessment methods and their ML/FT risk understanding has largely improved after the NRA process. DNFBP sectors, including DPMS, undergo supervision for prudential and conduct of business purposes, which can include AML/CFT issues.
8. Overall compliance by FIs has improved in recent years. A significant number of licence revocations for serious ML/TF violations has had a cleansing effect. However, the monetary penalties imposed for AML/CFT breaches are relatively low, and not sufficient to be dissuasive. The frequent use of licence revocations may indicate a failure to address problems early, as well as a willingness to apply serious tools when needed.
9. Communication of risks and obligations is generally done well through a variety of tools. The *Personal Account* maintained by Rosfinmonitoring and the training provided by ITMCFM are particularly useful in expanding the knowledge and understanding of obligations across the private sector.

Recommended Actions

1. The BoR should detach prudential and AML/CFT on-site inspections. Planning of the latter should be based on ML/TF risk of the relevant financial institution. This should include both scheduled AML/CFT inspections, and more frequent use of unscheduled inspections when merited.
2. The BoR off-site/remote supervision should be modified by developing more sensitive means to determining the risk profile of individual supervised institutions, taking account of the quality of entities' control measures.
3. In order to better inform the risk-based approach to supervision, supervisors should deepen their understanding of the ML/TF risk of each individual institution by expanding the data available. The BoR should obtain additional information from law enforcement and other government authorities. Supervisors should keep the sectoral risk assessments up-to-date and should use the results to allocate ML/TF supervisory resources in full accordance with the existing risks.
4. Supervisors should ensure that AML/CFT deficiencies identified during examinations lead to supervisory actions that are dissuasive and effective.

Progressive remedial actions should be strengthened in order to avoid further violations, particularly by multiple offenders.

5. Regulators should expand the data sources available to determine if an individual is fit and proper to be a BO or to hold a management and/or a controlling position of a FI, in particular to assess if any applicant is associated with criminals or organised criminal groups. This could be done by obtaining information or intelligence concerning on-going investigations from relevant authorities (Police, Rosfinmonitoring, etc.).
6. DNFBP supervisors need to improve supervision based on the ML/TF risks identified. The DPMS sector needs to be better supervised given the significant ML/TF risks in the sector. DNFBP supervisors should also exercise more thorough controls over licensing requirements, and apply sanctions where needed.

476. The relevant Immediate Outcome considered and assessed in this chapter is IO.3. The Recommendations relevant for the assessment of effectiveness under this section are R.14, R. 26-28, R.34, and R.35.

Immediate Outcome 3 (Supervision)

477. Russia has several authorities responsible for AML/CFT supervision of FIs and DNFBPs. The relevant supervisors are:

- BoR: for CIs (banking groups) and other FIs (securities market participants, management companies, insurance organisations, microfinance organisations, credit consumer cooperatives, non-state pension funds and pawnshops).
- Roscomnadzor: for federal postal communication and telecommunication operators.
- Rosfinmonitoring: for real estate agents, leasing companies, payment service operators and factoring companies.
- FTS: for casinos, lotteries, and sweepstakes and betting offices.
- Assay Chamber: for DPMS.
- Notarial Chambers, Chamber of Lawyers: for notaries and lawyers respectively.
- MoF, in conjunction with two SROs of auditors which are supervised by the MoF, Federal Treasury in conducting inspections: for auditors (accounting activities).

478. TCSP activity is not regulated as a separate category for economic activity or for AML/CFT supervision. Legal professionals have no designated AML/CFT supervisor and GPO conducts some activities to oversee the implementation of the AML/CFT legislation.

479. Positive and negative aspects of supervision were weighted most heavily for credit institutions, highly for consumer credit co-operatives and microfinance

companies and DPMS, moderately for the securities, real estate, MVTS services, payment acceptance services sectors; and less heavily for the remaining sectors (lawyers, notaries, legal professionals, accountants, and TCSP, insurance sector, private pension funds, mutual insurance companies, casinos, mutual investment funds, investment fund management companies), based on the relative materiality and risk in the Russian context.

Licensing, registration and controls preventing criminals and associates from entering the market

Financial Institutions

480. Strengthened controls were introduced from 2013 onwards, and there are now thorough checks on the fitness and propriety of persons in controlling positions in the sector. Since 2018, mandatory requirements have been tightened further. The fitness and propriety requirements for founders, shareholders, directors, and senior management include assessing the qualifications (such as higher education, work experience and performance) as well as business reputation (no recent convictions for intentional breaches and/or crimes, no involvement in extremist activities, no criminal prosecution in case of bankruptcy of legal entities, or fictitious bankruptcy of legal entities). The BoR maintains a list of persons (7 068 persons as of 1 January 2019) whose activities led to the damage of FI's financial position or violations of laws and regulations, and whose business reputation is therefore considered unsatisfactory.

481. The BoR also conducts fit-and-proper testing of BOs. The BoR requests BO information from the entities and verifies it against the USRLE and commercial websites. It also seeks to understand the source of fund and the relationship of owners. In order to enhance background checks, the BoR cross-matches the databases of owners and senior management of FIs with data from the FTS and the MoI (regarding the presence or absence of criminal records). No application for licensing has been rejected because of the BO failed to meet the fit-and-proper requirements (see Table 6.1 for the applications dealt with by the BoR).

Table 6.1. Number of licence applications dealt with by BoR[59]

		2013	2014	2015	2016	2017	2018
Credit Organisations	Received	16	13	8	6	0	3
	Approved	10	7	2	3	0	1
	Rejected	9	6	6	4	0	1
Insurance	Received	510	170	40	34	22	35
	Approved	210	58	15	10	10	13
	Rejected	300	112	25	24	12	18
Securities	Received	316	328	172	76	57	21
	Approved	105	94	37	29	36	24
	Rejected	70	32	52	26	21	20

482. There are strong mechanisms to ensure that licensing requirements are respected on an on-going basis. The BoR must approve any changes to financial

[59] The inconsistencies in the totals in the three columns are caused by the receipt of documents in the current year with a decision made in the following year.

institution ownership above 10% and any changes to senior management, both of which require the conduct of fit-and-proper checks (for example, in 2017, the BoR refused the appointment of one person who applied for a board member position, as the person had undischarged convictions). Every quarter the BoR requests the MoI to verify the criminal status of any persons in executive bodies and ensure that significant owners do not have any outstanding convictions.

483. Compliance with licensing requirements is also considered in the course of on-going supervision, which is used as a way to re-evaluate the fit-and-proper test of FIs registered prior to 2013. Table 6.2 shows a sharp increase in the number of identified violations from 2014 onwards, which reflects more stringent controls adopted by the BoR. The BoR indicates that as of March 2019 there were no persons with undischarged or outstanding convictions in the economic sphere controlling or holding senior management positions in a financial institution.

Table 6.2. Breaches of licensing requirements (due to criminal records in brackets) committed by credit institutions; and actions taken by the BoR

	2013	2014	2015	2016	2017	2018
Number of violations identified	6 (0)	126 (2)	188 (0)	127 (0)	146 (1)	201 (0)
Requests for management replacement	2 (0)	51 (2)	86 (0)	57 (0)	101 (0)	165 (0)
Requests for eliminating the violation	4 (0)	75 (0)	102 (0)	70 (0)	45 (1)	36 (0)

484. The verification of business reputation focuses only on the criminal records (and in some cases criminal prosecution) of the applicant. This leaves the possibility that persons associated with criminals but who have not been convicted may own or control FIs, which is a material risk in Russia (see IO.7, Box 12 and Table 12). The business reputation requirement could be enhanced if the BoR sought information or intelligence on on-going investigations from any relevant authorities (Police, Rosfinmonitoring, etc.). By expanding the sources of information employed when considering an application, the BoR could have a more complete picture to assess if any applicant is associated in any manner with criminals, in particular organised criminal groups.

485. For FIs not licenced by the BoR, there are generally sound measures to prevent criminals from controlling the institution. Prior to the registration of payment operators and microfinance organisations with the Federal Tax Services, Rosfinmonitoring accesses its internal databases to see potential connections between the applicants and any criminal person, rejecting around 25% and 34% of applications in the respective sectors between 2013 and 2018. Roscomnadzor licences the Russian Post, and the decision on the appointment of the director is made by the Government taking into account mandatory fit and proper requirements. Roscomnadzor also verifies the applications for a licence by mobile operators and from 2013 to 2018 rejected 11 out of 873 applications.

486. The authorities have taken action to identify and suppress the provision of financial services without a licence, which is treated as a serious criminal offence (see IO.7). In one case from 2018, a person linked to an organised criminal group was convicted for conducting banking activities without a licence and sentenced to 3 years in prison and a fine of RUB 300 000 (EUR 4 000). The BoR also helped to shut down a number of unlicenced foreign exchange operators which were identified from

advertisements on paper or online. The Russian authorities indicated that the risks of using a number of tools for the illegal provision of financial services (e.g. hawala) in the conditions of Russia are minimised.

DNFBPs

487. Federal Tax Service licences casinos and other organisations carrying out gambling activities in bookmaker offices and sweepstakes and verifies the legal source of the paid-in capital, as well as the criminal records of founders and BOs. Between 2014 and 2018, a total of 19 (out of 24) licensing applications had been rejected because they were inconsistent with the licensing requirements, four of which were rejected because of non-compliance with mandatory requirements for preventing criminals from becoming BOs. During on-site inspections, the FTS conducts criminal record checks, and licences can be suspended or revoked if violations are identified (no violation has been found thus far). On-line gambling is not allowed but the FTS identified around 95 000 illegal online gambling providers between 2016 and 2018.

488. Real estate agents must register with Rosfinmonitoring, which, before registration, conduct checks on criminal records on founders, BOs and persons holding controlling positions. On-going monitoring is conducted through inspections by reviewing relevant documents and by screening databases (including Rosfinmonitoring databases) in order to identify possible cases of criminals directly or indirectly possessing, controlling or managing entities, although this does not necessarily identify criminals' associates in such roles. During 2013-2018, Rosfinmonitoring refused registration of 1 394 real estate organisations (22% of 6 358 applications, including 9 organisations due to outstanding convictions of BOs), and 191 individual entrepreneurs (12% of 1540 applications, no outstanding convictions identified).

489. There are market entry controls for DPMS, lawyers, notaries and auditors that require them to be registered by regulators or by SRBs. During the registration process, the Assay Chamber requests Rosfinmonitoring to carry out checks of criminal records on its behalf. After market entry, the Assay Chamber and the SRBs conduct ongoing monitoring when they become aware of position changes or during on-site inspections, and withdraw registration or terminate professional status for criminal violations. Any change of the sole executive body or a BO in the DPMS sector will trigger a criminal record check, and there are cases of DPMS being refused or having their licence revoked for criminal reasons. Notaries need to first pass a qualification exam and can be dismissed if they repeatedly violate laws or are disciplined. There were four cases in 2015 and two cases in 2016 in which notaries were deprived of their right to execute notarial activities as a result of committing an intentional crime.

490. Auditors must register with the SRB, which verifies criminal records and requests information from other sponsoring auditors. Besides the market entry stage and on-going business reputation controls, the Federal Treasury conducts on-going inspections of audit organisations (generally the most significant in terms of size of business) and of the SRB in relation to its members. The Federal Treasury can also request the assistance of Rosfinmonitoring to perform verifications of criminal registers.

491. The accreditation of lawyers can be withdrawn for the commission of intentional crimes, violation of professional ethics, non-performance of duties or

inadequate fulfilment of decisions of chambers of lawyers. From 2013 to 2017, the Lawyers Chamber withdrew the accreditation to 165 lawyers (approx. 0.2% of the total lawyers per year) because of convictions for intentional crimes.

492. There are deficiencies in the ability to prevent criminals' associates from owning, controlling or holding a management function in all DNFBPs.

493. To sum up, in the banking and other sectors, the entry market controls have significantly intensified since 2013, both during licensing and as part of on-going supervision. However, there remain weaknesses, including the narrow scope of propriety checks which are limited to checking that persons have no recent convictions for intentional crimes and do not check for other factors (e.g. association with criminals). In the DNFBP sectors, especially for DPMS, lawyers and notaries, it is necessary to apply more stringent measures in order to identify unqualified professionals when ownership changes, particularly taking into account the large number of participants.

Supervisors' understanding and identification of ML/TF risks

Financial institutions

494. Over recent years, supervisors have developed a good understanding of the ML/TF risks in the sectors they supervise. The BoR effectively improved its ML/TF risk understanding in 2013 by introducing a methodology for assessing the risk of suspicious transactions, and developed a risk assessment methodology in 2016/2017 to include comprehensive factors. It improved its understanding of ML/TF risks during the first NRA process. Building on the NRA it developed a specific SRA for ML/TF in November 2018.

495. The risk analysis of the SRA is to some extent reasonable and detailed. The SRA took into account a number of factors contributing to the NRA, such as the sectoral and individual institution's characteristics, information from Rosfinmonitoring about ML/FT risks, involvement in suspicious transactions analysed through the BoR payment system, results of previous supervisory inspections. The SRA report available to assessors analysed some risks associated with suspicious transactions, but had few conclusions on ML/TF threats and vulnerabilities (and none for non-credit financial sectors). Russia explained that in addition to the risk factors already included in the NRA, the BoR also considered 33 further types of threats and 22 types of products/services' vulnerability within the sectoral risk assessment.

496. One of the main purposes of the SRA was to risk-rank each sector under the BoR supervision. CIs are rated high risk, professional securities market participants, insurance organisations (excluding mutual insurance societies) and credit consumer cooperatives are rated heightened (significant) risk, micro-finance organisations are rated moderate risk, management companies and private pension funds are rated low risk.

497. The BoR emphasised that the SRA helps to optimise resource allocation and consider further risk mitigation measures. However, the resource allocation does not seem to be fully in line with the sectors' ML/TF risks and the findings of the SRA have not yet informed supervisory activities well (see below). In particular, there is a

divergence between the ML NRA and the SRA risk ratings in areas of insurance and micro-finance sectors, which may affect the priority of supervisory measures.

498. The institution-level risk understanding has greatly improved, although this still requires further enhancement. Until 2017, the BoR's understanding of the risk profile of each institution was driven by prudential considerations, with some elements of ML/FT. Since 2017, and with the development of the NRA process, the BoR has given increased attention to ML/TF risks related to products/services and types of clients. Since 2016, the ranking is based on a model that takes into consideration three main criteria:

- **Transaction risk –** the extent to which a financial institution is involved in suspicious transactions of a complex or unusual nature (such as suspicious cross-border wire transfers, illegal encashment, and transit transactions, which the BoR can identify in aggregate form by monitoring the volumes of transactions of each institution).
- **Non-compliance with the AML/CFT legislation** – assessment of the compliance of a financial institution with AML/CFT regulations. This is mainly assessed by verifying the compliance of internal controls rules, and the existence of a qualified ML compliance officer; and
- **Risk of AML/CFT system inefficiency –** the extent to which an institution's AML/CFT system is implemented in practice. This is based on any deficiencies or breaches committed by an institution and how serious or systematic those deficiencies and breaches are. The areas of focus are CDD; STR filing; TFS implementation; and any other AML/CFT functions.

499. The criteria used by the BoR are also informed by risk leads provided by Rosfinmonitoring, LEAs and FTS; information from prudential supervisors (e.g. breaches of applicable legislation, lack of transparency of the business model or of specific transactions, lack of financial resilience and heightened risks for lenders and depositors) and information from foreign supervisors. Based on this information, individual FIs are assigned one of three different risk levels within their sector (relative to the level of the risk for the sector as a whole), as shown in Table 6.3. The risk ranking of each institutions is updated quarterly.

Table 6.3. Risk allocation per group of FIs (average in a given year)

Sectors	Risk ratings	2016	2017	2018
Credit Institutions	high	22%	16%	9%
	medium	15%	16%	9%
	low	63%	68%	82%
Securities Market Professionals	high	0.6%	0.9%	0.7%
	medium	0.0%	0.0%	0.0%
	low	99.4%	99.1%	99.3%
Insurance Entities	high	4.1%	3.0%	0.9%
	medium	2.9%	2.1%	0.1%
	low	93%	94.9%	99%
Micro-Finance Organisations	high	2.9%	2.7%	2.7%
	medium	0.5%	0.2%	0.3%
	low	96.6%	97.1%	97%

500. Russia utilises narrow criteria to classify institutions as high and medium risk, which leaves a large proportion of institutions in the low risk category. This risk classification method seems to be designed in response to the challenge posed by a significant number of credit institutions involved in high-risk transactions and providing direct assistance to criminals, and it reflects the priorities of the BoR to clean-up the banking sector and ensure a rapid improvement of AML/CFT systems in CIs (see below for supervision and sanction). It is a positive sign to see the proportion of high and medium risk institutions is decreasing. This approach appears to be reasonable given the context, but needs to be improved for a more mature supervisory model.

501. The institution-level risk understanding is largely based on exposure to certain risky transactions and their degree of informed breaches. It could be improved by paying additional attention to assessing potential non-compliance, and to characteristics of each institution's business lines, products, and client base (such as identification of PEPs or other high risk customers).

502. Rosfinmonitoring has an adequate understanding of the sectoral ML/TF risks in the sectors it supervises. The ML/TF risk assessment automatically gathers inputs (operational data, transaction reporting information and compliance behaviour) from all reporting entities, and in conjunction with information from LEAs, FTS and other sources (such as negative information from the media). On that basis, Rosfinmonitoring assigns a risk rating to each reporting entity (four-tier risk levels). Rosfinmonitoring's understanding of risks is also informed by ML/TF typologies, entities' products, services, customers and geographic locations. Rosfinmonitoring updates the risk assessment of supervised institutions on a regular basis. New risks identified for an individual institution or an institution which has failed to file STRs or mandatory reports will trigger a review of the risk profile.

503. Roscomnadzor carried out a sectoral ML/TF risk assessment in 2016-2017 concluding that the risk level of using mobile communication operators and postal communication infrastructure for ML/FT purposes is classified as moderate. Four-levels of risks are assigned. A number of factors are considered including market conditions, volume of transactions, targeted customers, types of services, limitations on transactions and risky activities involved in the sector. Roscomnadzor updates the risk rating of each institution based on information from Rosfinmonitoring about risks

in the activities of the entity, information from prosecutorial authorities, as well as possible violations of the AML/CFT legislation. Roscomnadzor may need to increase its understanding of risks by itself, especially the TF risks, as there is a large number of remote postal offices and the provision of cash delivery activities.

DNFBPs

504. DNFBP supervisors mainly base their understanding on the NRA process and on information on typologies developed by Rosfinmonitoring. DNFBP supervisors carried out sectoral risk assessments (Rosfinmonitoring for the real estate sector, FTS for the gambling sector, the Assay Chamber for DPMS, the Notarial Chambers together with Rosfinmonitoring on notaries). They use risk assessment models taking into account various criteria: activities, shares of the entities, characteristics of regions and operations, typologies, compliance with the preventive measures requirements, the information provided by Rosfinmonitoring, and the results of NRAs.

505. Casinos are categorised as low ML/TF risk, which is partly due to the relatively strict requirements on market entry and participation. The DPMS sector is considered as a heightened level of ML risks and a low level of TF risks by the Assay Chamber, with 90% of participants in this sector micro or small enterprises. But it is characterised by the dominance of certain regions, based on geographical, climatic and historical factors (e.g. regional specialisation), which lead to a significant differentiation of the level of ML/FT risk in different segments. The FTS and Assay Chamber's understanding is reasonable and in line with the NRA results.

506. Supervisors of auditors conducted a risk assessment in 2017, and briefly analysed threats, vulnerabilities, risks of using the sector in ML/TF schemes, and risk mitigation measures. The assessment shows that poor-quality auditing and fraudulent actions by customers using auditor services pose the most substantial ML/TF risks. Based on the findings that the auditors had a high level of awareness and the level of vulnerabilities in the sector is close to low, the overall ML/TF risk for the sector was rated as low.

507. Sectoral risk assessments on lawyers have been conducted twice: by the Federal Chamber of Lawyers in 2016, and by the MoJ, together with the Federal Chamber of Lawyers in 2018. These considered threats, vulnerabilities, risks and risk mitigation measures, and the 2018 version also took into account the results of the national risk assessment. The legal professionals sector is assessed as low risk for ML/TF by Rosfinmonitoring and the GPO, with the same methodology as other DNFBPs.

508. Supervisors of lawyers, notaries and auditors had the same view that the low risk of these sectors is mainly due to the limited activities they undertake – they do not buy or sell real estate on behalf of their clients, manage clients' money or organise the creation, operation or management of companies (except notaries who may certify related contracts) – and their generally low level of involvement in suspicious transactions. The risk understanding of the supervisors is reasonable; however, it requires a better understanding of the ML/TF threat exposure of the sectors as a whole, and of the vulnerabilities of different participants. In addition, supervisors should be familiar with typologies in order to have an adequate view of how the sectors may be abused.

Risk-based supervision of compliance with AML/CFT requirements

Financial institutions

509. Since 2013, supervisory actions by the BoR have been informed by a ML/TF risk-based approach, and have been improved since the update to the risk assessment methodology in 2016/2017, and further deepened following the NRA in June 2018. BoR's supervision aims to limit the high-risk financial services provided by FIs and prevent FIs from getting involved in illegal activities, which is consistent with the findings of the NRA. However, the supervisory model is not fully risk-based and needs improvement.

510. The BoR conducts off-site supervision, as well as both planned and ad-hoc on-site inspections of FIs.

Off-site supervision

511. Since the development of the off-site supervision tools in 2017, the BoR has prioritised off-site supervision. It assesses each institution's "AML/CFT system effectiveness" (as part of the institution's economic performance assessment) quarterly, based on many risk indicators including: involvement in suspicious transactions monitored by remote AML/CFT analysts; potential AML/CFT breaches informed by Rosfinmonitoring; and results of analysis of internal reporting documentation by the BoR. Supervision is conducted based on the results of the assessment: once risk indicators are triggered, the BoR conducts enhanced examination and requests additional documents and information. At the end of this off-site inspection process, a report is issued indicating violations, remedial actions, and follow-up measures.

512. Meetings with bank owners and/or managers or (ad-hoc) AML/CFT on-site inspections can be conducted on the basis of results of off-site supervision. If no risk indicators are triggered, only continuous off-site monitoring (and sometimes meetings with officers) is carried out.

513. Detecting suspicious transactions involving FIs is a priority for remote supervisors, who pay much more attention to transactions related to transferring funds abroad and transit transactions, which is in line with the NRA. However, off-site supervisory measures do not take into account the results of a comprehensive analysis of ML/TF risks and lack an overall review of compliance and control measures of FIs.

Planned on-site inspections

514. Planned AML/CFT on-site inspections are not separate from prudential supervision. There is a legal obligation on the BoR to conduct on-site inspections of CIs every two years (and of non-CIs every three years). Within this legal constraint, the selection of FIs for planned on-site inspections is determined by the prudential risk profile, although it also takes into account the findings from remote AML/CFT supervisors. These scheduled inspections consume a large proportion of the BoR's available supervisory resources. They may in some cases influence the RBA used in AML/CFT supervision (for instance to divert the BoR's time and attention from AML/CFT higher risk entities) and may cause conflicts between priorities when selecting targets.

515. AML/CFT issues may be considered during planned inspections (and were included in around 50% of CI inspections during 2014-18, 32% in 2018). In cases of high ML/TF risks, this may be the sole focus on the inspection, though this is rare (see Table 6.4). Since 2017, the risk profile of each institution has informed the scope and intensity of the AML/CFT component of a planned inspection (indeed, one of the purpose of the on-site inspection is to confirm the off-site findings). The average duration of AML/CFT inspection in planned on-site inspections of credit institutions during 2018 was 24 working days, with the participation of around five supervisory staff. Prior to 2017, the AML/CFT component of planned inspections was based on inadequate consideration of ML/TF risk, and normally on other priorities, for example verifying the implementation of new legislation. Very few planned inspections focus exclusively or principally on AML/CFT, which the team believes is insufficient given the size and risk exposure of the banking sector.

Unscheduled on-site inspections

516. Unscheduled on-site inspections are carried out on the basis of risk ratings (if sustained high-risks are identified) or when the BoR seeks to remedy a particular emerging problem or situation (whether prudential or AML/CFT related). AML/CFT-targeted ad hoc on-site inspections can also be triggered by ML/TF risks, unaddressed repeated violations by credit institutions or unexplained transaction patterns, or by the results of remote supervision.

517. Unscheduled on-site inspections can be conducted on AML/CFT issues alone. However, most unscheduled inspections were conducted for prudential purposes (though with AML/CFT compliance checks included in a growing percentage: from 20% in 2014 to 29% in 2018). There are very few AML/CFT-targeted unscheduled on-site inspections. Unscheduled inspections which did include AML/CFT were conducted with the participation of 3-5 specialists for around 19 days on AML/CFT issues. Russian authorities indicated that if the AML/ CFT issue is included in the on-site inspection, then it is treated as a priority.

Overall impact of inspections

Table 6.4. Number of planned and ad hoc inspections of CIs

year	Planned inspections			Ad hoc inspections			Off-site AML/CFT supervision
	Total	incl. AML/CFT	exclusively on AML/CFT	Total	incl. AML/CFT	exclusively on AML/CFT	Supervisory activities in which violations were identified
2014	551	327	19	266	55	3	555
2015	454	230	4	193	38	3	206
2016	408	202	3	177	34	5	425
2017	341	180	3	119	33	1	222
2018	286	91	1	98	29	2	313

518. After improving the remote monitoring tools, off-site supervision carried out by the BoR shows effectiveness in detecting suspicious activities and detecting non-compliance with STR filing requirements, as more breaches have been identified with supervisory measures reflected quickly. However, supervisors cannot adequately

detect violations by FIs only through remote analysis of internal reports or other requested documents. In order to improve entities' compliance and ensure prompt remediation of problems, on-site supervision is indispensable. On-site supervision of a general nature (i.e. not exclusively focused on violations already identified through remote supervision) is also an essential tool.

519. Assessors are concerned about the insufficient number of on-site inspections of AML/CFT issues, and are particularly concerned about the declining number of such inspections as the BoR shifts its focus to off-site AML/CFT supervision. While recognising the BoR's strategic decision to move to a primarily off-site model of supervision, and their view that reliance on on-site inspections is outdated and costly, the assessors nevertheless consider that the current model is over reliant on remote forms of supervision, and has insufficient flexibility to schedule on-site inspections based on AML/CFT risks (as opposed to prudential risks).

Non-credit institutions

520. AML/CFT supervision of non-credit FIs has also only recently moved to a risk-based approach. For each supervisory activity, the BoR's supervisors considered ML/TF risks to determine the scope and intensity of AML/CFT inspections. As Table 6.5 shows, there is a steadily increasing trend of on-site inspections and off-site supervision of Non-credit FIs from 2014 until 2017, but the number of inspections has since declined, with a sharp decrease of planned inspections in 2018, which is due to the recent development of a risk-based approach and the off-site supervision technologies after mid-2017. Said "technologies" allow supervisors to access to databases and obtain more information from entities. Supervisors indicate that if high ML/FT risks are detected during remote supervision and if it is impossible to obtain the necessary information remotely, an on-site inspection is conducted. However, for example, some risks and violations may not be detected remotely but may be identified during on-site inspections, thus it could be missed by supervisors if predominantly focusing on remote supervision.

521. Based on a simple calculation, Russia seems to be investing significantly more resources into ensuring compliance by the sector they have categorized in the SRA as moderate risk (i.e. Microfinance), instead of investing resources into heightened risk sectors, especially for the insurance sector. And comparatively, more supervisory activities should be carried out for CIs, although this may also be an indication that non-credit FIs were not adequately supervised on a ML/TF risk basis before 2017.

Table 6.5. Number of planned and ad hoc AML/CFT inspections for non-credit FIs

	2014			2015			2016			2017			2018		
	Planned	Ad hoc	Off-site	Planned	Ad hoc	Off-site	Planned	Ad hoc	Off-site	Planned	Ad hoc	Off-site	Planned	Ad hoc	Off-site
Securities Market Professionals	8	2	22	11	0	47	4	0	46	2	0	15	3	2	20
Insurance Entities	7	1	93	13	2	60	16	0	54	6	0	54	3	1	25
CCCs	6	0	82	7	1	166	7	1	253	38	5	464	7	3	408
Micro-Finance Organisations	1	0	134	5	0	229	13	1	309	12	0	395	2	2	355

Other supervision activity

522. The BoR has sufficient resources to conduct risk-based supervision. Within the BoR, its headquarters, six main branches, and each of the BoR's 80 regional divisions have officers responsible for AML/CFT supervision. The headquarters and main branches in the AML/CFT structure co-ordinates and controls the activities of regional AML/CFT divisions, including oversight of the 11 largest and systemically important institutions. As of January 2019, the BoR's AML/CFT Divisions had 1 030 employees, of which 260 employees worked in the central office, and others in regional offices. Another 270 employees of the Inspection Department could carry out inspections on AML/CFT issues.

523. The BoR supervision verifies compliance with AML/CFT requirements such as recording, storing and presenting information on activities subject to mandatory controls (mandatory reporting, approving and updating the rules of internal control, the appointment of special officials and their training, etc.) and the implementation of internal controls (CDD, assessment and risk management of clients, suspicious transactions reporting). The BoR also verifies that FIs have tools to implement TFS (e.g. existence of databases and screening databases against the lists every three months), while Rosfinmonitoring verifies that each FI incorporates the updated lists without delay.

524. Since the introduction of an RBA, the purpose of the inspections varies from case to case. For high-risk institutions, the intensity of inspections is increased, for example by requesting more information on their performance, expanding the scope of examinations or designating authorised representatives. Other supervisory measures, such as meeting with the management bodies, issuing recommendations, and providing training events for reduced risk FIs are implementing. However, it is unclear how the SRA informs the supervisory activities.

525. Rosfinmonitoring has conducted AML/CFT-specific on-site and off-site inspections on payment operators using a risk-based approach. For high-risk institutions, on-site inspections and desk-based reviews are conducted to verify compliance with the AML/CFT requirements. For institutions rated as having a moderate level of risk, Rosfinmonitoring conducts off-site reviews and applies remote corrective measures such as issuing letters on deficiencies in the internal control systems. For low-risk institutions, preventive measures such as training, outreach letters and events are conducted. The duration of the on-site inspection does not exceed 30 days, while the desk-based review takes less than 90 days, depending on the complexity of the test, with 3-5 supervisors involved. There were around 2 000 payment operators and the percentage of on-site inspections steadily declined from 4.8% in 2013 to 1.5% in 2017/2018, showing a decreasing number of risky institutions over time. Rosfinmonitoring employs 50 AML/CFT supervisors.

526. Postal and telecommunication operators received planned supervision including inspections based on a risk-based approach, in which AML/CFT inspections were considered when making annual planning. Based on different categories of overall risks assigned to each entity, on-site inspections are carried out for the groups of significant and moderate risk and remote supervisory activities are conducted for moderate and low risk. Each on-site inspection is carried out by 3-5 supervisors with a duration depending on the complexity of the activities but usually does not exceed 20 days. Specific AML/CFT supervisory activities were carried out when potential risks

or violations were found mainly on a documentary request basis and mostly informed by Rosfinmonitoring.

527. The Personal Account on the Rosfinmonitoring website is a key supervisory tool. This plays an active role in off-site monitoring and helping supervisors find risks or identify non-compliant behaviour in order to utilise a risk-based approach (e.g. indicating a possible weakness in implementing new requirements if an institution's compliance staff have not yet accessed guidance on those requirements through their personal account). It provides a platform for the communication between supervisors and regulated entities, and a mechanism to increase awareness of legislative requirements and risks. Supervisory documents including requirements, guidelines, TFS lists etc., are posted, and internal control rules and mandatory/STR reporting were received. Supervisors can get a view of an entity's own risk rating and compliance with AML/CTF/CPF requirements by reviewing information and questionnaire responses provided by the entity, or through monitoring whether entities download TFS lists and conduct on-line training. Entities could independently identify problems of implementation of internal control and voluntarily take remedial actions.

528. Supervisors (esp. the BoR) have a good relationship with other authorities (e.g., GPO, FTS, RCS and LEAs). Rosfinmonitoring has concluded co-operation agreements with all supervisory authorities, which set out a framework within which information is exchanged such as on registration, high-risk entities, typologies, supervisory results of compliance of entities, schemes and methods of ML/FT. In addition, Rosfinmonitoring reports to supervisory authorities about identified violations of the AML/CFT legislation in their supervised sectors. Information not covered by agreements can also be exchanged by sending requests to related authorities.

DNFBPs

529. Most DNFBP sectors undergo supervision for conduct of business purposes, which can include AML/CFT issues; except for the real estate sector, for which Rosfinmonitoring has conducted AML/CFT specific supervision. AML/CFT supervisory activities were carried out when potential risks or violations were found mainly on a documentary request basis and mostly informed by Rosfinmonitoring. The Personal Account is widely used among DNFBPs, and acts as an off-site monitoring function to some extent, as well as helping entities to improve compliance.

530. According to the results of the NRA, the gambling sector is classified as low risk for ML/TF. Rosfinmonitoring provides information on the risks identified, suspicious activities and the use of Personal Accounts by entities to the FTS, who carry out inspections on internal controls and AML/CFT compliance. The FTS also monitors the payment of winnings provided in real time by casinos, betting offices and lotteries, based on which supervisory activities would be conducted when ML/TF risks identified.

531. The majority of real estate agents operate as individuals or small businesses. Other intermediaries such as notaries and lawyers cannot engage into real estate transactions. Rosfinmonitoring's regional offices directly interact with the private sector and carry out on-site and off-site inspections (with an average of one third of their staff allocated to supervision roles). Rosfinmonitoring's central office provides methodological support, risk assessment and planning of supervision activity. The

personal account is frequently used to request information, inform risks and warnings of non-compliance. Rosfinmonitoring confirmed that the few high-risk real estate entities were inspected, while off-site supervision included around 70% of the sector. Other control measures came into force to mitigate risks such as introduction of "property information disclosure" to prevent manipulation of prices and mechanism to prevent multiple resale. The risk associated with cash transactions in the real-estate sector is a main focus of Rosfinmonitoring. Transactions above RUB 300 000 (around EUR 40 000) must be automatically reported to Rosfinmonitoring, from which it could have a view of and monitor cash transactions. Rosfinmonitoring note that the lower mortgage rates offered in recent years have reduced the use of cash in real estate transactions, although cash remains one of the preferred methods.

532. Supervisory measures taken by the Assay Chamber include conducting scheduled and unscheduled on-site inspections and documentary checks, requesting information and operations reports from supervised entities, requiring entities to fill in a questionnaire in personal account on the Rosfinmonitoring website to assess risks, and carry out outreach activities. The Assay Chamber conducts on-site inspections on high and significant ML/TF risk entities. Documentary checks are carried out on significant risk entities, an annual program of preventive measures is developed for entities with a moderate level of risk, and control over entities with low risk is carried out on the basis of requests for information and analysis of mandatory statistical reporting. When selecting the targets for inspection, the Assay Chamber mainly considers the availability of information on violations of AML/CFT legislation and/or involvement in conducting suspicious operations received from Rosfinmonitoring and other federal executive bodies, citizens and organisations, risky activities (e.g. performing export-import operations) conducted according to the sectoral risk assessment results, compliance with regional risk criteria.

Table 6.6. Supervision of DPMS

	2013	2014	2015	2016	2017	2018
on-site inspections (entities with high and significant level of risk)	340	538	501	563	764	703
documentary checks (entities with significant level of risk)	116	150	282	193	183	426
preventive measures (entities with moderate level of risk)	4741	5013	5129	5256	5339	5402

533. Auditors and accountants are supervised by the MoF, the Treasury and the SROs of auditors. Participants within the sector are divided into three levels of risk, depending on which the frequency of checks for the external quality control is carried out. High risk entities (audit for socially significant economic entities) are checked by SROs of auditors and the Federal treasury every three years; generally medium risk entities (other audit organisations) and low risk entities (individual auditors) are checked by SROs once every five years. However, the checks are for prudential purpose with AML/CFT issues inspected by SROs, and the risk criteria is not an ML/TF basis.

534. Lawyers and notaries also face a low level of ML/TF risks according to the NRA, and receive prudential supervision. As pointed out previously, the AML/CFT supervisory activities were carried out when potential risks or violations were found

mainly on a documentary request basis and mostly informed by Rosfinmonitoring. For the period from 2017 to 2018, notarial chambers have initiated 83 disciplinary proceedings against the notary due to non-compliance with AML/CFT requirements.

535. Legal professionals do not experience routine AML/CFT supervision. The GPO oversee the implementation of laws by government bodies and heads of commercial and non-profit organisations, although not formally identified as the AML/CFT supervisor for legal professionals, carry out some inspections and has identified a number of violations for legal professionals who did not complying with the legislation and were subject to administrative fines.

Remedial actions and effective, proportionate and dissuasive sanctions

Financial institutions

536. The BoR has a range of supervisory remedial measures and financial sanctions available. These include preventive measures (warnings, written notices to management, meetings) and enforcement measures (issuance of orders on the elimination of violations, monetary penalties, restrictions on individuals conducting financial activities, restrictions on the scope of operations, revocation of licence). Warnings have rarely been issued to CIs after 2014, and officials are informed directly instead.

Table 6.7. Sanctions for AML/CFT violations by CIs

	2013	2014	2015	2016	2017	2018
Warnings	247	233	0	0	0	0
written notice to the BOD/management about the shortcomings in its activities	181	196	509	334	307	598
Meetings	15	14	21	53	15	20
Fines on CIs	218	234	117	209	232	332
Average amount of fines on CIs (thousand RUB)	67.4	71.3	223.4	554.3	734.3	309.2
Fines on officials	55	69	61	102	133	87
Average amount of fines on officials (thousand RUB)	15.8	16.4	21.0	24.7	28.8	31.1
Limitation on certain transactions[60]	97	128	136	109	44	38
Bans on individual banking operations[61]	17	10	12	7	1	3
Orders on elimination of AML/CFT violations	136	95	226	189	159	359
Total number of licences revoked (includes AML/CFT reasons)	32 (8)	86 (36)	93 (34)	97 (35)	51 (24)	60 (35)
Number of revocations of licences only due to AML/CFT violations	2	11	10	0	0	2

537. Supervisors take a graduated approach to promoting and enforcing remedial actions to address deficiencies identified through inspections. They usually first

60. Meaning quantitative limits on certain transactions e.g. the maximum volume of transactions conducted by a credit institution, during a specified period of time, with all its clients or with a particular client.

61 Meaning that a credit institution is prohibited from making specific operations (specified by the BoR), no quantitative limits apply.

provides opportunity for the institution's explanations, and then may issue a "Rectification Order" with a deadline for remediation. The institution is required to submit a list of measures it will take to prevent further violations, including actions on personnel (reprimands, deprivation of the bonus, replacement, dismissal), remediation measures for systems and controls (refining software, modifying internal control rules, enhance control over monitoring of transactions, improve performance etc.), increasing staffing or resources allocated to the relevant tasks, conducting audits, or organising training events. The BoR regularly reviews the status of remediation, hears reports from senior executives, and guides the follow-up work until the deficiency is addressed in a satisfied manner. If the FI fails to comply by the deadline or more risk triggers are identified, then more intensive measures and/or financial sanctions are applied.

538. The choice of a particular sanction takes into account the number and severity of the violations as well as the level of ML/TF risks of the institution. The type of sanction, including the amount of monetary penalties, becomes more severe for repeated violations. However, sanctions are not sufficiently dissuasive, particularly monetary sanctions. The average amount of fines on CIs increased for the period from 2013 to 2017, and dropped in 2018. The amounts are not sufficiently dissuasive in light of relatively low amounts (averaging about 734.3 thousand RUB, approx. EUR 10 000, per CI in 2017). The imposition of ancillary sanctions on individuals with regard to providing financial services and restricting transactions of credit institutions publicised the poor performance of officials and appear more dissuasive, although they are used to a significantly less extent.

539. As shown in Table 6.7, the use of most types of remedial actions and sanctions increased from 2017 to 2018, especially Notices, Orders and fines. There was a slight increase in the total breaches identified in 2018 (5%, from 2 428 to 2 538), while at the same time the number of breaches committed by high-risk CIs decreased - since the number of CIs in the high risk category itself halved. This may indicate an effective use of remote supervision to identify more breaches on less risky CIs, and also shows the use of the full range of penalties. Russia has provided examples of remedial actions to help CIs improve compliance and also of medium- to heightened-risk CIs which have progressed to losing their licence during one year.

540. Revocation of a financial institution's licence is the most severe supervisory sanction available to the BoR. This has been used in a number of circumstances in the last five years. Revocation of a licence is typically applied only following unaddressed violations of prudential and/or AML/CFT requirements, although there are also cases where it was applied due to a very limited number of serious breaches. Authorities explain that AML/CFT and prudential problems often form a mutually reinforcing spiral in seriously troubled institutions. In past cases, banks have weakened or abandoned their AML/CFT controls in an attempt to attract illicit funds to solve problems of liquidity or solvency. Equally, the loss of business as a result of supervisors' findings of AML/CFT violations can seriously affect the nature and volume of business – particularly for a small or specialised bank. By the time a bank's problems become so severe that licence revocation is considered, it is frequently impossible to clearly assign the revocation to either AML/CFT or prudential causes only. Nevertheless, there are some cases where revocation has been undertaken for AML/CFT reasons only – including the two revocations effected in 2018.

541. Revocation of a banking licence is effective and dissuasive. It could also be considered proportionate, given the context and evolution of the financial sector throughout the last three decades, as mentioned above in Chapter 1. The example below shows that the BoR had to resort to this measure after being unsuccessful in remediating important failures for a long time.

Box 6.1. Case of Bank Licence Revocation in 2018

During monitoring activities, the BoR established that Bank U had been involved in suspicious cross-border transactions for a long-time. A number of supervisory activities were carried out repeatedly (6 times during 12 months) and a number of actions were taken, including meeting with officials, issuing Notice and Orders to address the identified violations, imposing fines, and even imposing restrictions on attracting funds from individuals. However, Bank U did not decrease the volume of these suspicious cross-border transactions. The BoR also found that the Bank U carried out high-risk transactions associated with the sale of cash proceeds by retail companies, and the BoR was convinced that the management and owners of Bank U negligently did not take effective measures aimed at preventing the involvement of its clients in suspicious activities. In these circumstances, the BoR decided to revoke the banking licence of Bank U.

542. The sanctions imposed on non-credit FIs increased from 2013 to 2017 before falling back in 2018, which is in line with the trends of supervisory actions taken by supervisors. Preventive measures were increasing in 2018 by means of meetings, calls to inform about shortcomings identified in NCFIs activities, and recommendations for remediation, as a result of off-site supervision. Very few violations on the identification of BOs and PEPs were found before 2016, but the number increased in 2017 and 2018, which showed a raising attention on FIs' performance in these areas. Most of the violations found were related to internal controls, record-keeping and freezing of assets. There were around 3 800 violations (violations were counted by each client and transaction) found on the below NCFIs in 2017, most of which were violations related to internal controls and the identification of customers. These figures may show that supervisors were tightening supervision and reducing tolerance for violations from 2014 to 2017, at the same time, show that the breaches are persistent and non-compliance does not seem to be on the downward trend. As the new remote supervision tool has recently been introduced, more time is needed to assess the effectiveness of the tool.

Table 6.8. Sanctions for AML/CFT violations by non-credit CIs

	2014	2015	2016	2017	2018
Preventive measures			-	709	892
Warnings (Total)	363	485	529	782	554
Securities	33	30	31	9	10
Insurance	86	51	32	38	17
Micro-finance	133	198	239	324	235
CCC	88	158	215	395	276
Management Co.	12	15	7	16	14
Private pension funds	11	33	5	0	2
Fines (No. [amount] in thousand RUB)	47[6,120]	64[5,100]	107[9,632]	113[10,750]	109 (8588)
Securities	6[960]	9[650]	8[550]	2[400]	1 (50)
Insurance	6[1100]	14[1090]	18[1121]	12[805]	5 (870)
Micro-finance	25[2860]	25[2500]	42[4901]	39[2585]	27 (2950)
CCC	9[500]	11[610]	31[2510]	59[6910]	43 (4718)
Management Co.	1[700]	1[50]	1[50]	1[50]	0 (0)
Private pension funds	0	4[200]	7[500]	0	0 (0)
Orders to eliminate AML/CFT Violations	0	1060	921	1927	1626

543. Rosfinmonitoring issued orders, imposed administrative penalties, suspended activities, and disqualified officials when violations were found. Roscomnadzor only issued orders and imposed fines on entities or officials. According to the results of the inspection, Rosfinmonitoring and Roscomnadzor impose fines on the entity or the person who committed the offense and at the same time give an order to eliminate the violations within a short period of time. If the violations failed to be eliminated, more stringent sanctions would be imposed including disqualification of officials or suspension of activities. Preventive measures and sanctions imposed on officials were actively imposed. As more than 90% of the subjects monitored by Rosfinmonitoring are either individual or micro enterprises with insignificant amounts of income (no more than 10 thousand euros per year), fines imposed are relatively low. For example, the average amount imposed on a real estate participant in 2017 is RUB 63 000 (approx. EUR 870). Supervisors indicate that in recent years, the number of AML/CFT violations is decreasing.

DNFBPs

544. Real estate agents, dealers in precious metals and stones and gambling participants can be sanctioned in the same way as FIs (i.e. in accordance with article 15.27 CAO). In practice, warnings, orders to eliminate the violation within a certain period of time and an administrative penalty are commonly used by supervisors as remedial actions. Sanctions are imposed progressively based on the nature and severity of the violations.

545. Since 2014, Rosfinmonitoring has issued on average around 200 Orders to legal entities of realtors and 155 Orders to officials, suspended 55 organisations' activities, and executed disqualification of 15 officials subject to AML/CFT violations. Monetary penalties were imposed on both legal persons and natural persons.

Violations and fines showed a decreasing trend which may indicate sound supervisory measures had been carried out. Assay Chamber suspended activities on 14 entities, 9 of which in 2017, and disqualified three officials in 2015. Orders were issued and fines were imposed on entities and officials (see Table 6.9). For those entities or individuals being punished, sanctions imposed seems proportionate and to some extend dissuasive since around 90% of DPMS are small and micro-business, and less violations were found during the follow-up inspections. Based on the NRA, a program was adopted in order to increase the transparency of DPMS sector, to improve the procedure for special registration and to expand the powers of the supervisory authority. Thus, considering the total number of participants in the DPMS sector, more remedial measures are expected.

546. In 2017 and the first half year of 2018, 146 and 607 protocols on administrative offenses were drawn up by FTS on gambling sector. FTS issued administrative offenses and made instructions and recommendations to address non-compliance. In total, 45 fines amounting to RUB 730 000 were imposed in 2017 and 216 fines were imposed in 2018 amounting to RUB 5 005 K .

Table 6.9. Sanctions for AML/CFT violations of real estate agents and DPMS

		2014	2015	2016	2017	2018
Real Estate Agents	Fines on entities	158	138	76	68	65
	Fines on officials	193	144	61	59	64
	Amount of sanctions (thousand RUB)	22578	21520	13041	8004	8342
DPMS	Orders on entities	36	63	23	149	174
	Orders on Officials	93	111	94	151	192
	Fines on entities	127	54	50	94	101
	Fines on officials	89	48	49	68	84
	Amount of sanctions (thousand RUB)	15,732	5,011	3,470	11,625	21491

547. Remedial actions and sanctions in the form of issuing warnings, orders and suspension of membership were commonly used by the federal treasury on auditors when AML/CFT violations were found for organisation - on average 200 warnings, 50 Orders, and 18 suspensions, but fewer were imposed on individuals - no more than 10 each year. Very few numbers of fines were imposed - about 3-4 for organisations and 1-2 for individual auditors. Lawyers and notaries were imposed disciplinary liability when failed to report mandatory or suspicious transactions. Corrective measure of sending address letters to notaries were conducted to improve the level of AML/CFT compliance. Similarly to DPMS, more remedial measures are expected.

Impact of supervisory actions on compliance

548. Representatives of FIs and DNFBPs that the team met during the on-site visits indicated a positive impact of supervisory activities. Under the guidance and instruction of supervisors, they increasingly understand the AML/CFT obligations and are willing to improve the level of compliance.

549. The overall level of compliance by credit institutions appears to have been improving in recent years (see IO.4). Violations among credit institutions have declined, particularly in 2018, namely for breaches of internal control rules and suspicious and mandatory transactions reporting requirements. This may be explained by the revocation of licence of non-compliant institutions, which embodies a horizontal deterrent effect. It should also be noted that the number of licenced credit institutions has significantly decreased since 2014, which may explain the lower number of violations.

550. The BoR indicates that it works with entities to improve screening systems, maximise their efficiency and automation, optimise methodologies and approaches to identify suspicious transactions, and has instructed credit institutions and NCFIs to attempt to prevent illicit transactions (rather than simply reporting them). Under the instruction, a steady decline in the volume of some types of suspicious transactions has been seen: the volume of suspicious transactions of transfer of funds abroad was RUB 816 billion in 2014, RUB 501 billion in 2015, RUB 183 billion in 2016, and RUB 77 billion in 2017. This may be a sign that institutions are more able to identify and prevent illicit transactions (although it should be noted that the number of wire transfers abroad has also significantly decreased since 2014) and criminals have been deterred from using the financial sector for ML. However, the overall level of breaches is still high (see IO.4).

551. It should be noted that a significant number of violations are still found in the financial sector, including credit institutions (see IO.4). This may reflect the use of automated tools to identify more violations; nevertheless, assessors are concerned by the number of credit institutions that are still found to be non-compliant with key AML/CFT provisions.

552. It is noted that the BoR has had to resort to extreme remedial actions such as revoking licences in a number of cases, which shows that remediation of violations by some credit institutions was not forthcoming. While revocation is a useful tool to eliminate some market participants that consistently fail to comply with AML/CFT requirements, and also a deterrent for future violators, this sanction would not be applicable in all circumstances (e.g. for systemically important FIs). There is also a concern that mid- to large size credit institutions would lack incentives to comply with lesser sanctions.

553. Rosfinmonitoring carries out remote monitoring of compliance with mandatory requirements by supervised entities on an ongoing basis, and assesses the level of AML /CFT compliance in all sectors. As mentioned before, a special role is played by the Personal Account on the Rosfinmonitoring portal, which allowed FIs and DNFBPs to assess their ML/FT risks and to remotely eliminate deficiencies in internal controls. In recent years, as reflected by indicators in the Personal Account, there was an increase in the share of law-abiding institutions among institutions that registered in Rosfinmonitoring for each sector in the area such as internal controls requirements, TFS obligations, taking training program, reporting, and voluntary co-operation. There is a trend of growing use of Personal accounts by DNFBPs.

554. Supervisors in Rosfinmonitoring have seen a gradual decrease in the involvement of transactions in shadow schemes (e.g. carrying out lending activities without a licence) - in the sector of payment operators from 2013 to 2017 decreased by 2.5 times, in the sector of realtors for the same period - by 5 times, and found the

proportion of violations eliminated by the entities under its supervised ambit is increasing. Roscomnadzor increased inspections since 2014, and found more violations, while the proportion of violations eliminated achieved 100%. The volume of suspicious transactions performed in the sector of telecom operators for the period 2013-2018 as a whole had decreased by more than 4 times, and in the postal sector - by dozens of times.

555. Though a steady increase is seen on the proportion of violations eliminated by REs to the whole violations, there were still on average around 5% of repeated violations on the AML/CFT requirements are committed by institutions. In addition, some institutions met did not consider that the level of the fines was a significant incentive towards greater compliance, and indicated the incentive arose instead from the reputational damage within the market associated with the publication of the fact that a penalty had been applied.

Promoting a clear understanding of AML/CFT obligations and ML/TF risks

556. Supervisory authorities have a variety of ways to improve the level of understanding by the private sectors of the requirements in the field of AML/CFT and ML/FT risks through the issuance of guidelines, publication of typologies, explanations and feedback, publishing documents on the official websites and in the Personal account, holding seminars, forums, organizing training events, compliance survey etc. Supervised entities that the team met during the on-site visit indicated that the above actions were necessary, useful and helpful. However, the DPMS sector is not well informed of the ML/TF risks (see IO4). Guidance and typology to some specific sectors, namely the NCFI sector, are not sufficient and not detailed enough to provide reporting entities with clear, specific and in-depth information (such as on the implementation of BO requirements).

557. The official websites of supervisory authorities provide methodological and practical assistance to supervised entities on new requirements, new schemes, new risks identified, thematic sections on AML/CFT/PF and most frequently encountered violations. The BoR communicates to FIs typologies of ML behaviour, which FIs need to use to monitor patterns of transactions. The Personal Account maintained by Rosfinmonitoring is used by Rosfinmonitoring to communicate directly with each supervised entity (such as to communicate new TFS lists, the NRAs, sectorial assessments, and new STRs typologies and codes). There were 65 000 REs connected to the Personal Accounts by the end of the on-site visit and around 1-2% DNFBPs who were not yet registered. Institutions met during the on-site visit found Personal Accounts useful.

Box 6.2. The Role of ITMCFM

The ITMCFM plays a key role in promoting a clear understanding of AML/CFT obligations and ML/TF risks. It achieves this objective by conducting training and research in the field of AML/CFT as well as publishing translated FATF related documents. The ITMCFM, together with the professional community and supervisory bodies, has developed

specialized masters' degree programs in partnership with a network of universities, aimed at training future employees of both government agencies and the private sector. Graduates of these programmes are employed throughout both the public sector and financial sector in AML/CFT roles.

In addition, the ITMCFM provides extensive training to employees of reporting entities (managers, chief accountants, lawyers and employees responsible for the organisation and implementation of internal control). The training programme includes: the international AML/CFT system, the institutional and legal framework of the Russian AML/CFT system, experience in implementing risk-based approach, internal control rules, TFS obligation, the rights and obligations to carry out operations with monetary funds or other assets, requirements on reporting to the Rosfinmonitoring, criteria for unusual transactions, ML/FT risks and typologies etc. Since 2013, the ITMCFM and its partner organisations trained more than 80 thousand persons in the form of targeted briefing for AML/CFT purposes. 86% of trainees found training to increase the efficiency of their professional activity.

558. The Compliance Council plays an active role in promoting risk understanding, discussing compliance issues and sharing information and best practices among supervisors and supervised entities, which operates in all federal districts and local units with more than 100 leading experts in the field of AML/CFT. Since 2018, over 200 meetings have been held, 18 new typologies of suspicious activities have been reviewed.

Overall conclusions on IO.3

559. Supervisors have recently improved the risk-based approach to supervision. The BoR has implemented some aspects of risk-based supervision since 2013 and improved it in mid-2017, however, the risk understanding on the sectorial and individual levels needs further improvement. The licensing requirements for credit institutions have been strengthened since 2013 and now have largely mitigated the risk of criminals being the owners or the controllers of credit institutions, although associates are still not fully grasped by the controls of the BoR. With the shift towards remote supervision, the BoR is identifying more deficiencies, but the shift has further decreased the number of on-site AML/CFT inspections, which was already low. Even though a number of licence revocations have been applied, sanctions are not effective or dissuasive in all cases and monetary penalties imposed were quite low. While overall recent improvement of compliance among most sectors is noted, the level of violations is still high (see IO.4). DNFBPs supervisors have their own risk assessment method; however, the ML/FT risk understanding is largely improved after the NRA process, and most DNFBPs sectors undergo prudential supervision.

560. Russia is rated as having a moderate level of effectiveness for IO.3

.

CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS

Key Findings and Recommended Actions

Key Findings

1. The risk of misuse of legal persons in the perpetration of money-laundering schemes is high. Based on the information collated during the NRA processes, Russia has a developed understanding of the ML risks posed by Russian legal persons, although the data set on specific vulnerabilities and on the types of abusive activity could be expanded. Russia has identified as main risks the use of straw men and shell companies (e.g. to conceal identity) and foreign persons owning Russian entities in money-laundering schemes (such as to perpetrate fictitious foreign trade deals). TF risk understanding is less developed.
2. Russia has put in place a number of mechanisms which significantly mitigate the higher risks for misuse of legal persons for ML/TF purposes. In particular, there are stringent rules at registration and since mid-2016, the FTS has strengthened the checks to identify inaccurate information and inactive companies. As a result, the accuracy of the Company Register (USRLE) has improved as demonstrated by the drastic drop of companies with indicators of possible fictitiousness (from 1.6 million in 2016 to 247 000 in January 2019, representing roughly 6% of the total legal persons in Russia).
3. The competent authorities regularly access information of Russian entities for their own purposes. There is a good co-operation in investigative activities between FTS and Rosfinmonitoring, as well as between FTS and Law Enforcement authorities. This has resulted in a large number of administrative and criminal sanctions, which contribute to making legal persons less attractive to criminals. The sanctions have, however, a limited range and their dissuasiveness could be improved.
4. The USRLE is considered a source of BO information where (i) all the shareholders who are natural persons are in the registry and (ii) no doubts arise as to other person being the BO.
5. Credit institutions are also a source of BO information. Most legal persons have a bank account (the absence of a bank account is an indicator of fictitiousness and would trigger checks by FTS) although the verification of

information by reporting entities is largely based on the USRLE which may not always contain information leading to the BO. In addition, it remains a challenge to access accurate BO information when a foreign person owns a Russian entity.

6. In 2016, the law established a requirement for all legal persons to maintain BO information and provide it to Rosfinmonitoring and FTS, on request. In practice, mainly the FTS has made use of this feature in the course of tax audits. These checks have focused on high-risk entities from a tax compliance perspective and a reduced number of serious breaches on accuracy of BO information held by legal persons was found.
7. Services to trusts and companies are not specifically regulated as a separate economic activity and are not covered by the AML/CFT law. Services to companies are tightly regulated and monitored. For example, the incorporation on behalf of a third person always requires a notarized legal authorization signed by the incorporator and domiciliation of more than five legal persons at one address is an indicator of potential fictitiousness. Certain legitimate services can and are provided, in particular by legal professionals. Legal professionals are AML/CFT obliged entities, yet they are not properly supervised and, as such, cannot be relied upon to hold adequate, accurate and current basic or BO information.

Recommended Actions

1. Russia should enhance dissuasiveness of fines for failure to provide and maintain basic and BO information, particularly, by increasing the use of ancillary sanctions, namely the disqualification of natural persons.
2. Russia should continue to develop its understanding of the ML/TF risks posed by legal persons and legal arrangements. This should be done by using more sources of information (to include information from vulnerabilities generated by the lack of proper AML/CFT supervision of legal professionals and by specifically looking at the role of intermediaries, gatekeepers and other service providers), and by further enhancing the connection of legal persons with specific types of business conducted, delivery channels of Russian legal persons and geographic exposure. The enhanced risk understanding should feed into the existing mitigating measures to prevent the misuse of legal persons, particularly those of FTS.
3. Russia should enhance the measures aimed at verifying the accuracy of BO information through an even closer collaboration between FTS and Rosfinmonitoring. This can be achieved by:
    a) Rosfinmonitoring and FTS expanding the current risk indicators so that mitigating measures can target not only fictitious and shell companies but also legitimate legal entities that may be misused for ML/TF;
    b) Rosfinmonitoring sharing with FTS all relevant intelligence received on refusal to conduct transactions/open business relationship by FIs/DNFBPs due to inability to conduct CDD or for ML/TF suspicion;

c) Enhancing the mechanisms to assist FIs and DNFBPs to identify and verify BO information. For example, FTS could notify competent authorities or the credit institutions holding accounts of any legal person (i) for which information in the USRLE was updated and (ii) found to be in breach of holding adequate, accurate and current BO information.

4. Russia should extend the scope of the AML/CFT law to all persons who provide as a business legitimate services to trusts and companies. Russia should also ensure that all these persons are properly supervised for AML/CFT purposes, particularly legal professionals, in order to ensure reliable information on legal persons and arrangements.
5. Russia should continue to enhance the accuracy of basic information held by the USRLE.
6. Compatible with relevant domestic and international provisions, Russia should expand the use of the information available through tax channels (particularly the AEOI) in order to investigate legal persons and arrangements involved in ML/TF.

561. The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this section are R.24-25.[62]

Immediate Outcome 5 (Legal Persons and Arrangements)

Public availability of information on the creation and types of legal persons and arrangements

562. There is a variety of information and documentation contained in the company register (USRLE). All legal persons must be registered in the USRLE and must provide information such as, name, address, registration authority, directors, managers and founders. Information on shareholders is available for all types of legal persons, which could be established in Russia (for JSC, only if one shareholder exists and, in case of multiple shareholders, there is data on the holders of the shareholders registers).[63] Most information and documentation contained in the USRLE is publicly available on the FTS website (www.nalog.ru), including the note of inaccuracy and the dates of every update, with exception of documents on the identification of natural

62 The availability of accurate and up-to-date basic and BO information is also assessed by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes. In some cases, the findings may differ due to differences in the FATF and Global Forum's respective methodologies, objectives and scope of the standards.

63 In 2019 banks and other FIs have been exempted from disclosing shareholders information. On 4 April 2019, Russia passed Government Decree 400 exempting companies under foreign sanctions and other to disclose publicly information on their executives, shareholders, subsidiaries, and affiliates. Russian authorities state that this Decree only allows companies not to publicly disclose shareholders. However, they remain obliged to maintain this information and provide it to competent authorities, on demand.

persons (e.g. a director). Relevant information regarding non-commercial organisations is also available on the official website of the MoJ (www.minjust.ru).

563. Detailed instructions about the procedure for incorporation and types of legal persons that may be created in Russia are available on the website of the FTS (www.nalog.ru). The legislation does not provide for the establishment of legal arrangements and Russia is not a party to the Hague Trust Convention.

Table 7.1. Number of legal persons registered in the with USRLE (2014-2018)

	2014	2015	2016	2017	2018
Commercial organisations					
General partnerships	298	253	217	189	145
Limited (commandite) partnerships	498	497	439	367	296
Limited liability companies	3 778 274	3 962 627	3 724 114	3 597 536	3 338 503
Joint stock companies	142 366	126 074	102 293	86 440	73 098
Including:					
Non-public joint stock companies	4415	12 915	19 077	23 380	26 283
Public joint stock companies	227	1 213	1 318	1 262	1 176
Production cooperatives	28 448	21 650	14 870	13 111	10 990
Unitary enterprises	24 066	23 262	21 034	18 624	15 194
Other commercial organisations	17 187	16 011	33 007	12 924	8 768
Sub-total of commercial organisations	3 991 137	4 150 374	3 895 974	3 729 191	3 446 994
Non-commercial organisations					
Consumers cooperatives	82 719	87 043	88 625	86 883	84 086
State and municipal enterprises	294 167	271 091	251 161	243 591	221 433
Other non-profit organisations	291 600	311 923	318 058	311 670	323 903
Sub-total of non-commercial organisations	668 486	670 057	657 844	642 144	629 422
Total	4 659 523	4 820 432	4 553 818	4 371 335	4 076 416

Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal persons

564. Overall, Russia has a developed understanding of the misuse of legal persons for ML, less so relating to TF. The risk assessment of legal persons was conducted as a part of the ML and TF NRAs. A range of information sources was used. For example, law enforcement authorities, supervisory authorities, FIs and DNFBPs were involved in the process by filling in a questionnaire on the ML/TF threats and vulnerabilities, as well as providing comments on the submitted information. In the mentioned questionnaires, interviewees had to assess the level of vulnerabilities of different types of legal persons for their misuse for ML/TF purposes. Other sources included examination of completed criminal cases and financial investigation materials or analysis of Rosfinmonitoring's database on STR related to transactions conducted by legal persons. The FTS was involved by filling in a questionnaire on the ML/TF threats and vulnerabilities, providing comments on the submitted information, statistics and data on incorporation and types of legal persons.

565. According to the ML NRA, legal persons are misused either as front companies to conceal fictitious activity in trade-based ML schemes or to conceal the real owners through strawmen managers/shareholders. Concealment of the BO of a Russian legal person through a foreign complex structure was also identified. All these typologies were attributed a high risk.

566. Limited liability companies (LLCs) are identified as the entity posing the highest threat on the basis of a range of information, such as STRs, criminal cases and survey of the private and public sectors. Russian authorities state that this outcome is determined by a number of factors: (i) ease of registration of such companies, (ii) limited liability of the founders/shareholders for the company's obligations, (iii) the possibility of one person to establish a large number of companies. The wide range of activities LLCs are allowed to engage in also contribute to its widespread use, representing more than 80% of all registered legal persons in Russia (see Table 7.1). Nevertheless, these features do not seem to represent a very sophisticated and in-depth risk analysis of LLCs since they are common (almost inherent) characteristics of this type of legal person. Russia could improve its risk understanding by further enhancing the connection of legal persons with specific types of business conducted, delivery channels of Russian legal persons and geographic exposure. The risk assessment could also take into account the vulnerabilities posed by the lack of supervision of legal professionals and the absence of any AML/CFT coverage for trusts and company service providers.

567. Certain types of legal persons were assessed (such as NPOs) as well as specific sources of funds that can be directed for the purposes of TF (for example, legal funds received from commercial activities). The assessment team considers that the NPO risk assessment would benefit from the incorporation of more granular information (see IO.1 and 10).

568. The NRA found that foreign TCSPs are abused to set up legal persons and arrangements abroad and conceal BO of illegal assets obtained in Russia. This conclusion is further confirmed by the information received by FTS in 2018 through the first automatic exchange of tax information indicating that a significant number of Russian tax residents make use of international structures (around 3 750 individuals had controlling interests in foreign legal persons and 250 are settlors or beneficiaries of foreign legal arrangements).[64]

569. However, the understanding of the vulnerabilities and risks of legal persons through the misuse of service providers is not developed and the role and activities of intermediaries, gatekeepers, or other service providers in Russia are not fully understood. A number of persons can and do provide services to legal persons in Russia, including lawyers, notaries, accountants, and legal professionals. Russia identified around 600 attorneys who can provide services such as consulting legal services (preparing legal documents, providing legal support in the establishment of legal persons and the provision of their activities) but no information was provided on the number of notaries and accountants who would be involved in these activities. Legal professionals are covered by the AML/CFT Law and are able to advise on the setting up of legal persons, legal arrangements (outside Russia) or to manage their assets from Russia, in return for a fee. Legal professionals are not properly supervised (see IO.3), and so little information is available on the relative risks of this sector. There is no separate regulation for other persons to provide services to trusts and companies and these activities are not covered by the AML/CFT framework; competent authorities connect this fact to *de facto* non-existence and impossibility to provide these services (for example, the criminal prohibition to act on behalf of someone else

64 Further FTS investigations identified 37 individuals who were suspected of managing trusts from Russia, but none was subsequently confirmed.

without proper authorisation and the tight controls by FTS on registering shareholders and domiciles).

Mitigating measures to prevent the misuse of legal persons and arrangements

570. Russia has adopted a wide range of mitigating measures which are having a significant impact at preventing the misuse of legal persons. These measures target the higher risk areas identified by Russia and include: tight checks of the FTS to improve the accuracy of information in the USRLE; the actions taken by FTS and LEAs to tackle the misuse of legal persons; legal requirements on legal persons to hold their own BO information and collaboration with FIs to prevent criminal transactions of legal persons.

Accuracy of basic information contained in the USRLE

571. The Russian authorities took a number of measures, particularly since 2017, to improve the accuracy of information contained in the USRLE. These measures in particular target the misuse of legal persons through fictitious persons (strawmen) and inactive (shell) companies. The FTS conducts thorough checks when companies apply to the USRLE for registration or for updating existing information. These include conducting automated checks at registration and on an on-going basis to verify the identity and documents of the applicant natural persons (incorporator, member, head of a legal person) and whether any natural or legal persons have been disqualified from conducting business. The verification also includes checking against indicators of dubious activity, namely whether the founder has multiple companies registered at his/her name ("mass incorporator") and whether the same address is used for several legal persons ("mass registration address"). USRLE also verifies if there is any pre-existing information of previous checks or from tax audits. Where triggers are raised, FTS conducts more thorough checks and could initiate monitoring activities and possible sanctioning.

572. The number of applications for registration refused by USRLE has greatly increased since 2017 (see table 7.2). This is due to the increased monitoring competences granted to FTS, by the increased number of unreliable documents identified and by the number of natural and legal persons which are excluded from pursuing economic activity through legal persons. The FTS is resourced to conduct this verification process, with 250 people specifically assigned for this task. Every region has one registration centre and staff is assigned based of statistical information (depending on workload on a given moment).

Table 7.2. Number of applications for registration refused by USRLE

	2014	2015	2016	2017	2018	Total
Number of decisions on refusal for registration in the USRLE:	236 416	259 087	321 123	452 417	533 783	1 802 826
Including						
At the creation of a legal entity	39 946	42 799	64 937	109 342	160 538	417 562
Based on judicial decision preventing the registration body of certain acts - "l" of Article 23 L129	n/a	3 196	6 944	8 817	11 679	30 636
Based on judicial decision preventing a stakeholder of pursuing economic activity - "m" of Article 23 L129	n/a	7	21	10	0	38
Based on disqualification of administrator – "n" of Article 23 L129	n/a	576	1 009	527	459	2 571
Based on unreliability of documents – "p" of Article 23 L129	n/a	17 801	41 218	78 887	139 774	227 680

573. FTS is entitled to make a record of the unreliability of information about the legal person without a court decision, and has made extensive use of this tool since 2016. As shown in Table 7.3, FTS has identified 30 000 legal persons with inaccurate information in the beginning of 2017. As of January 2018, the number of legal persons in the registry with such deficiency was more than 571 000. Russian authorities assert that the increased figure for 2017 is due to the fact that, during this period, the territorial bodies of the FTS work out the main array of legal persons with signs of unreliability of provided data. The number of unreliable information goes down in 2018, which may indicate that the number of companies with outstanding deficiencies is decreasing. On the records of unreliable data made in 2018, 77.3% were entered in relation to information on the address of the legal person; 12.7% in relation to the director and 10% in relation to the founders.

574. Basic information updating should occur at least once a year or earlier if necessary, either pro-actively by legal persons or at the request of the FTS, if inaccuracies are detected. In the latter case, a note of inaccuracy is introduced in the register and the legal persons are given one month to correct, otherwise they are excluded from the USRLE. Exclusion of the legal person is an administrative decision that leads to its liquidation. FTS indicated that 18% of legal persons having records of inaccuracy updated the information in the USRLE. The rest has been liquidated or is in the process of liquidation.

575. FTS was entrusted with enhanced competences in 2016, when it was granted authority to take measures against natural persons previously involved in the creation of shell/front companies (inactive companies). A legal person which has not provided tax reporting and has not carried out transactions on at least one bank account in the last 12 months is excluded from the USRLE. The checks are triggered by lack of tax declaration, and then focuses on whether the company has conducted bank transactions. Information on bank account movements is obtained directly by Russian FIs or by foreign tax authorities when the company has a bank account abroad, on a needed basis. Where the company is found to be inactive, FTS can liquidate the company administratively.[65]

[65] Legal entities that were excluded from the USRLE did not have accounts in banks located abroad.

Table 7.3. Number of administrative actions by FTS in relation to natural and legal persons

	2014	2015	2016	2017	2018	Total
Legal persons to which a record of unreliability was introduced	n/a	n/a	30 189[66]	571 842	400 771	1 002 802
Legal persons excluded from the register due to having fictitious information or being inactive (art.21.1 of Law 129)	383 367	181 843	655 895	546 518	573 549	2 341 172

576. As a result of the efforts described above regarding the verification of information held in the USRLE, Russian authorities state that the number of fictitious or inactive companies registered was reduced from 1.6 million in 2016 to around 247 000 in January 2019 (approximately 6% of the total number of registered legal persons). These efforts are to be welcomed and the assessment team encourages Russia to continue them, given that strawmen and shell companies are considered high-risk areas.

577. Russia has also introduced an automated system of control over VAT refund (ASK VAT-2).[67] This system allows to identify actions aimed at minimising the difference between incoming and outgoing VAT to be paid to the state budget using shell companies and fictitious invoices which, according to authorities, has decreased the setting up of "shell/front companies.

578. Only the founders can make an application to register a company in Russia. Persons acting on behalf of the founders can only provide the service of handing over corporate documentation to the FTS by way of a power of attorney previously attested by a notary. This is a tool to mitigate the risk that the real founders or controllers of a legal person hide behind another person. However, notaries do not seem to have a full understanding of their CDD obligations when conducting such services (see IO.3).

579. FTS also takes preventive measures against misuse of legal persons for TF. Verifications at registration includes checking that a person in the list of radicalised or terrorist natural persons or organisations cannot be a founder non-commercial organisation. In addition, a person who was previously the head of an organisation recognized as a terrorist and which was liquidated due to a court decision cannot be a founder of a non-commercial organisation for 10 years.

Application and enhancement of criminal provisions for misuse of legal persons

580. Russia has made good use of criminal provisions to mitigate the misuse of legal persons. A measure to mitigate the risk of fictitious information in the register is the disqualification of shareholders. Shareholders who, with proven intent, fail to submit information to USRLE, submit it falsely or in a non-timely manner may be

66 This figure only relates to the second half of the year of 2016.

67 This system compares information about purchases and sales in real time, thus revealing discrepancies in VAT declarations. Just by using this system, in the first quarter of 2018 it was possible to collect additional RUB 107,4 billion for the state budget, which is 11.2% more than the same period of the previous year.

prevented from establishing a company or being a manager/shareholder for up to three years (see Table 7.4).

581. In case of repeated or serious violations by legal persons or their shareholders, the FTS may apply to court requesting to liquidate the legal person (see Table 7.4). These requests to courts were filed by the territorial bodies of the FTS on the grounds of inaccuracy of information about the address of the legal person. The increase in the number of court rulings in 2017 is due to the strengthening of work of the territorial bodies of the FTS in that area. The decrease in 2018 is due to the increasing shift to the administrative domain as of 2016, e.g. introduction of records of unreliable information and administrative liquidation (see Table 7.3).

Table 7.4. Number of actions decided by courts against natural and legal persons for failure to provide accurate information to USRLE

	2014	2015	2016	2017	2018	Total
Disqualified persons who may not hold positions of company director (CEO) for up to three years	705	1786	4014	7210	7919	21 634
Number of companies liquidated under court decision	n/a	2 306	3 600	5 123	2 496	13 525

582. In 2011, the Criminal Code was added with article 173.1, on the responsibility for illegally creating or reorganizing legal persons and article 173.2, on illegally using documents for creating or reorganizing legal persons. These additions enhanced the system's capacity to counteract the misuse of legal persons, with more offences being identified, indictments being brought to court, and convictions being issued, as shown in Table 7.5; on sanctions see below). Although the prosecution rate does not have a stable pattern, the conviction rate is steadily increasing with figures above 40% in 2016 and 2017 and above 50% in 2018, which is deemed a positive result.

Table 7.5. Number of crimes identified, indicted, and convictions in relation to natural persons providing false information, documentation to the USRLE or establishing a legal person with false name

	2014	2015	2016	2017	2018	Total
Number of crimes identified	443	487	1 744	5 278	9 662	17 614
Provision of false information to USRLE (CrC Art. 170.1)	216	219	292	319	182	1 228
Establishment of legal persons through fictitious names – nominees (CrC Art. 173.1)	206	254	935	2 590	4588	8 573
Provision of false documentation to USRLE (CrC Art. 173.2)	21	14	517	2 369	4892	7 813
Number of criminal cases that are sent to court with an indictment	123	207	480	1 997	3 141	5 948
Provision of false information to USRLE (CrC Art. 170.1)	86	97	128	161	90	562
Establishment of legal persons through fictitious names – nominees (CrC Art. 173.1)	30	105	130	499	708	1 472
Provision of false documentation to USRLE (CrC Art. 173.2)	7	5	222	1 337	2343	3 914
Prosecution rate	27,7%	42,5%	27,5%	37,8%	32,5%	
Number of convicted persons	56	67	196	915	1655	2 889
Provision of false information to USRLE (CrC Art. 170.1)	38	44	70	93	54	299
Establishment of legal persons through fictitious names – nominees (CrC Art. 173.1)	10	21	34	128	267	460
Provision of false documentation to USRLE (CrC Art. 173.2)	8	2	92	694	1 334	2 130
Conviction rate	*45,5%*	*32,3%*	*40,8%*	*45,8%*	*52,6%*	

583. Overall, the use of criminal actions against natural persons involved in creating or managing companies under false names and addresses has greatly increased since 2017. This is also the result of information shared by FTS to LEAs, which is increasing since 2015. Co-operation between tax and law enforcement authorities is producing positive results.

Box 7.1. Case example (Information on BO, requested through international co-operation with co-operation between RFM and FTS).

In August 2018, the Cyprus FIU was informed about the embezzlement of LLC "T" by transferring funds on fictitious grounds to investment company "A" (Cyprus) and their further legalisation. Rosfinmonitoring also provided information held by Russia on the identity of the director of LLC "T" to the Cyprus FIU, which was obtained by the territorial body

of Rosfinmonitoring from a FI and other sources, such as the USRLE (in co-operation with FTS).

Due to the lack of information on the founders of a foreign company, the Cyprus FIU was requested to provide information of the BOs of investment company "A", which came to confirm that the director of the LLC "T" and investment company "A" was the same person.

Information about the BO received from the Cyprus FIU was used as evidence in the on-going legal procedure filed by FTS with the arbitration court regarding the subsidiary liability of the persons controlling LLC "T" and investment company "A". Such director (and BO of company A) is currently on the Federal wanted list.

Database on refusals by FIs

584. Rosfinmonitoring and BoR have communicated to banks typologies of potentially criminal transactions through legal persons. Table 7.6 shows that FIs are applying the right of refusal to a certain extent. Since the inception of the database in 2015, more than 1.8 million transactions or new business relations were not conducted or established and RUB 666 billion (around EUR 9 billion) prevented from being transferred. Roughly a quarter of those refusals are related to legal persons who are suspected to be shell companies by Russian authorities. These figures are welcomed, particularly taking into account Russia's profile as a source country of criminal proceeds. The fact that FIs rejected more transactions/business relations in 2016 could mean that the application of CDD is improving, which further discourages criminals from using legal persons to conduct ML through the financial sector. However, the recent downward trend presents some concerns, for the reasons stated under IO.4.

Table 7.6. Banks' refusals to conduct transactions/start business

	2015	2016	2017	2018	Total
Number of refusal to conduct a transaction or to start a business relation	237 681	677 509	582 527	380 309	1 878 026
With respect to legal persons	66 936	151 861	153 474	89 022	461 293
With respect to foreign structures without forming a legal person (trusts)			1	3	4
Amount prevented from transfer (billions of RUB)	135	160	181	190	666

585. Rosfinmonitoring maintains a database related to customers in respect of which FIs have taken the decision either to refuse to conduct a transaction or to open a business relationship due to impossibility to conduct CDD. Russian authorities state that this information is collected and considered by Rosfinmonitoring and is then transferred,[68] on a daily basis, to the BoR in order to be shared with and used by FIs in their risk-based approach. It is not intended to provide an affirmative indication that a particular customer should be declined in services, since it may happen also with *bona*

[68] For instance, information about the (i) FIs that refused, (ii) client to whom such a decision was made, (iii) date of the refusal, (iv) basis of the refusal or (v) transaction (currency, amount, grounds, description of its unusual nature).

fide customers and decision to refuse may be based on other factors, e.g. related to counterparties of such customer. Information is also shared with the FTS, although in processed form (e.g. with identification of tax evasion schemes; participants on such schemes, including the role of each participant; legal persons with signs of fictitiousness and identified BO of those legal persons) providing risk-overviews usually related to shell companies and tax evasion. Rosfinmonitoring receives feedback from the FTS on a quarterly basis about the usefulness of that information when conducting tax inspections. Russian authorities state that, in 98% of cases, such tax evasion schemes were subsequently confirmed by the FTS and, in 2017, allowed this authority to collect evidence of tax violations and informed tax claims for the amount of RUB 14 billion.

Obligation for legal persons to possess information on their BOs

586. In 2016, Russia introduced an additional measure to prevent the misuse of legal persons and improve the possibility to access BO information: legal persons are required to hold information about their BO, to store such information and provide it to FTS and Rosfinmonitoring on request.

587. This requirement has been monitored by the FTS in the course of tax audits, demonstrating that companies maintain BO information and get sanctioned when they do not. FTS conducts initial desk audit analysis that cover all legal persons in Russia and enable it to choose which will undergo on-site checks. Since the establishment of the BO information obligation on legal persons, 20 164 on-site checks were conducted in 2017 and to 14 152 on-site checks were performed in 2018, all related to entities which are in breach of their tax obligations. In the course of these, the authorities requested BO information to around 227 legal persons in 2017 and 2 700 legal persons in 2018, having identified its absence or unreliability in 49 cases and minor technical issues (e.g. untimely provision of BO information) in 1 451 cases.

Table 7.7. Tax inspections on legal persons conducted by FTS

	2015	2016	2017	2018	Total
On-site inspections	30 662	26 043	20 164	14 152	91 021
where shell companies were detected	7 066	7 555	7 758	5 179	27 558
where BO information was requested			227	2 700	2 927
where breaches of identification and provision of information on BOs was detected				1 500, of which 49 on absence or inaccurate BO information	1 500, of which 49 on absence or inaccurate BO information[69] (on sanctions, see below)
Cases sent to LEA	7 001	6 011	4 149	3 272	20 433
Criminal cases opened by LEA	1 826	1 781	1 155	1 458	6 220

588. This activity is performed in the context of tax audits that are assigned on the basis of tax risks or tax non-compliance. Even though in some cases FTS discovers ML

69 The relevant legal provisions defining the procedure for legal persons to provide BO information to competent authorities (GR913) came into force on August 18, 2017. The FTS

activity related to tax evasion and shares information with LEAs, these indicators do not include ML/TF risk indicators, which could be considered when verifying BO information. Overall the activity conducted by FTS, while still fairly recent, is significant and is producing positive outcomes as they seem to indicate that legal persons are complying with the obligation to hold accurate and current BO information to a large extent.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons and legal arrangements

589. Russian authorities are able to access basic information on legal persons from the USRLE. Regarding BO information, there are two different sources: from FIs and DNFBPs or from the legal person itself.

Financial institutions and DNFBPs

590. Banks represent the source of BO information in virtually all cases when the authorities request it from the private sector. Rosfinmonitoring is the main requesting authority, and LEAs request it to Rosfinmonitoring during the course of investigations, or can obtain it from banks for evidence. Rosfinmonitoring and LEAs report that they have no difficulties obtaining information from banks. Rosfinmonitoring applies network analysis to identify funds related to the owners and BOs of legal entities.

591. However, there are challenges regarding the understanding of BO definition and implementation of BO requirements among FIs and DNFBPs (see IO.4). In addition, from interviews with FIs and DNFBPs the assessment team is of the view that they consider the USRLE as a primary source to confirm information provided to them by the legal person regarding BO. While the correspondence of basic and BO information under the USRLE may only occur regarding legal persons with simple structures, the early results obtained by the FTS on the BO information held by legal persons themselves seem to be positive, which mitigates the shortcoming identified in IO.4.

592. A possible challenge to obtain information from banks is that not all legal persons created in Russia may have a bank account in the country, since no such obligation exists. However, Russian authorities maintain that legal persons have an incentive to have a bank account in Russian credit institutions as its absence is an indicator of possible fictitiousness triggering additional checks (as of 1 January 2019, 120 786 legal persons did not have a bank account, which amounts to 2.96% of registered legal persons). This gap is mitigated by the fact that, as noted above, if within the period of one year a legal person does not submit tax reports and does not conduct transactions on at least one bank account (the absence of the bank account is equal to the absence of transactions) is considered to have ceased its activities, being subject to exclusion from the USRLE.

Access and exchange of financial information

593. Banks have an obligation to inform the FTS on bank accounts held in Russia, within a month, on the opening, closing or changing the details of a bank account (i.e. name, address or account number) – article 86 (1.1) of the Tax Code and article 12 (2)

started to send requests of information on BO only at the end of the year. Due to the administrative procedures, breaches were found and legal persons sanctioned only in 2018.

of Law 173. Competent authorities, including MoI, FSB, other LEAs and courts, can obtain information on bank accounts from FTS through the system of inter-agency electronic interaction in the form of the electronic document within hours. In 2018, FTS responded to more than 280 000 such requests, demonstrating a good co-operation with other authorities (see also Box 7.1). Investigative authorities can obtain information on a certain bank account, including the amount of funds on the account, without a court order. This is an important feature since, as explained above, FTS considers the lack of a bank account as an indication of possible fictitiousness.

594. In addition, in the framework of the accession of Russia to the international automatic exchange of financial information for tax purposes,[70] FTS annually receives information from foreign tax authorities on Russian tax residents whose accounts and other financial assets are located in foreign FIs. The FTS also receives information from Russian FIs with respect to customers that are foreign tax residents on an annual basis. In addition, trustees are required to declare the fee they receive for managing assets held by a foreign trust to the FTS as well as the controlling person of the trust. Since September 2018, this framework allows the FTS to obtain data on financial accounts of the Russian taxpayers from competent authorities of 74 foreign jurisdictions. This agreement increases transparency of legal persons and improves the exchange of tax information. Given the risk profile of misuse of legal persons in Russia, there is potential to make greater use of information held by FTS for ML/TF investigations.

Box 7.2. Identification of companies owned in false names

In 2017 Rosfinmonitoring conducted analysis of a number of STRs related to the execution of court orders amounting to RUB 64.5 million (EUR 880 880). It was identified, that the same company M was receiving funds from a number of other companies using court orders, issued by the same court, in a short period of time. As a result of further analysis Rosfinmonitoring detected that company M was owned by a «mass owner» (an individual owning a large number of companies), which indicated that he probably was a straw man, and almost all of the received funds were withdrawn in cash shortly after the execution of transactions. This information was disseminated to MoI in the Penza region, and law enforcement later identified that debts, settled in court, were based on fictitious contracts between companies. This way, the banks could not refuse to carry out transactions when suspicions arise, because the transfers were based on court decisions. As a result, in 2018, law enforcement initiated a criminal case (falsification of evidence) against the BO of company M, who was identified by the bank.

[70] Convention on Mutual Administrative Assistance in Tax Matters dated 25 January 1988; and the multilateral Agreement of the competent authorities on the automatic exchange of financial information dated 29 October 2014.

USRLE

595. In case of simple corporate structures, the USRLE may be used as a source of BO information when legal ownership corresponds to the BO. This information is provided free of charge to a range of authorities (e.g. federal and state authorities, local governments and other state bodies, the BoR, courts).

596. As shown above, FTS has taken significant measures to improve the accuracy of information in the USRLE and to strike off inactive and fictitious companies. While the assessment team acknowledges and commends this, there are a number of issues that arise. First, this increased focus is fairly recent having mostly started in 2016. Second, and more significantly, the registry continues to suffer from limited entry requirements for legal persons in prior years, which is consistent with the very significant number of legal persons that are being excluded from the register (more than 2 million from 2014-2018, as shown in Table 7.3). The fact that the trend of exclusions from legal persons from the registry only started decreasing in 2018 is an indication that the FTS is consistently working to reduce the number of entities with unreliable information. The team deems this result positive and encourages to be continued in the future as it enhances the quality of information held in the registry. However, the team considers the yearly figures noteworthy and the number of entities with unreliable information at the end of 2018 not to be negligible (around 10% of the total number of legal persons registered). Indeed, from the interviews with the private sector and with competent authorities, assessors confirmed that the USRLE is a primary source of information, notably either to obtain BO information or to verify it. The team is concerned with the fact that legal ownership may often differ from BO information in simple company structures, although this is mitigated with the fact that legal persons are broadly compliant with holding accurate, current information on BO, as referred above. Another issue of concern is that the whole system may be relying on flawed basic information to a certain extent since the process to enhance its quality is fairly recent.

Legal entities and legal arrangements

597. As of 2017, Rosfinmonitoring, FTS and their territorial bodies can obtain information pursuant to article 6.1 of the AML/CFT Law, which requires legal persons to hold information on their BOs. This information must be provided to authorities upon request as rapidly as possible but, in any case, not exceeding five working days to competent authorities. In practice, only FTS has made use of this tool to obtain BO information during its tax audits.

598. As referred above, in 2018, the FTS found 49 serious breaches (either absence or inaccurate BO information) and 1 451 minor breaches out of 2 700 requests to high-risk legal persons for tax purposes. As stated above, the actions of the FTS are welcomed and incentivized going forward in order to ensure the availability and accuracy of BO information of legal persons.

599. The FTS indicated that for the tax period 2017 around 3 750 individuals declared having controlling interests in foreign legal persons and 250 individuals in foreign legal arrangements. However, until the end of the on-site, no trustees had been identified by authorities.

Effectiveness, proportionality and dissuasiveness of sanctions

600. The sanction legislative framework provides for a comprehensive range of civil, administrative and criminal liability for non-compliance with the requirements for providing appropriate information on legal persons to competent authorities. In relation with administrative sanctions applied under paragraph 4 of article 14.25 of the Code if Administrative Offences (breaches of registration requirements of legal persons and individual businessman) the following statistics were provided:

Table 7.8. Administrative sanctions on breaches of registration requirements

	2014	2015	2016	2017	2018	Total
Decisions imposing administrative sanctions	17 466	18 130	26 809	39 899	41 112	143 396
Including a fine	7 017	10 688	20 132	33 276	35 327	106 470
Failure to submit or submission of unreliable data	7 000	10 700	17 100	30 900	33 697	99 397
Disqualification of shareholders and directors	705	1 786	4 014	7 210	7 919	21 634

601. The increase in the amount of both administrative sanctions and criminal occurrences may indicate that Russia is giving priority to mitigating the risk of abuse of legal persons. The assessment team particularly commends the increase of the use of ancillary sanctions, e.g. disqualification of shareholders and directors, which are considered to be more dissuasive than pecuniary sanctions, especially those with the indicated figures, since they are not seen as just a cost of doing business, are financially less measurable and can have a deeper and lasting impact of the entities' way of conducting business. According to Russian authorities the minimum amount of fine imposed pursuant to the referred article 14.25 was RUB 5 000 (EUR 65) and the maximum RUB 10 000 (EUR 125).

602. In 2018, the average amount of fine impose pursuant to this provision was RUB 5 140 (EUR 95), which means that the minimum amount is applied to most breaches. Sanctions on breaches of identification and provision of information on BOs by a legal persons also seem to follow the same pattern. Case-examples provided by Russian authorities demonstrate that courts generally convict legal persons for non-compliance with the lowest possible administrative fine (RUB 100 000, EUR 1 250) irrespective of the seriousness of the breach. (Not providing information to authorities or doing it in an untimely manner – which are considered minor breaches by authorities – is given the same importance as absence or inaccurate information – which are considered major breaches by authorities).

603. Available sanctions are not fully proportionate and dissuasive. Administrative fines have a limited range since its lower and upper bands are low (e.g. for breach of identification and provision of information on BO by a legal person, fines range from RUB 30 000 to 40 000 (EUR 400 to EUR 530) on natural persons and from RUB 100 000 to 500 000 (EUR 1 250 to EUR 6 500) on legal persons. Disqualification ranges from one to three years. Criminal fines have the same problem (e.g., an individual presenting false information or setting up a fictitious company is punished up to EUR 4 000 and 7-month of his/her salary) and this is the most frequent form of punishment for crimes regarding articles 170.1, 173.1 and 173.2 (see IO.7).

Deprivation of liberty up to three years (five years if this crime is committed by a group of people by prior agreement) is considered to be dissuasive, although not proportionate given the types of offences in play and especially taking into account the sanctioning context (low minimum and maximum amounts of fines – see R.24).

Overall conclusions on IO.5

604. Overall, risk understanding in Russia is well developed for ML, less so for TF. A range of mitigating measures in place. The USRLE contains a good amount of basic information, and the process to enhance its accuracy is on-going and achieving positive outcomes. The registry may be relied on for BO information only for legal persons with simple structures, when it corresponds to legal ownership. Legal persons also hold information of their BOs. Information sharing between competent authorities is a strong feature in Russia, notably between the FTS, Rosfinmonitoring and LEAs. FIs/DNFBPs and legal persons, are the main source of BO information, which is rapidly accessed by authorities. The assessment team considers that this system is comprehensive and is producing quality outcomes as well. However, interviewed FIs and DNFBPs rely on the USRLE as a primary source for verification of BO information. This weakness is to some extent mitigated by the activity of the FTS in checking BO information held by legal persons which, in turn, are also customers of FIs. The sanctioning regime is not fully proportionate and dissuasive.

605. Russia is rated as having a substantial level of effectiveness for IO.5.

7

CHAPTER 8. INTERNATIONAL CO-OPERATION

Key Findings and Recommended Actions

Key Findings

1. Russia provides MLA in a constructive and timely manner, responding to nearly 6 000 requests per year. The GPO ensures that MLA requests are executed by the appropriate authority and requests are generally answered within one to two months. Wide feedback from the FATF global network on Russia's provision of MLA trended positive, with a few complaints.
2. Russia swiftly considers and executes extradition requests using an administrative procedure. Russia does not extradite its own citizens, but it is prosecuting individuals domestically when evidence is supplied by the requesting state. Extradition for ML has been denied for legal reasons not relating to nationality on a handful of occasions.
3. Russia seeks formal assistance to pursue ML, TF, and predicate offences with transnational elements to a satisfactory extent. Authorities have intensified their efforts to recover criminal assets in recent years, however the level of judicial co-operation sought in tracing and seizing assets in ML cases is lower than expected from a source country for proceeds. The FIU, through its international requests, plays an active role in identifying assets.
4. Rosfinmonitoring facilitates the execution of incoming requests in a constructive and timely manner. The process of exchanging information is regulated through appropriate procedures and guidelines. Feedback from international partners is largely positive. While in a few isolated cases partners indicated concerns about the co-operation received, there do not appear to be major issues concerning the constructiveness and timeliness of international co-operation provided by Rosfinmonitoring.
5. Rosfinmonitoring demonstrates good performance in making requests for assistance to foreign counterparts, with a growing number of outgoing requests in the last six years. The geographic coverage and subject matter of outgoing requests is consistent with the risks identified by the NRAs. Requests for BO information comprise a significant share within the total.
6. LEAs make active use of international co-operation requests through liaison officers and Interpol. However, authorities seem to be over-reliant on

Interpol notices rather than bilateral requests, and the effectiveness of this mechanism is unclear.

7. There are mechanisms for supervisory co-operation, and the BoR exchanges information with its foreign counterparts. Nonetheless, the level of co-operation in this field needs improvement to be fully commensurate with the risk profile of Russia as a source country for potentially illicit funds.

Recommended Actions

1. Russia's competent authorities (including LEAs and GPO) should continue to provide constructive co-operation to all partners sending valid requests.
2. Russia should continue seeking co-operation in asset tracing and confiscation, including from countries outside of its immediate vicinity that receive significant amounts of suspected criminal funds from Russia. Early consultation with countries about the scope of assistance that can be provided regarding asset recovery would be beneficial to increase the chances of success or quicken recovery of assets
3. In light of Russia's extensive use of Interpol, Russia should improve its systems to ensure that in all cases it provides sufficient factual and legal evidence when seeking the surrender of wanted persons.
4. Competent authorities should continue to improve the form and the content of the requests for co-operation sent abroad, notably by providing more identifying information.
5. Rosfinmonitoring should continue and increase proactive spontaneous disclosures to international counterpart, especially those in transit countries, to share information on subjects with a nexus to foreign jurisdictions or transactions with cross-border elements.
6. Rosfinmonitoring should also continue to improve the quality and completeness of its responses, particularly for key proceeds destination countries, ensuring that it clearly communicates to partners whether there are any practical challenges to accessing requested information in specific cases.
7. The BoR should more proactively build relationships with and request information from foreign financial supervisors on the interim and final destination of cross-border money flows, as well as on the basic and BO of the legal entities used in such transactions.
8. Russia should ensure that its case management systems and processes within LEAs and GPO remain harmonised and effectively monitor the progress of all formal requests considering the high volume and the different authorities that might receive MLA requests.

606. The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The Recommendations relevant for the assessment of effectiveness under this section are R.36-40.

Immediate Outcome 2 (International Co-operation)

Providing constructive and timely MLA and extradition

607. Russia generally provides MLA in a constructive and timely manner and swiftly executes extradition requests. This is based on an analysis of the processes in place, interviews with relevant authorities, statistics on the provision of assistance, a review of case examples, and feedback from the FATF global network.[71]

Mutual Legal Assistance

608. Most MLA requests to Russia are handled by the General Department of International Legal Co-operation (GDILC), within the GPO, which processes more than 6 000 incoming MLA requests annually. Requests for judicial co-operation, such as for in-court testimony, are handled by MoJ. The bulk of MLA requests are pre-trial, investigative requests, and these are dealt with through GPO. Since 2017, requests made under the Minsk Convention on Legal Assistance are processed directly between counterpart authorities, so the IC and FSB have joined the GPO and the MoI as competent authorities who can receive and respond to MLA requests within the CIS. GPO is made aware of all incoming requests, even if they are sent directly to LEAs, and tracks all cases, including for the purpose of monitoring internal performance. LEAs have international co-operation divisions that monitor the progress of their own responses, but overall supervision is carried out by GPO. While direct exchanges between counterparts may be timesaving and efficient for frequent partner countries, it also creates challenges to track all requests. In practice, there were no examples of lost requests.

609. GDILC is the competent authority under most of Russia's MLA agreements, including all bilateral agreements, and conducts oversight and co-ordination for all incoming MLA requests. Its role is to review incoming MLA requests for treaty compliance and determine whether assistance should be provided on the basis of reciprocity. Assessors reviewed examples of MLA provided by Russia on the basis of reciprocity, such as a request from Nigeria in a ML case and requests relating to financial crime investigations from Oman and Guatemala, which were granted and treated no differently than treaty-based requests.

610. The process in place to consider and execute incoming MLA requests is appropriate. During initial screening, GDILC verifies that execution of an MLA request complies with Russian law and would not damage the sovereignty or security of Russia. Officials then determine whether any additional information is needed from the requesting state. Based on the assistance requested, GDILC decides which LEA headquarters should execute the request, or refers the request straight to the relevant region or territory if local investigative action is necessary. Assigned investigators decide independently the steps to take to execute the request and obtain approval from

[71] In total, 34 jurisdictions provided feedback on their formal and informal international co-operation experience with Russia in recent years: Argentina, Armenia, Australia, Belarus, Belgium, Canada, China, Cyprus, Denmark, Estonia, France, Hong Kong China, Hungary, India, Indonesia, Israel, Italy, Japan, Kazakhstan, Kyrgyzstan, Latvia, Lebanon, Macao China, Monaco, New Zealand, San Marino, Slovenia, Spain, Sweden, Switzerland, Tajikistan, Ukraine, United States, and Uzbekistan.

the head of their agency or the court, if needed for coercive measures. GDILC counts 112 staff, which is sufficient to deal with the workload of incoming and outgoing MLA.

611. There is a process ensuring that assistance is generally provided in a timely fashion. Russia prioritises its responses based on the urgency of the assistance requested as stated by the requestor and whether the request falls into one of the key risk areas as identified by the ML or TF NRA. This is responsive to jurisdictions and also means that co-operation requests are a source for tracking national risks and identifying leads. An electronic case management system for the entirety of GPO assists in controlling the execution of incoming requests, including document management, although reminders pertaining to individual requests are initiated manually, not automatically. GPO does generate monthly statistical reports on MLA interactions and other forms of international co-operation, including requests dealing with identification, freezing, or seizing of assets (see table 8.1), which helps to gauge on-time performance. GDILC follows up on the timely execution of all foreign requests, including by sending email reminders to domestic authorities. Overall, the system appears to work in practice, as there is no substantial backlog of incoming requests and there were not pervasive concerns mentioned by partner jurisdictions about the timeliness of assistance provided by Russia.

Table 8.1. Incoming MLA Requests (GPO, MoI, IC, FSB)

	2013	2014	2015	2016	2017	2018
Requests Received	5 157	5 292	5 942	6 374	6 350	6 614
Relating to asset tracing	35	48	37	51	33	49
Requests Executed	4 321	4 895	5 212	6 123	6 033	5 952
Relating to asset tracing	21	47	45	48	32	29
Outstanding from Previous Periods	43	261	329	391	377	411
Relating to asset tracing	27	39	37	24	23	18
Requests Denied Due to Lack of Compliance with Relevant Treaty	4	5	76	98	41	23
Requests Returned to Country for Follow-Up Due to Lack of Compliance with Treaty	99	164	81	66	89	45

612. The average length of time required to execute MLA requests between 2013 and 2018 was 1-2 months and this has remained consistent over time. This is relatively swift compared with many jurisdictions' average response times, but assessors note that complicated requests do require longer to execute, especially if they entail numerous investigative actions. The apparent increase in requests outstanding is somewhat concerning. The Russian authorities explained that most outstanding requests are from the latter part of the previous reporting period (i.e., November-December of the calendar year) and that the share of outstanding requests does not generally exceed 6.5% of the total. The number of outstanding requests carried over from year to year is a relatively small proportion of the whole, indicating timeliness, yet it was not possible to determine how many of the currently outstanding requests have lingered for many years or are under long-term consideration without having been rejected or responded.

613. On average, 326 requests per year are partially answered by Russian authorities and the responses are generally supplemented with additional information until fully executed. Delays in MLA execution appeared to stem from the peculiarities of certain treaties (e.g. a treaty with Cyprus with especially strict requirements) and the gradual completion of requests occurred when they necessitated action in numerous territories or districts or when parts of incoming requests required clarifications or phased execution.

614. Co-operation provided by Russia pertaining to asset tracing appears to be adequate. The large majority of requests seeking assistance in identifying assets stem from ML investigations. Four requests have been sent to Russia seeking the identification of assets linked to TF in the last three years.

615. As noted in Table 8.1, a larger proportion of requests relating to asset identification remain outstanding at the end of each calendar year as compared with the entire universe of incoming MLA (66% outstanding versus 6.5%). This is considered normal because these requests often require a relatively more complex investigation. Russia notes that such requests do not often contain sufficient information about the location or identification of the assets, since the very purpose of such a request is to pinpoint assets and determine their true ownership or control. Russia charges pre-investigative authorities with the execution of such requests, which can take more time than the usual two-month response time applicable to other MLA requests. Russia can enforce judgments or sentences pertaining to conviction-based confiscation, although there has not been an occasion to complete such a case yet (one relevant request did not lead to confiscation as the natural and legal persons were not found). Since 2013, Russia has received 39 seizure requests and executed 33 of them (85%); of 27 requests received relating to ML, 25 were executed (93%). Assessors examined recent (2016) case examples of seizure requests executed by Russia from a variety of countries, involving mainly currency or funds held in bank accounts and stemming from drug, ML, and fraud investigations. MoI was the authority that completed the seizure in each case. The relatively new direct enforcement authority contained in the CPC can be expected to streamline the processing of future confiscation requests that meet Russian legal requirements.

616. Russia rarely refuses to execute MLA requests. Legally, it may do so if the requested assistance is likely to prejudice sovereignty or security or is contrary to Russian law. Indeed, there was an increase in requests denied in 2015-2016 attributable to a large number of rejections to one country (87% in 2015 and 78% in 2016). These denials were premised on a likelihood to prejudice the sovereignty, security, public order or other essential interests of Russia. Otherwise, the overall denial rate remains extremely low and has flattened again in 2017-2018. It is a positive feature that Russia applies no monetary threshold in providing MLA assistance. However, there is a domestic threshold related to tax evasion. The offences in CrC Articles 198-99 must be considered large scale to qualify as a crime and, correspondingly, as a basis for ML (see R.3, c.3.4). While the thresholds are much lower than those in other jurisdictions and they are aggregated over time, one extradition request was denied because it involved a *de minimus* amount of taxes evaded.

617. In MLA feedback from the FATF global network, most jurisdictions found Russia's responses to be of satisfactory to good quality, and some noted recent improvements and few delays. One country raised issues with the form of Russian

responses (not the substance), difficulty in obtaining updates on MLA requests, and some delays in receiving the assistance requested. Another noted complications stemming from differences in law and criminal procedure, but affirmed that these issues were able to be resolved through bilateral discussion. One country stated that Russia did not provide bank records for an account thought to be located in Russia, implying that the sensitivity of the subject matter of the request may have been the reason. Predominantly negative feedback about the quality of MLA was provided by 2 out of 34 countries. For one of these, Russian authorities provided recent information about positive co-operation. The other noted significant problems in MLA co-operation in some cases; these cases relate to an on-going political dispute. Co-operation on matters outside the political dispute appears to be proceeding smoothly. Overall, the feedback on MLA trended positive, with some outlying complaints.

618. No breaches of confidentiality were reported, and the fact of the receipt of a request, and its contents, are only disclosed by Russia to the extent necessary for execution.

Extradition

619. Extradition requests are generally swiftly considered and executed. Between 2013 and 2018, Russia received approximately 1 439 extradition requests per year in all criminal cases. There has only been one incoming extradition request related to TF, which was granted in 2013. For ML, over six years, there have been 21 requests. On average, Russia is executing 984 extradition requests per year and is denying 175 per year.

Table 8.2. Incoming Extradition Requests (predicate offences)

	2013	2014	2015	2016	2017	2018
Requests Received	43	70	90	52	27	15
Requests Granted	43	67	90	52	25	15
Requests Denied	0	3	0	0	2	0

620. Of the 21 requests for extradition related to ML, eleven were granted and ten were denied. The reason for six of the ten denials was that the person sought was a Russian citizen. Four of the ten denials involved conduct that did not constitute an offence under Russian law. The assessors saw examples showing that before issuing substantive denials, the authorities considered the requests in a deep and non-perfunctory way. But discounting the denials based citizenship, the percentage of extraditions related to ML that were denied is notable, at approximately 1/5 of all requests. Nevertheless, Russia indicates that the number of denied requests has decreased over time and no extradition request for ML has been rejected since 2017.

621. Overall, Russia extradites eligible non-citizens quickly. The extradition process is administrative in nature and the matter will only reach a court if the wanted individual challenges his or her extradition. There are two procedural issues that can potentially slow down the extradition. First, the General Prosecutor (GP) or the Deputy GP makes the final decision on extradition, and there is no fixed period in which the GP must make a decision. In practice, the decision appears to be timely, but this is a

potential bottleneck. Second, Russia does not extradite Russian citizens (see below) and nationality checks can take up to six months due to the possibility of the suspect having former USSR citizenship and, thus, even unbeknownst to the person, Russian citizenship. While these could theoretically result in delay, no country providing feedback reported trouble with lengthy extradition processes. Assessors found that cases of a non-sensitive nature result in extradition in only 2-3 months after receipt of the request, which is indeed swift, and is comparable to processing times for EU or Nordic arrest warrants or other simplified procedures.

622. Russia prioritises the execution of extradition requests on the basis of how long it can detain a person once he or she has been located. This means that requests pertaining to crimes of small to medium gravity are processed first because the detention period for such crimes is only six months. For serious offences, the detention period can be twelve months and for grave offences, it can be up to eighteen months. While this is a practical approach that increases the chances that a person located and arrested will not be prematurely released (and perhaps the only approach possible under the legal constraints), it may decrease the flexibility of the authorities to permit an urgent ML or TF request to jump the line. Russian authorities note that they will consider extraditions marked urgent, but in reality, most extradition requests are designated as such. If official resources are occupied with handling a request for a person who can no longer be detained by law, then cases of arguably greater importance may have to wait. However, since wanted persons are searched for on a first-come, first-served basis and the procedural clock only starts upon arrest, this is not considered to be a deficiency in practice.

623. Russia demonstrated through case examples that it can act rapidly in extradition matters even when the decision is challenged in court. For example, in a request from Azerbaijan pertaining to embezzlement of USD 60 million, the defendant appealed the extradition. Despite the litigation, in which the defendant was unsuccessful, the total time between arrest and surrender to Azeri authorities was four months.

624. Russia does not extradite its own citizens, but, as detailed in Table 8.3 and Box 8.1, Russia will prosecute individuals when it refuses extradition on the grounds of nationality. The likelihood of prosecution often depends on whether the foreign authority provides evidence sufficient for Russia to open an investigation and bring its own charges. Some of Russia's frequent international partners make requests for prosecution in lieu of requesting arrest or extradition, which they know will be denied on citizenship grounds. The significant number of pending requests under consideration in Table 8.3 may indicate the time it takes to locate the suspect or, alternatively, some delay in submitting the cases for domestic prosecution. Still, the even numbers of requests per year and executed requests per year signify that Russia is generally keeping up with the volume of requests in this busy area of co-operation.

Table 8.3. Foreign Requests to Prosecute Non-Extraditable Russian Nationals

	2014	2015	2016	2017	2018
Incoming Requests to Prosecute Russian Nationals for Crimes Committed Abroad	202	98	106	125	134
Requests Rejected Including for Treaty Breaches	18	5	3	5	3
Requests Pending	184	93	103	120	131
Requests Executed to Prosecute Russian Citizens in Russia	122	129	99	109	127

Box 8.1. Prosecution in lieu of extradition

On 7 April 2015, GPO refused to satisfy the request of Kazakhstan to extradite A, since this person was a Russian citizen. A was charged with intentional infliction of serious bodily harm under the Criminal Code of Kazakhstan. Instead, GPO executed Kazakhstan's request to prosecute A. On 13 July 2016, a court in Chelyabinsk found A guilty of committing a similar crime under Russian law (CrC Art. 111) and sentenced the defendant to imprisonment (3 years) and probation (1 year).

Seeking timely legal assistance to pursue domestic ML, associated predicates and TF cases with transnational elements

625. Russia's ML/TF cases would often have an international dimension, as criminal proceeds are often laundered abroad and TF threats relate at least in part to international groups and the FTF phenomenon. In this context, Russia seeks formal assistance to pursue ML, TF, and associated predicate offences with transnational elements to a satisfactory extent, even though the level of judicial co-operation sought in tracing and seizing assets in ML cases is lower than expected.

Mutual legal assistance

626. Russia sends approximately 4 841 requests for MLA on average every year. An appropriately small ratio of these are denied or returned for technical reasons. The GPO sends the majority of requests, except requests to CIS countries where co-operation occurs directly between competent authorities (see above).

Table 8.4. Outgoing MLA Requests (GPO, MoI, IC, FSB)

	2013	2014	2015	2016	2017	2018
Requests Sent	5 962	5 498	5 351	4 718	4 116	3 403
Relating to asset tracing (ML only)	19	32	17	27	32	7
Requests Executed	6 049	5 924	5 428	4 996	4 159	3 025
Relating to asset tracing (ML only)	10	30	20	20	25	12
Requests Outstanding from Previous Periods	1 699	1 517	954	799	456	338
Relating to asset tracing (ML only)	15	24	26	20	27	33
Requests Denied Due to Lack of Compliance with Relevant Treaty	49	51	36	35	35	83
Requests Returned to Russia for Follow-Up Due to Lack of Treaty Compliance	46	46	42	30	40	35

627. The GPO monitors the progress of outgoing requests on behalf of the Russian sender and sends periodic reminders and requests for updates to foreign authorities. Liaison officers from Russian LEAs, consultations with countries processing a high volume of Russian requests, and meetings on the margins of international fora are also used to advance requests. GPO or LEAs occasionally provide feedback to countries on the helpfulness of responses to Russian requests.

628. To assist with drafting good quality outgoing MLA requests, samples of requests for various purposes are provided to prosecutors and LEAs. All letters transmitted undergo a quality check by GDILC before they are directed to a foreign authority. The types of assistance most frequently sought by Russia include witness interviews; records requests; identification, seizure or confiscation of assets; and inquiries for ownership information relating to possible shell companies.

629. Feedback from the FATF global network indicates that Russian requests are generally clear, normally well translated, and actionable. Countries noted that Russian authorities were mostly responsive to requests for additional information and submitted requests related to a variety of offences, particularly fraud, embezzlement, corruption, and tax crimes, which is largely in line with Russia's identified areas of high risk for ML. A few jurisdictions mentioned that on occasion, the crimes unique under Russian law that are the subject of the requests may pose dual criminality obstacles,[72] or that the status of the subject of the request as a witness or accused person required clarifying dialogue. One country that provided negative feedback on assistance

[72] According to Russian authorities, the main challenge in obtaining formal assistance is a lack of dual criminality in the requested state. For instance, some international co-operation feedback cited cases related to CrC Article 193 as problematic, as this crime is largely without foreign equivalent. The law criminalises "evading the execution of the duty to repatriate foreign currency or Russian currency funds."

received from Russia noted positively that it was able to successfully execute all recent incoming MLA requests from Russia. Another country mentioned that upon asking for clarification on a Russian MLA request, it received no answer. Another country noted a lack of factual detail in some MLA requests and a lack of clarity as to how legal persons that were the subjects of the requests were connected to the alleged criminal scheme. Overall, the feedback pertaining to MLA requests received from Russia was largely positive, with a few exceptions indicative of the need for moderate improvements in explaining the circumstances of the investigation or certain legal and technical details to foreign partners.

630. The average length of execution of Russian MLA requests by CIS member states is usually quicker than for requests sent to other jurisdictions. It generally takes Russia 3-5 months to obtain a response within CIS, and 5-12 months to obtain a response from all other jurisdictions. This can be explained by the direct contacts between counterparts and a level of similarity in legal traditions.

631. Russia has sent a total of 12 MLA requests related to the identification of assets linked to TF starting from 2016 through 2018. Eleven of these requests were granted, showing good proactivity and productivity in this high-risk area.

632. As shown in Table 8.4, Russia sends few requests to trace assets in ML investigations: on average, 22 MLA requests per year. This is lower than expected from a source country for predicate proceeds and also considering that there are more than 3 100 ML investigations annually in Russia, 652 of which are for the type of offences more likely to have international ties. Russian authorities explained that tracing and seizure requests relating to predicates (since predicates are, as a rule, charged alongside ML) are commonplace. Such requests may be used to further financial investigations. Many FIU requests, as discussed below, are used for this purpose, although if these FIU requests bear fruit, the assessors would expect more subsequent MLA requests seeking coercive action or to formalise intelligence into evidence for court proceedings.

Table 8.5. Outgoing MLA Requests on Assets Related to Predicate Offences

	2013	2014	2015	2016	2017	2018
Requests Sent	16	19	12	44	72	106
Requests Executed	3	12	6	26	36	47
Requests Outstanding from Previous Periods	8	19	21	15	33	49
Requests Denied Due to Lack of Compliance with Relevant Treaty	2	5	12	0	20	2

633. As demonstrated by the number of requests and case examples, Russia has increased its focus on tracing and seizing criminal assets located abroad and has been making positive progress in this area since 2016. This is expected by Russian authorities to be a growth area. Considering that financial outflows from Russia spiked in 2013 and that it takes time to investigate and trace assets, the assessors considered it an encouraging sign that requests related to seizure were on the rise, but expected to see a more aggressive pursuit of assets laundered abroad. However, between 2011 and 2017, there were some successful requests related to the confiscation of assets in

Switzerland, Monaco, Latvia, and France concerning significant sums related to ML, fraud, and embezzlement. While Russia sometimes seeks enforcement of its own judgments abroad, it often provides information to countries which prompts them to open investigations resulting in domestic assets seizure. It remains to be seen whether this strategy will result in the repatriation or sharing of assets with Russia, but it deprives criminals of their assets nonetheless. In one case, a country declined to freeze the accounts upon Russian request because Russia did not provide a court order. This obstacle can be overcome by the authorities, who stated that Russian judges are now more comfortable than in years past in asserting jurisdiction over assets located abroad.

634. There are opportunities to improve engagement with foreign countries regarding asset recovery. As described in IO.8 victim compensation is a key tenet of the Russian criminal justice system. However, associated recovery tools, whether restitution, fines, prosecutor's claims, or civil lawsuits, may not be deemed criminal in nature by some countries, and, as such, some requests may fall outside of the scope of MLA treaties or multilateral conventions. The lack of criminal confiscation conducted by Russia, while not an issue in the domestic setting, may have unintended consequences to limit international co-operation. While the response capacity of other countries or the narrowness of certain treaties is not necessarily a deficiency attributable to Russia, the authorities could start early engagement with the foreign country where assets are located to enhance the chances of successful repatriation.

635. Russia's experience in securing assistance from countries in non-criminal asset recovery proceedings has been mixed. For example, in one of the laundromat spinoff cases, Russia's DIA was recognised by a foreign court as the bankruptcy administrator for a Russian financial institution. The bank was intentionally bankrupted by an OCG that included senior bank management. Russian court judgments pertaining to more than EUR 1 billion are at issue in this ongoing matter, and there have been some initial court victories in Russia and in the foreign court which may yet result in the recovery of assets hidden by the perpetrators using foreign trusts. In another example involving a different country where accounts had been initially frozen during the course of a criminal investigation, the foreign court declined to recognize a Russian judgment and transfer funds to the Russian Federal Bailiff Service on behalf of a civil plaintiff. The defendant was convicted by a Russian court, which, as part of its sentencing decision, satisfied the victim's lawsuit for damages, a common practice in the Russian system. While the foreign authorities have appealed the decision and Russian authorities believe this represents a mere procedural hurdle, there is a potential that this approach to asset recovery will be less effective when seeking assistance in certain jurisdictions and may result in delays and expensive litigation costs.

Table 8.6. Outgoing MLA Requests Seeking Seizure of Assets in ML and Predicate Cases

	2013	2014	2015	2016	2017	2018
Requests Sent	2	5	1	12	31	17
Requests Executed	0	0	1	2	15	11
Requests Pending	7	9	6	14	29	32

636. As shown in Table 8.6, there are more requests sent to identify and trace assets than to actually seize or confiscate them. As often the case, assets are conveyed to nominees or new legal persons or transferred out of the jurisdiction receiving the MLA request, which requires new requests to new countries to continue the search. For this reason, Russia relies on FIU requests for tracing, which may elicit quicker responses. As seen above, Russia is sending more seizure requests lately. The speed and close co-ordination between the FIU and LEAs/prosecutors will characterise Russia's success in this area in the coming years, but currently, the practice of routinely recovering assets abroad is still taking shape.

Extradition

637. Russia makes some use of extradition requests. Russia sends, on average, approximately 356 extradition requests per year in all criminal cases (Table 8.7 shows the outgoing extradition requests for ML, TF and predicate offences only). Russia is able to extradite 180 persons pursuant to these requests per year, on average, and is receiving 64 denials of extradition per year, on average. Considering that persons often cannot be located abroad, this is deemed to be a normal rate of denial. In real terms, the total number of outgoing extradition requests appears to be low, especially in light of several case examples discussed where defendants were described as absconded or tried in absentia. The denial of extradition rate, measured using the average number of requests sent and denied as a proxy, is around 17%. This is higher than expected, but may be due in part to a lack of dual criminality or the counting of a "person not located" as a denial. Some of the alternative offences for potential ML activity described in IO.7 do not commonly have foreign equivalents.

Table 8.7. Outgoing Extradition Requests in ML, TF, and Predicate Offences

	2013	2014	2015	2016	2017	2018
Outgoing Extradition Requests related Predicate Offences						
Requests Sent	37	43	64	100	51	52
Requests Granted	8	30	21	35	13	6
Requests Denied	4	5	8	14	6	3
Outgoing Extradition Requests Related to ML						
Requests Sent	9	5	8	14	6	8
Requests Granted	1	1	2	1	2	3
Requests Denied	0	0	4	5	3	0
Outgoing Extradition Requests to TF						
Requests Sent	10	7	11	20	24	3
Requests Granted	1	4	1	6	10	1
Requests Denied	1	4	3	6	8	0

638. Russia frequently asks Interpol to post red notices or less formal diffusion notices for wanted persons. The requests are formulated by the relevant domestic authorities (e.g. MoI, FSB, etc.) and are approved by the head of the preliminary investigative agency. They must be in line with the relevant instructions, judicial decisions on preventive detention, and pertinent MoJ orders. The requests are then sent to Interpol's National Central Bureau in Moscow, which reviews them for compliance with Interpol rules. GPO confirms with Interpol the intention to arrest and extradite the person. Despite an intensive use of Interpol tools, assessors could not determine whether these requests produced results relative to the large number of requests. Since diffusion notices can be posted without prior vetting by Interpol's General Secretariat and are circulated directly by a National Central Bureau to all or some Interpol members, it is important that these notices be based on sufficient evidence to enhance the likelihood of arrest leading to extradition.

639. In international co-operation feedback, one jurisdiction mentioned that it rejected four of six incoming extradition requests due to legal obstacles and/or non-compliance with the European Convention on Human Rights. Another country noted that Russia did not consistently send arrest warrants or extradition decisions with its requests, however, these issues were addressed promptly through the negotiation of a new bilateral treaty that entered into force between the countries in 2018. Other jurisdictions noted that if they had any extradition requests from Russia, they were able to be processed smoothly.

640. Over the last six years, the percentage of total extradition requests that related to ML/TF or associated predicate offences was 21% (77 out of 356). Feedback echoed these statistics, with some jurisdictions noting that Russian extradition requests often related to terrorism or financial or economic crime. This is weighed positively.

Seeking other forms of international co-operation for AML/CFT purposes

641. Russia actively seeks other forms of international co-operation for AML/CFT purposes. Co-operation is sought by the FIU, LEAs, FCS, and BoR.

Rosfinmonitoring

642. Rosfinmonitoring cooperates well with foreign FIUs, both members and non-members of the Egmont Group. To facilitate the exchange of information, it has concluded more than 100 co-operation agreements and is able to provide co-operation on basis of reciprocity, as well. The Egmont Secure Web is used for information exchanges, along with other protected channels (e.g. diplomatic) and, where necessary and practicable, face-to-face meetings and similar communication with foreign counterparts. Diagonal co-operation is carried out in accordance with the Egmont Group Operational Guidance, although cases of requesting or providing such co-operation are rare.

643. Rosfinmonitoring maintains detailed statistics on international co-operation. The process of exchanging information is regulated through standard operational procedures and guidelines (using templates and specific forms for internal control and follow-up). Rosfinmonitoring employs advanced systems for data and case management with sophisticated use of information technology, and has implemented measures to provide for the security (including physical) and confidentiality of the information under its possession.

644. Overall, the FIU has demonstrated that it makes active use of ML-related requests for assistance to foreign counterparts. Over the last six years there has been an increase in the number of outgoing requests (from 452 in 2013 to 740 in 2018), which is indicative of a more proactive approach by Rosfinmonitoring to seek assistance internationally (see Table 8.8).

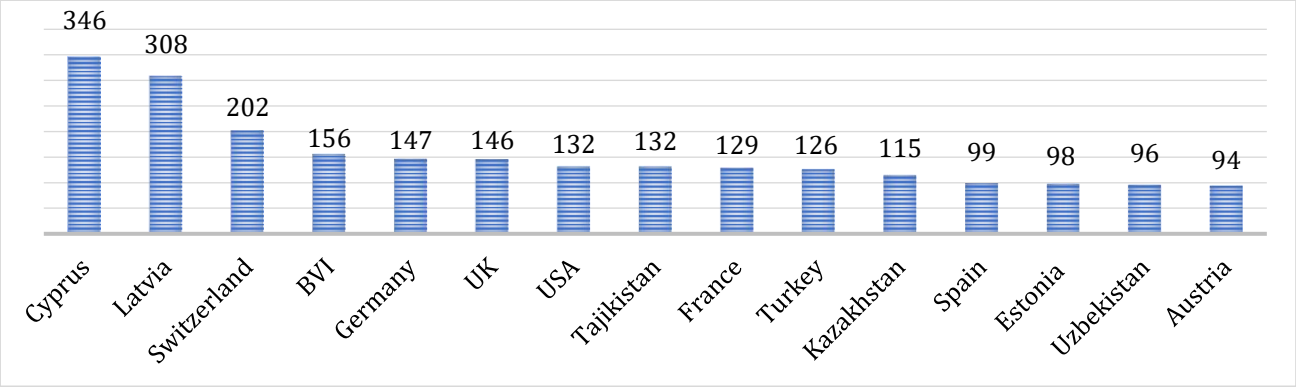
Table 8.8. Requests and disclosures sent to foreign FIUs (total and by subject matter)

	2013	2014	2015	2016	2017	2018
Outgoing requests	452	325	400	878	677	740
Including those related to suspicious on:						
Fraud in financial sector	107	88	128	213	244	218
Illegal drug trafficking	35	48	43	37	53	63
Embezzlement of budgetary funds	129	104	152	253	244	230
Corruption/ abuse of power	100	78	127	222	165	164
Including those seeking to obtain:						
Basic information	288	190	249	591	430	485
BO information	190	130	158	401	309	322
Number of outgoing requests refused	0	7	6	38	5	2
Average response time (days)	71	56	51	33	35	28
Outgoing spontaneous disclosures	0	0	4	11	218	156

645. The geographic coverage of outgoing requests is reasonable and reflects Russia's risk profile as a "source" country for criminal proceeds. Figure 8.1 shows that

Rosfinmonitoring intensively interacts with the FIUs of "transit" and, less frequently, "destination" countries for such proceeds.

Figure 8.1. Number of requests sent to foreign FIUs by destination (2013-2018)



646. The subject matter of outgoing requests is consistent with the risks identified by the 2018 NRAs and earlier risk assessments (see Table 8.8). In 2018, more than 80% of the requests were made in relation to embezzlement of budgetary funds, fraud in the financial sector, corruption/ abuse of power, and illegal drug trafficking.

647. The refusal rate varies year-on-year, but the aggregate rate for the last 6 years is less than 2%, showing that Rosfinmonitoring is generally able to obtain the information sought. The average response time on outgoing ML requests has significantly improved (from 71 days in 2013 to 28 days in 2018), which is indicative of more efficient practices of exchanging information with foreign counterparts. Among recent examples of refused assistance, are a foreign FIU rejected assistance because the predicate offence ("illegal banking activity" as defined in the Criminal Code of Russia) was not covered by the national AML/CFT legislation of the requested country. In addition, a case where the foreign FIU refused assistance in connection with drug trafficking with the explanation that the case was not related to AML/CFT and needed to be forwarded to the LEAs in charge of drug control in the requested country.[73] One country noted that the predicate offence underlying the request was not always made clear. (Russian authorities advise that the issue could pertain to translation and not to the substance of the request.)

648. In the last few years, Rosfinmonitoring has developed a propensity to disclose information spontaneously to foreign counterparts (see Table 8.8).[74] While 153 out of 218 disclosures sent in 2017 had the same content and were addressed to all Egmont Group members in connection to a Ponzi scheme organised by a Russian national there is positive dynamics in the number of spontaneous disclosures (11 in 2016; (218-153) = 63 in 2017; 156 in 2018). Given the large volume and types of information accessible to Rosfinmonitoring, and the number of disseminations made to domestic law

[73] This information is provided not necessarily to identify potential deficiencies on the Russian side but to give a fuller picture of the international co-operation framework and practice.

[74] The abrupt increase of the number of spontaneous disclosures in 2017 was due to the launch of the international project "Milky Way," which aims to establish networking practices with FIUs possibly having interest in subjects and transactions analysed by Rosfinmonitoring.

enforcement authorities[75] (e.g. in terms of ML-related spontaneous disclosures, 3 438 in 2017 and 4 029 in 2018), the FIU should maintain and further enhance the efforts towards proactively making spontaneous disclosures to international counterparts – especially those in "transit" countries – to share information on subjects with nexus to foreign jurisdictions or transactions with cross-border elements.

649. Russia's performance in making requests for assistance on TF-related matters is also good. Between 2013 and 2018 Rosfinmonitoring on average sent to foreign FIUs around 170 requests on TF-related matters per year. Many of the TF-related requests to foreign counterparts are on Russian nationals suspected for aiding / abetting or joining international terrorist organisations as FTFs (the respective figure reported in media was around 4 000 in 2016). Moreover, a significant part of requests and, more importantly, spontaneous disclosures by Rosfinmonitoring is made within the framework of the international "ISIL Phase 2" project and CIS / regional "Barrier" operation, thus making the international sharing of terrorism and TF-related information a systemic and regular practice within the FIU.

650. The below examples demonstrate cases where Rosfinmonitoring successfully sought international co-operation to exchange financial intelligence with its foreign counterparts for AML or CFT purposes.

Box 8.2. Seeking intelligence from foreign FIU to support operational analysis to counter ML and TF

Case example 1

A Russian citizen, being the manager and founder of non-resident companies registered in Estonia, organised illegal withdrawal of funds through the accounts of his companies, as well as companies "A" and "M" registered in Estonia in the name of someone else. The reported purpose of cross-border transfers from the accounts of resident organisations to the accounts of companies "A" and "M" was investment in a construction project to build a hotel and sports complex on land plots to be purchased in Latvia. On 1 September 2016 and 19 January 2017, Rosfinmonitoring sent requests to the FIU of Latvia asking to confirm the facts of sale of land plots. At the same time, requests were sent to the FIU of Poland to obtain information on cash flows of the accounts held by the target. The information received from the FIU of Latvia established that all transactions for the sale of land in the territory of Latvia were fictitious. Additionally, the Latvian FIU indicated the lack of information on any development and construction works on the specified land plots. Moreover, the investment contract of March 2015 was not registered in the land cadastre of Latvia. The Polish FIU provided information confirming that the subjects made dubious financial transactions on accounts opened in Polish banks. Information obtained by Rosfinmonitoring through international co-operation contributed to the

[75] The conclusion in this paragraph duly appreciates that fact that not all disseminations to domestic law enforcement authorities would require a subsequent spontaneous disclosure to foreign counterparts.

initiation of a criminal case under article 193.1 of the CC ("Carrying out the Currency Transactions of Remitting Foreign Currency or Russian Currency Funds to Non-Residents' Accounts with Fake Documents").

Case example 2

Within the investigation initiated under operation "Barrier", a regional office of Rosfinmonitoring carried out verification of information obtained from a payment system on transfers from one of the Russian regions to the territory of Turkey, Syria and Iraq, more precisely to the areas bordering with or controlled by the ISIL. Thanks to co-operation with the Federal Security Service information in respect of 24 persons potentially providing financial assistance to individuals associated with terrorist organisations was obtained. As a result of Rosfinmonitoring co-operation with the FIU of Turkey and the US FinCEN, activities of the terrorist cell "O" that collected and further transferred funds using bank cards and money remittance systems to Turkey in the interest of the ISIL were stopped. The law enforcement agencies in Russia arrested 5 persons, who were charged under article 205.1 of the CC ("Contributing to Terrorist Activity"); 1 person was charged under part 2 of article 208 ("Organisation of an Illegal Armed Group, or Participation in It") and part 2 of article 205.5 of the CC ("Organizing the Activities of a Terrorist Organisation and Participation in the Activities of Such Organisation"); 1 person put on the wanted list, and 2 persons were arrested by law enforcement agencies in Turkey for connection with ISIL

Law enforcement

651. Interpol is used by LEAs to seek information from foreign authorities in ML and TF investigations and cases to some extent compared to the larger number of Interpol requests sent in all criminal matters (from 2013 to 2018, Russia sent between 13 000 and 18 500 requests to Interpol in total. In a number of cases these requests are red flag notices for wanted persons (see above)).

652. There is a quite developed co-operation between FSB, MoI and relevant foreign counterparts. This includes joint operations between Russia and CIS countries in areas of terrorism, terrorism financing, as well as money-laundering related to narcotics, cybercrime, and smuggling of human beings.

653. Since 2015, the FCS has been granted the status of a currency control body and controls dubious foreign exchange transactions, including those related to overstatement of the value of imported goods. Operational information, including with respect to the movement of cash, is exchanged within the framework of the regional communication hub of the World Customs Organisation – the RILO-Moscow created by the CIS countries. . Since 2011, the national communication nodes of the customs services of the RILO-Moscow member countries have introduced information on 1 216 cases of offenses detected during the movement of cash into the CEN network. While FCS appears to be generally active in seeking co-operation, its work in identifying ML and TF cases related to suspicious cash and import/export movements within the EEU is hindered because the different customs agencies of the EEU do not have a

mechanism to share information (see also IO.8). The Russian authorities report that a project on sharing information on ML/TF is at the stage of approval by the member states.

654. FCS is also active in identifying trade mispricing through import-export transactions that may occur at fictitious costs. If there is a suspicion in the exercise of illegal financial transactions, based on the declaration of goods, unreliable information about products and/or their cost to be paid to non-residents, FCS requests the competent authorities of foreign states clarifying data. From 2015 to 2018, FCS sent 40 requests to 18 countries, 26 requests of which have been responded to. In the event a response confirms the discrepancy between the information presented in the declaration and the factual circumstances, and there are strong grounds to believe that the information declared to customs is fictitious, FCS transfers the information to BoR, which will require the relevant bank to consider the opportunity to refuse the transactions or terminate the bank account. From 2015 to 2018, FCS sent BoR information on dubious financial transactions conducted by more than 280 organisations. FCS estimate that these measures prevented illegal currency transactions worth more than USD 3.7 billion (USD 2.5 billion in 2015, USD 900 million in 2016, USD 300 million in 2017, and USD 9 million- in 2018), showing a significant reduction in dubious foreign trade operations in goods.

Bank of Russia

655. BoR seeks international co-operation to some extent. Table 8.9 shows the number of outgoing requests made by BoR. Before 2017, there was no centralised system in place for maintaining statistics on requests for international co-operation with regard to business reputation of owners and managers of FIs, which explains the sharp increase of the relevant indicator of incoming requests since 2017.

Table 8.9. Number of outgoing requests made by BoR to foreign counterparts

		2013	2014	2015	2016	2017	2018
1.	Outgoing requests	13	4	2	0	23	24
	Including those seeking to obtain:						
1.1	Customers' BO information	12	3	2	0	22	20
1.2	Information on owners/ managers of FIs	1	1	0	0	1	4
	Including those that have been:						
1.3	Responded by foreign counterparts	13	4	1	0	10	7
1.4	Refused by foreign counterparts	0	0	1	0	7	7
1.5	Under review as of the reporting date	0	0	0	0	6	11

656. Most requests sent by the BoR seek to obtain BO information of the customers of foreign FIs allegedly owned/controlled by Russian persons, where they are counterparties of dubious transactions with the customers of Russian FIs, as well as information on the further movement of the funds. Russian FIs do not have significant presence abroad and the foreign FIs operating in Russia are subsidiaries of well-known international financial groups (for which statutory and financial information is widely available in open sources). Therefore, it is reasonable that BoR does not make many requests seeking to obtain information on, for example, the internal AML/CFT procedures or the business reputation of the owners and managers of foreign banks represented in Russia, which nevertheless is regularly verified on the basis of published financial and audit reports.

657. Given the decreasing but still significant number and amount of cross-border transactions potentially related to the prevalent ML methods identified in the 2018 ML NRA (e.g. use of front companies to syphon proceeds of corruption and other crimes out of the country, and facilitation of trade-based ML), the BoR should be more proactive in requesting information from foreign financial supervisors on the interim and final destination of cross border flows, as well as on the basic and BO of the legal entities used in such transactions. BoR advises that each request sent to foreign counterparts relates to a number of customers in several foreign banks; for example, 47 requests sent over the period of 2017-2018 have covered 240 clients of 99 foreign banks. While the practice of grouping and aggregating requests for international co-operation does not allow for an objective assessment of the BoR's efforts to trace individual actors and transactions suspected for ML/TF, the level of international co-operation is not comparable to that of the FIU. This is noteworthy given that the BoR is responsible for supervising the whole financial sector for AML/CFT, which is the main risk domain as far as potentially high-risk/dubious cross-border transactions are concerned.

658. The below example demonstrates a case whereby the BoR successfully involved in international co-operation to exchange information with its foreign counterparts for AML purposes:

Box 8.3. International co-operation sought by BoR for AML purposes

In 2017, the BoR sent requests to the banking supervision authorities of 22 foreign states, and in the first half of 2018 to the banking supervision authorities of 9 foreign states. These requests pointed out to certain clients of foreign credit institution, who received funds from Russian legal entities through numerous suspicious transactions. The BoR requested information on the BO of the recipient companies and further directions of money transfers. As a result of interaction with foreign banking supervision authorities in the sphere of AML/CFT, the BoR received valuable information about the recipients (most of them Russian nationals), as well as in some cases about the further use of the suspicious funds, mostly to confirm the conclusion of the BoR that the main purpose of these cross-border transactions was the financing of illegal imports. The information was sent to FCS for testing its use within risk-based control and adjustment of customs value. FCS confirmed the value of the information and the possibility of its use for such illegal purposes. Through the feedback from foreign counterparties, the BoR received further confirmation of the dubious nature of the transactions with the involvement of Russian nationals. Despite the fact that some countries pointed to the need to address these issues using the FIU potential and the ESW communication channel, the foreign regulators took measures to reduce the number and volume of suspicious transactions, in particular by closing accounts and suspending operations, which was also an effective way to cut down illegal withdrawal of funds from Russia.

Providing other forms international co-operation for AML/CFT purposes

659. Request prioritisation and processing appear to be designed and implemented in a way that facilitates their execution in a constructive and timely manner. Table 8.10 presents the requests received by Rosfinmonitoring over the last 6 years:

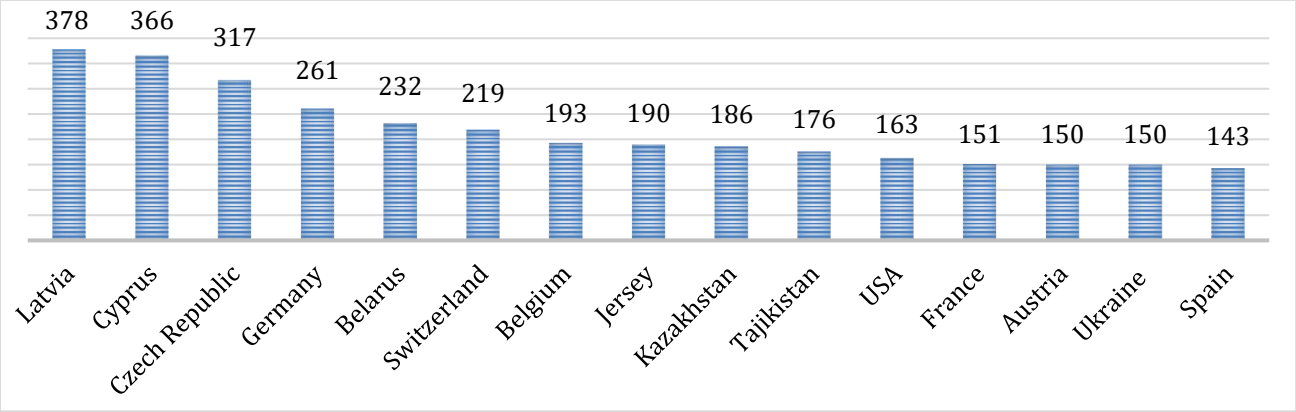
Table 8.10. Requests related to ML received by Rosfinmonitoring

	2013	2014	2015	2016	2017	2018
Incoming requests	846	627	597	493	486	439
Including those related to suspicious on:						
Fraud in financial sector	35	62	133	95	88	48
Illegal drug trafficking	21	14	22	18	15	20
Embezzlement of budgetary funds	17	28	47	32	38	35
Corruption/ abuse of power	38	26	46	35	34	20
Including those seeking to obtain:						
Basic information	253	210	200	180	165	205
BO information	22	27	25	17	10	44
Average response time (days)	66	64	60	41	28	30
Incoming spontaneous disclosures	3	87	125	203	292	437
Materials sent to LEA proactively	4	47	52	161	172	104

660. The performance in responding to requests is good. Over the last 6 years there has been a decrease in the number of incoming requests (from 846 in 2013 to 439 in 2018), which could be attributed to the significantly lower volumes of potentially suspicious outgoing cross-border transactions and, as a consequence, to a lesser need for foreign counterparts to request assistance from Rosfinmonitoring. The average response time on ML requests has significantly improved (from 66 days in 2013 to 30 days in 2018), which is indicative of improved Rosfinmonitoring capacity to process and handle requests from foreign counterparts.

661. As in the case of outgoing requests, the geographic coverage of incoming requests is reasonable and reflects Russia's risk profile, as shown in the below diagram on the top-15 requesting jurisdictions over the period of 2013-2018.

Figure 8.2. Number of requests received from foreign FIUs by destination (2013-2018). Source: Rosfinmonitoring



662. The performance in responding to requests for assistance on TF-related matters is good, as well. Between 2013 and 2018, Rosfinmonitoring on average received around 63 requests per year from foreign FIUs. As in the case of outgoing TF-related requests, most of the incoming requests pursued to obtain financial and other necessary data necessary for furthering financial investigations. Since 2016, Rosfinmonitoring has routinely used the power to freeze (block) money or other assets of the individuals and entities suspected of participation in terrorist activity (including the financing of terrorism) on requests received from foreign FIUs. The average response time on TF-related requests has significantly improved (from 67 days in 2013 to 36 days in 2018). Rosfinmonitoring indicates that it has never refused ML or TF-related co-operation on any incoming requests over the last 6 years (see the below section on the feedback from the Global Network). In relation to both ML and TF-related information exchanges, Rosfinmonitoring refers to successful networking practices with numerous FIUs to facilitate information exchange and intelligence sharing on complex and significant cases.

663. The below examples demonstrate cases whereby Rosfinmonitoring successfully provided international co-operation to exchange financial intelligence with its foreign counterparts for AML and CTF purposes.

Box 8.4 Co-operation provided by Rosfinmonitoring

Case example 1

Rosfinmonitoring received a request from the Czech FIU on company "I" incorporated in the Czech Republic by a Russian citizen "T", in connection with suspicion of ML. According to the information from the Czech FIU, the company received funds from Russian and foreign organisations and subsequently transferred them through to other contractors in different countries. In the course of the analysis, Rosfinmonitoring found out that Russian contractors of company "I", some of which were controlled by person "T" and others by the third-tier contractors, were involved in fictitious trade activities. This information was sent to the FIU of the Czech Republic, as a result of which the FIU decided to freeze funds of company "I" and initiate criminal proceedings against person "T". On 17 September 2018 a criminal case under article "Money Laundering" was initiated, and funds totalling USD 1 million received from the account of the US company "L", which was further supposed to be transferred as a loan to the Russian company "A", were arrested.

Case example 2

On 3 September 2018, the FIU of Latvia sent a request to Rosfinmonitoring in respect of Person "M", who was a close relative of a former PEP. FIU of Latvia requested information on the criminal case initiated in respect to the suspect, on the persons related to the suspect, and on the sources of the funds in his accounts. Rosfinmonitoring informed the Latvian FIU that, according to the information of the Russian law enforcement agencies, the suspect and his brother – a former PEP – were subjects of a criminal case under part 4 of article 159 ("Fraud") of the CC in connection with the theft of funds in the performance of the contract for the construction of the stadium for the FIFA World Cup. The damage from the actions of the defendants amounted to more than RUB 2.5 billion. Rosfinmonitoring gave permission to the FIU of Latvia to disseminate the information to the Latvian law enforcement agencies for intelligence purposes, and requested permission to disseminate the information received from FIU of Latvia to the Russian law enforcement agencies.

Case example 3

Due to interaction with a LEA, Rosfinmonitoring received a list of persons who had travelled to a conflict zone for joining ISIL. Further verification identified that money was transferred though bank accounts of Persons A and M and subsequently cashed out in the territory of Russia and Turkey.

Relevant findings were sent to the LEA and served as the basis for initiation of criminal case concerning persons involved according to Part 1 of Article 205.1 of the CC.

During the investigation of criminal cases, interaction was carried out with the NCB Interpol, the Consular Department of the Russian Foreign Ministry, the involved LEA, as well as with the special services of the Syrian Arab Republic and the Republic of Turkey. Interaction was carried out in the form of requests and responses to them.

The information received from these agencies was fully used in the criminal case to prove the involvement of the defendants in terrorist activities.

Feedback from the Global Network

664. Further to a call from the FATF to the Global Network, 34 responses were received with feedback on international co-operation provided and sought by Russia. Regarding FIU and LEA co-operation, a majority (83%) of the jurisdictions having responded to the respective section of the FATF inquiry provided very positive or generally positive feedback on their experience of interacting with the Russian counterparties. In case of regulatory/supervisory and other forms of co-operation, all responses (100%) to the respective FATF inquiry, although few, were very positive or positive.

665. Nevertheless several issues were raised as concerns in negative feedback from members of the Global Network, including three partner countries which are important destinations for potential proceeds of crime generated in Russia. This feedback noted, inter alia, failures to provide adequate and timely information, which imply that the Russian authorities should endeavour to further improve their performance in providing timely and high-quality co-operation with all their partners in response to valid requests for such co-operation. It also noted issues related to Rosfinmonitoring's access to law enforcement or other databases; the prioritisation of requests; and the practice of providing interim updates.

666. Assessors followed up these issues to discuss the underlying situation with regard to each case, and Russian authorities set out the actions they have already taken in response to this feedback. Authorities had also followed-up bilaterally with those countries signalling problems. Overall, the feedback does not identify any major issues concerning the constructiveness and timeliness of international co-operation provided by Rosfinmonitoring to its foreign counterparts.

667. LEAs, including the MoI, the FSB, and the FCS, generally provide co-operation to relevant counterparts, predominantly through Rosfinmonitoring, which is seen as the key domestic authority in matters related to the provision of informal international co-operation (i.e. other than MLA and extradition considered in the analysis for Core Issues 2.1 and 2.2).

Bank of Russia

668. There are mechanisms for supervisory co-operation by the BoR. In its capacity of mega-regulator for the financial sector, the BoR cooperates with foreign central banks and financial regulators. To that end, it has concluded over 30 co-operation agreements devoted to or reflecting on AML/CFT matters. Diagonal co-operation is carried out through Rosfinmonitoring, although cases of requesting or providing such co-operation are rare. Whereas international co-operation remains focused only on investigations of serious (and generally criminal) misconduct affecting FIs, there appear to be other examples of supervisory co-operation with the competent authorities of European (e.g. Germany, Austria, Moldova) and other (e.g. India, Kazakhstan) countries to consider compliance and risk-related issues. Even though Russia is not a major international financial centre, the BoR should be seek to further expand efforts towards establishing and maintaining relationships with foreign supervisors to support supervision of those FIs with a cross-border presence or handling the greatest cross-border financial flows.

669. The process to exchange information is appropriate to the current level of interaction. Processing and follow-up on requests for co-operation is embedded within the document management system of the BoR, and due to the small number of requests received from foreign counterparts all incoming requests are considered as high priority and executed accordingly under the personal control of the BoR Deputy Governor. Table 8.11 presents statistical data on AML-related requests received by the BoR over the last six years:

Table 8.11. AML-related requests received by BoR

		2013	2014	2015	2016	2017	2018
1	Incoming requests	5	2	6	4	86	64
	Including those seeking to obtain:						
1.1	Customers' BO information	5	2	6	1	0	1
1.2	Information on owners/ managers of FIs	0	0	0	3	86	63
	Including those that have been:						
1.3	Responded by BoR	5	2	6	4	86	58
1.4	Refused by BoR	0	0	0	0	0	0
1.5	Under review as of the reporting date	0	0	0	0	0	6

670. The BoR receives requests for information from foreign supervisory authorities as part of the procedure to approve candidates for executive positions in companies supervised by foreign supervisors, as well as to approve transactions involving the acquisition of shares (stakes) of companies in foreign securities markets. Foreign supervisors request confirmation of the information provided by the candidates regarding their business reputation, enforcement measures applied to them by the BoR and similar information.

671. Given the limited presence of Russian FIs in foreign markets, the number of such requests seems reasonable and commensurate with their risk exposure. However, the fact that foreign financial supervisors do not approach the BoR specifically for AML-related information (e.g. BO of Russian customers served in foreign banks) could be indicative of the reality that it is the national FIU – rather than the central bank – that is considered by foreign competent authorities as the proper counterparty for AML-related exchanges. This is confirmed by the fact that, over the period 2016-2018 the BoR has sent to Rosfinmonitoring information on 75 foreign banks located in various countries (3 banks in 2016, 36 banks in 2017, and 36 banks in 2018), which were receiving dubious or suspicious transactions from Russian banks.

International exchange of basic and beneficial ownership information of legal persons and arrangements

672. Russia proactively seeks and provides co-operation on the basic and BO of legal persons. This is demonstrated by the significant statistics provided by different authorities on the requests made involving the ownership and BO information of legal entities. Requests for BO information comprise a significant share within the total number of outgoing requests (322 out of 740, or 43%, in 2018). This reflects the ML/TF risk-profile of Russia in which companies created in Russia or abroad are used to assist in the syphoning of money out of the country.

673. Russia provides information on basic and BO information of legal entities. Requests for BO information comprise a relatively modest share within the total

number of incoming ML requests (44 out of 439, or 10%, in 2018) compared to that of requests on basic information (205 out of 439, or 47%, in 2018). The authorities interpret that Russian legal entities are rarely used in foreign ML schemes and have a simple ownership structure, which makes requests for BO information not relevant. A few partners made complaints on the quality of the information received, but none of these complaints specifically indicated a problem with the exchange of information on legal entities.

Overall conclusions on IO.2

674. Russia provides MLA and extradition in a constructive and timely manner. Wide feedback from the FATF global network on Russia's provision of MLA trended positive, with a few complaints. Russia seeks formal assistance to pursue ML, TF, and associated predicate offences with transnational elements in line with the risk profile of the country, although the level of judicial co-operation sought in tracing and seizing assets in ML cases is lower than expected. Rosfinmonitoring cooperates well with foreign FIUs, both members and non-members of the Egmont Group. The process of exchanging information is appropriately regulated, and the FIU is active in both making and responding to requests on ML and TF. There is a quite developed co-operation between Russian LEAs and relevant foreign counterparts. Feedback from international partners is largely positive. Minor improvements are needed to continue improving the form and the content of the requests for co-operation sent abroad, and to further enhance the efforts towards proactively making spontaneous disclosures to international counterparts – especially those in "transit" countries.

675. Russia is rated as having a substantial level of effectiveness for IO.2.

TECHNICAL COMPLIANCE ANNEX

This annex provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerological order. It does not include descriptive text on the country situation or risks, and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report. Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in June 2008. This report is available from www.fatf-gafi.org/documents/documents/mutualevaluationoftherussianfederation.html.

Recommendation 1 – Assessing risks and applying a risk-based approach

This is a new Recommendation, which was not assessed in the 3rd round MER.

Criterion 1.1 **–** Russia has identified and assessed its ML/TF risks primarily through two separate NRAs completed in 2018. The ML NRA identifies the high-risk areas, threats and vulnerabilities as well as the authorities' final understanding of the national ML risks (categorised into high, increased, moderate and low risk groups). The ML NRA uses a wide range of information, including analysis of the legal framework, data on predicate crimes and cross-border financial flows. It considers intelligence data, surveys from the private sector, as well as qualitative data from examples of ML/TF investigations, supervisory findings and expert opinions. A summary of the ML NRA has been made public.[76] The key findings of the TF NRA consider successive stages of TF, i.e. raising, moving or using funds for terrorism purposes. For each stage, the report analyses TF methods in terms of threats, vulnerabilities and measures (to be) taken for mitigation of specific risks. There is a non-public (extended) version of the TF NRA which could not be provided to the assessment team for confidentiality reasons (as per Art. 5, Para. 4 of the Law on State Secrets).

Between 2014 and 2017, Rosfinmonitoring was producing annual threat assessments reports, which in part reflected on ML/TF risks, trends and methods. Following the 2018 NRAs, Russia has conducted sectoral risk assessments within the sectors supervised by the BoR, Rosfinmonitoring, the State Assay Chamber, Roscomnadzor, and the MoJ. Rosfinmonitoring and the MoJ have also carried out a separate assessment of FT risks in the NPO sector (see R.8). The results of the NRAs and the SRAs generally appear reasonable to ensure that Russia has identified and assessed its ML/TF risks.

Criterion 1.2 **–** Rosfinmonitoring is the designated authority responsible for the co-ordination of ML/TF risks assessments (RFMR, Art. 5(16.1)). Such co-ordination

[76] The main findings of the ML NRA are available at www.fedsfm.ru/content/files/documents/2017/keyfindings.pdf.

mainly takes place through the IAC AML/CFT/CPF, which is the domestic coordination mechanism set-up to ensure consistency of AML/CFT/CPF efforts, including risk assessments.

Criterion 1.3 – There is no legal requirement to update the NRAs, however, the authorities are committed to conducting full-scope cycles of risk assessments at least upon completion of the implementation period (3-5 years) of the current action plans developed on the basis of the NRAs. Rosfinmonitoring has produced annual assessments reports on national security threats since 2014, which provide for regular updates on the respective risk assessments (see c. 1.1).

Criterion 1.4 – Rosfinmonitoring has the responsibility to disseminate the NRA results to federal and state law enforcement agencies and supervisors, including self-regulatory bodies (RFMR, Art. 5(9.2)). The two mechanisms used for communication with government agencies are the IAC FATF Evaluation and the IAC AML/CFT/CPF. Communication to the private sector is arranged through the publication of a summary of the ML NRA on the Rosfinmonitoring website, as well as through the Advisory Council (composed of the largest professional associations and unions) and the Compliance Council (composed of the largest FIs and DNFBPs). The NRAs findings are also posted on the personal (secure) accounts, which reporting entities must open with Rosfinmonitoring.

Criterion 1.5 – Russia demonstrates allocating its resources and implementing measures based on the authorities' understanding of ML/TF risks. On the basis of the ML and TF NRAs, the authorities have endorsed two national action plans for the prevention and mitigation of identified ML and TF risks. The AML Action Plan specifies the agencies responsible for the implementation of defined measures and the priority of their implementation based on the severity of the identified risks.[77] The CFT Action Plan provides a list of prioritised recommended actions. Most competent authorities have conducted sectoral risk assessments and produced the respective working plans. These working plans demonstrate that competent authorities allocate their human and material resources based on the understanding of the key risks and the need for their mitigation. All competent authorities are equipped with appropriate human, financial, technical and other resources to tackle the tasks set out in the AML, CFT or the sectoral action plans.[78]

Criterion 1.6 – Russia does not provide for situations where FIs or DNFBPs are not required to apply the FATF Recommendations. The AML/CFT Law allows for exemptions from customer identification obligations for certain types of transactions and activities with monetary thresholds that are well below the ones established in the FATF Recommendations. The exemptions are disallowed whenever the obliged entities have ML/TF suspicions or doubts about the reliability of customer identification data.

77 As short, medium and long-term priorities, also specifying measures to be implemented on regular basis

78 To improve targeted control over the progress in the risk-based implementation of AML/CFT measures and allocation of resources, it would be beneficial if the action plans also define the dedicated resources to be (re)allocated for their successful implementation, as well as the quantitative and qualitative monitoring metrics with a view of identifying and addressing implementation impediments.

Criterion 1.7 – The AML/CFT Law defines that the nature and scope of CDD measures may differ depending on the degree (level) of ML/TF risk (Art. 7, Para. 1 (1.1) and Para. 2); however, there is no specific requirement regarding the application of enhanced measures (see c.10.17) where the country identifies higher risks.[79] This deficiency is largely mitigated because in certain higher risk situations obliged entities are required to apply measures providing for enhanced scrutiny, control or mitigation of risk, which touch upon different aspects of ML/TF risk identified by the ML and TF NRAs. In addition, various regulatory acts[80] set out the factors and indicators that affect assessment of ML/TF risk and require obliged entities to take mitigation measures.

Criterion 1.8 – There is no explicit requirement for simplified CDD to be allowed in case of identified lower risk; however, this is a minor deficiency as the cases where simplified CDD is allowed are not in conflict with the conclusions of the NRAs and represent objective characteristics of potentially low-risk relations[81]. Simplified CDD is not allowed when the transaction is subject to mandatory control, the person is involved in extremist or terrorist activities, or there are ML/TF suspicions regarding the customer, the transaction has a complex or unusual character, and there are doubts about the reliability of information provided by the customer (Art. 7, Para. 1.11 L115). In addition, simplified identification comprises most of the key elements of full (non-simplified) identification as set out in the AML/CFT Law (Art. 7, Para. 1(1)).

Criterion 1.9 – The AML/CFT Law sets forth requirements for obliged entities to assess and manage their ML/TF risks within the framework of their internal control systems (see c.1.10 and c.1.11). It also defines that supervision regarding organisation and implementation of internal control systems of obliged entities shall be exercised by appropriate supervisory bodies in accordance with their area of competence, as well as by Rosfinmonitoring where there are no specified supervisory bodies in the sphere of activities of individual obliged entities (Art. 7, Para. 9). Reference is made to the analysis for R.26 and R.28 for minor deficiencies on the structural and substantial elements of the AML/CFT supervisory regime.

Criterion 1.10 – Financial institutions and DNFBPs are required to take appropriate steps to identify their ML/TF risks, with a minor deficiency as set out below. The AML/CFT Law requires obliged entities to implement internal control systems (Art. 4), which should comprise programmes for assessing ML/TF risk (Art. 1.6 and Art. 4.9 of BRR №375-P; Art. 1.7 and Art. 4.4 of BRR №445-P; Art. 25 of RFMO №366, as well as Art. 4 and Art. 8 of GR №667). This includes being required to:

6. Keep documents regarding their risk assessments outcomes and the underlying analysis (Art. 25 and 37 of RFMO №366; Art. 4.9 and Art. 4.4 of, respectively, BRR №375-P and BRR №445-P; Art. 33(h) of GR №667).

79 Amendments requiring obliged entities to apply enhanced measures have been introduced and entered into force after the onsite mission (para 4.1 of BR375 and para 4.1 of BR 445).

80 Such as GD №667; BRR №375-P; and BRR №445-P

81 Simplified measures can only be taken in respect of identification of customers who are natural persons, in case of certain types of transactions and activities, such as money transfers or currency exchange transactions below RUB 100 000 (approx. EUR 1 340); consumer loans below RUB 15 000 (approx. EUR 200) etc.

7. Consider all relevant risk factors, as the client risk should be assessed taking into account information obtained through identification, monitoring of transactions (including suspicious transactions), types and terms of activities, geographic areas and other factors (RFMO №366, Art. 25; GR №667, Art. 8(c) and 14; RFMO №103; BRR №375-P, Art. 4.2-4.8, art.5.2; BRR №445-P, Art. 4.1-4.3, art. 5.2). Obliged entities are required to take measures commensurate to the risks based on the level of the risk assigned to a client (Art. 15 and 18 of GR №667; Art. 4.9 of BRR №375-P; Art. 4.4 of BRR №445-P).
8. Keep assessments up to date, including data on client risk rating (RFMO №366, Art. 26-27; BRR №375-P, Art. 4.9; BRR №445-P, Art. 4.4). The risk assessment programs should define the procedure and periodicity of monitoring transactions for assessing and revising client risk rating (GR №667, Art. 15).
9. Have mechanisms for providing risk information to authorities, as obliged entities are required to ensure timely provision of AML/CFT-related information to Rosfinmonitoring (Art. 1.4 in both acts, BRR №375-P and BRR №445-P). However, there are no defined mechanisms for providing risk assessment information to SRBs.

Criterion 1.11 – FIs and DNFBPs required to take risk mitigating measures, with a minor deficiency as set out below:

1. While FIs and DNFBPs are required to have in place policies, controls and procedures approved by the senior management (or sole executive body) to mitigate the risks identified by themselves (L115, Art. 7, Para. 2; RFMO №366, Art. 25; GR №667, particularly Art. 4(c), Art. 15 and Art.18; BRR №375-P, Art.1.3, Art. 1.6, Art. 4.1; BRR 445-P, Art.1.6, Art. 1.7, and Art. 4.1), there are no explicit provisions to require that internal control rules enable management and mitigation of the risks identified by the country or, alternatively, that the risks identified by the country are taken into consideration when obliged entities implement risk management and mitigation programs.
2. Obliged entities, and/or responsible employees/managers, have to monitor the implementation of internal control programs, conduct regular checks of their implementation (at least annual or semi-annual), report to top officials on ways for improvement, and take appropriate remedial measures (BRR №375-P; Art. 1.9, Art. 2.6; BRR №445-P, Art. 1.10, Art. 2.9; GR №667, Art.1.1, Art. 31, Art. 32).
3. Obliged entities are generally required to take enhanced measures and mitigate higher risks (however, see c.1.7 and c.10.17 for minor deficiencies).

Criterion 1.12 – The legislation does not permit financial institutions and DNFBPs to take simplified measures in managing and mitigating risks. Simplified CDD is possible only in limited circumstances applying thresholds well below the ones determined by FATF Recommendations and are not permitted in the presence of ML/TF suspicions (see c.1.8). FIs and DNFBPs are not allowed to identify lower risk situations independently.

Weighting and Conclusion

Most requirements are fully met, and there are only minor shortcomings with regard to the application of enhanced measures where the country identifies higher risks, permission of simplified CDD allowed only in case of identified lower risk, provision of risk assessment information to SRBs, and consideration of country risk information by obliged entities.

Recommendation 1 is rated largely complaint.

Recommendation 2 - National co-operation and co-ordination

In its last MER, Russia was rated largely compliant with former R.31. LEAs and supervisors did not adequately cooperate on the operational level with respect to potential systemic vulnerabilities such as illegal money and value transfer services.

Criterion 2.1 – The 2018 *Concept for Development of the National AML/CFT System*[82] is the most recent national policy document relevant to AML/CFT area. This document sets out prevalent risks in line with those identified by the ML and TF NRAs. Authorities have also developed a number of strategic policy documents articulating their understanding of challenges to the country's economic and physical security, with some relevance to AML/CFT. These include the National Anti-Drug Policy (2010-2020), the Strategy for Countering Extremism (2014-2025); the 2015 National Security Strategy (for 2016 onwards); the Strategy of Economic Security (2017-2030) and the National Anti-Corruption Action Plan (2018-2020). Early assessments of ML/TF risks (as described in the analysis for c.1.1 and c.1.5) have fed into the development of these documents and used to improve the legislative and institutional framework.

Criterion 2.2 – Rosfinmonitoring is the designated body responsible for elaborating policy and regulation in the AML/CFT area, as well as co-ordinating activities of all relevant agencies. To assist Rosfinmonitoring in its co-ordination function, authorities have set up the IAC AML/CFT/CPF (RFMO №304, Paragraph 3).

Criterion 2.3 – There are mechanisms to ensure policy and operational co-ordination. Policy makers, Rosfinmonitoring, law enforcement and judicial authorities, supervisors (including SRBs) and other competent authorities are represented in the IAC AML/CFT/CPF, the IAC Financial Crime, and the IAC FATF Evaluation. Other interagency coordination mechanisms are provided through the National Anti-Terrorism Committee, the State Anti-Drug Committee, the Presidential Council for Countering Corruption, and the Interagency CFT Committee.

Criterion 2.4 – Rosfinmonitoring has a mandate to combat PF (Art. 8, Para. 1 AML/CFT Law; Art.1 RFMR). The IAC AML/CFT/CPF is mandated to provide international co-operation on PF (including through the exchange of information), as well as other interaction on combating PF.

Criterion 2.5 – The IAC AML/CFT/CPF can involve in its work representatives of non-member agencies and institutions for the consideration of cross-cutting issues (IAC Regulations, Art. 4(d)), and therefore can be used to discuss any issue regarding the compatibility of AML/CFT requirements and data protection and privacy rules. The

[82] Published on the official Kremlin website on May 30, 2018

Law on Protection of Information categorizes information as either generally accessible or accessible under restrictions established by federal laws (Art. 5, Para. 2), and sets out the basic principle for processing of personal data to be carried out with the consent of the subject of personal data (Art. 5, Para. 3(2) and Art. 6, Para. 3(1)). The AML/CFT Law, while imposing a general ban on informing third parties about measures taken to combat ML/TF (Art. 4), permits the processing and dissemination of personal data without the consent of the subject of personal data when it is necessary to achieve the objectives of the law (Art. 8, Para. 2).

Weighting and Conclusion

All criteria are fully met.

Recommendation 2 is rated compliant.

Recommendation 3 - ML offence

In its last MER, Russia was rated largely compliant. The main deficiency was the lack of criminalisation of insider trading and market manipulation. Russia criminalised these predicate crimes in 2010 (Federal Law 224-FZ). During the follow-up process, Russia decriminalised self-laundering of amounts lower than RUB 6 million (approximately EUR 147 000). Russia then eliminated the threshold by enacting Federal Law 134-FZ. When Russia was removed from the regular follow-up process in 2013, old R.1 and R.2 were considered largely compliant.

Criterion 3.1 – ML is criminalised in Articles 174, 174.1, and 175 of the CrC, which are interpreted with the aid of judicial guidance.[83] Article 174 is a third-party ML offence, Article 174.1 is a self-laundering offence, and Article 175 prohibits the acquisition or sale of criminally derived property.

Article 174 prohibits performing financial transactions and other deals, in monetary funds or other property, where those funds or property are known to have been illegally acquired by others, "for the purposes of making the possession, use, and disposal of the funds or property seem lawful." Article 174.1 contains the same elements, but the funds or other property are acquired by the launderer as a result of his or her own commission of a crime. The *actus reus* under both articles is a "financial transaction" or a "deal," which broadly covers the acts of conversion and transfer under the Vienna and Palermo conventions.[84] The objects of both crimes are "monetary funds" or "other property" known to have been illegally acquired by one's self or others. This captures the knowledge element concerning the nature of the proceeds.

---

83 A number of orders of the Plenary Session of the Supreme Court have been provided to the assessment team. They represent the authoritative and final view on the interpretation of Russian law and are binding on lower courts. SC Order No. 32 (2015) was modified by SC Order No. 1 issued on 26 February 2019. All references to SC Order No. 32 herein reflect the amended version, in force as of the dates of the on-site visit.

84 SC Order No. 32 defines financial transaction as "any transaction in money (cash and non-cash settlements, cash operations, money remittance or changing, exchanging one currency to another, *etc.*)." (Emphasis added.) Deals may include acts aimed at establishing, varying, or terminating civil rights and obligations. Id.

Laundering with the *intent to conceal or disguise* the criminal origin of property is not explicitly criminalised. Under Articles 174 and 174.1, the offender must intend that the transaction or deal makes the possession, use, or disposal of such property "seem lawful."[85] However, committing a transaction with the specific intent of making one's possession or use of criminal property seem lawful is conceptually similar to concealing or disguising the illicit origin of the property or helping the predicate offender evade the consequences of his or her action. Furthermore, according to SC Order No. 32, as amended just prior to the on-site visit, the purpose of giving the appearance of legitimacy to the possession, use, and disposal of property "shall be understood as concealment of criminal origin, location, disposal, [or] movement of property…."

The conventions also mandate that the *acts* of concealing or disguising the "true nature, source, location, disposition, movement, or ownership of" property, where the offender knows the property to be proceeds, are criminalised. Articles 174 and 174.1 cover transactions or deals intended to make property "seem lawful." Transactions or deals can include acts to conceal or disguise; the purpose to make the property "seem lawful" covers the concepts of concealing the true nature and source of the property; and the reference in Articles 174 and 174.1 to the "possession, use, and disposal" of proceeds broadly covers the concepts of location, disposition, movement, or ownership.

Finally, the Vienna and Palermo conventions require the criminalisation of the *acquisition, possession, or use* of property, knowing, at the time of receipt, that such property was proceeds of crime. Article 175 prohibits the acquisition or sale of property "knowingly obtained in a criminal manner." In order for a person to possess proceeds, logically, they must have acquired them, and Russia criminalises acquisition. Furthermore, "acquisition or sale" in Article 175 covers most conceivable uses of proceeds, namely, spending them (e.g., one can "sell" the proceeds of crime in exchange for almost anything, including goods or services, a common "use" of ill-gotten gains as recognised in SC Order No. 32, para. 11). Thus, the Vienna and Palermo acts of acquiring, possessing, or using property are established. There is, however, a minor shortcoming in the knowledge element. The conventions require that the perpetrator knows at the time of receipt that the property was criminally obtained. Article 175 requires that the property was knowingly obtained in a criminal manner, which technically refers back to the intention behind the predicate offence, not necessarily the knowledge of the launderer at the time of receipt of the property. The Supreme Court has mitigated this gap by clarifying that for the purposes of Article 174 or 175, a court should consider whether the perpetrator "had previously known about the criminal origin of the property" and stating that he or she need not know the specific circumstances of the predicate (SC Order No. 32, para. 19).

The ML offences must be committed deliberately in order to be punishable (CrC Art. 24), and the Supreme Court has stated that the perpetrator must be found to have "knowingly" performed a financial transaction or deal (SC Order No. 32, para. 10).

[85] The implication is that possessing, using, or disposing of any property derived from crime is necessarily unlawful in Russia. This is a presumption built into to the offences contained in Articles 174 and 174.1.

Criterion 3.2 – Any criminal offence can be a predicate for ML. All required predicate offences are criminalised in Russia.

Criterion 3.3 – Russia does not apply a threshold approach.

Criterion 3.4 – The ML offences extend to most property, regardless of value, that directly or indirectly represents the proceeds of crime. Both Articles 174 and 174.1 apply to "monetary funds or other property." "Monetary funds" are not defined in the CrC, but whatever they do not include—such as real property or precious metals or stones—could be encompassed by the expansive definition of "other property." In Order No. 32, para. 1, the Supreme Court clarified that ML extends to (1) property whose illegal acquisition is an element of the predicate offence (e.g., bribe money); (2) remuneration for crimes committed (e.g., sums paid for hired killing); and (3) profits from the sale of contraband. The Order interprets "monetary funds" as cash denominated in foreign or domestic currency and non-cash monetary funds, including electronic monetary funds. A new clause added in 2019 states that the subject matter of the ML offences "can constitute, inter alia, monetary funds transformed from virtual assets (crypto currencies), obtained as a result of committing a crime." (SC Order No. 32, para. 1 (as amended)). The amended text of Order No. 32 stops short of asserting that virtual assets can be the subject of the offence – it makes funds "transformed *from* virtual assets" the potential subject of the offence, which is one transaction removed. For example, it is unclear if transactions involving the conversion of one VA into another can constitute an ML transaction.

"Other property" is understood as movable and immovable property, property rights, documentary and non-documentary securities, and property generated as a result of processing property obtained by criminal means. The inclusion of "property generated" means that indirect proceeds can be laundered, in addition to direct proceeds, and the ML offences do extend to transactions conducted with commingled property (SC Order No. 32, para. 3).

While the ML offence extends to tax crimes in line with 3.2, there is a minor gap in that it does not extend to property that is the proceeds of tax evasion regardless of value. Under CrC Article 198, in order to be considered a criminal offence, evaded taxes must exceed a monetary threshold. Because this threshold is low (around EUR 12 000) and measured over three years, this shortcoming is unlikely to have a material impact on tax-based ML offences.

Criterion 3.5 – To prove that property is the proceeds of crime, it is not necessary that a person be convicted of a predicate offence (SC Order No. 32, paras 4-5).

Criterion 3.6 – Predicate offences for ML can extend to conduct that occurs outside of Russia. Neither law nor Supreme Court guidance affirmatively addresses this issue or explicitly state that foreign conduct can be the basis for a predicate, but the recognition of foreign predicates aligns with Russia's "all crimes" approach and there are examples of ML based in part on foreign conduct.

Criterion 3.7 – The ML offence applies to persons who commit the predicate offence. Self-laundering is a separate crime under Russian law (CrC Art. 174.1).

Criterion 3.8 – It is possible for the intent and knowledge required to prove an ML offence to be inferred from objective factual circumstances. The intent required "may be established based on the factual circumstances of the case that indicate the nature

of the executed financial transactions or deals" (SC Order No. 32, paras 10, 19). Examples of facts that may demonstrate criminal intent are elaborated in the SC Order, i.e., the use of straw persons, transactions involving parties in offshore territories, and transactions lacking economic expedience or justification.

The CPC further establishes that mental elements may be inferred from facts (arts. 17, 73-74, 85).

Criterion 3.9 **–** The basic penalty for ML is a fine, however, the large scale enhancement, which can result in a sentence of imprisonment, activates at a relatively low threshold of RUB 1.5 million (approximately EUR 19 960). The maximum penalties available for the most severe violations of the ML offences are a term of imprisonment of 7 years and a fine of RUB 1 million (approximately EUR 13 385) or up to five years' salary or income. There are several additional sanctions which can be combined to fit the gravity of the offence, to include: compulsory labour, restrictions on freedom or activities, or deprivation of official position. There is flexibility to adjust punishment due to mitigating or aggravating factors described in CPC Articles 61 and 63. By comparison, the maximum sanctions available for other serious, non-violent offences are 10 years (fraud, CrC Art. 159), 8-10 years (bribery, CrC Art. 290), and 2-6 years (insider trading, CrC Art. 185.6). The penalties for ML included in the law are dissuasive and proportionate.

Criterion 3.10 **–** Legal persons do not face criminal liability in Russia due to fundamental principles of domestic law. For instance, Article 49 of the Constitution contains the presumption of innocence ("Everyone accused of committing a crime shall be considered innocent until his guilt is proved…."). CrC Article 5 states that "[a] person shall be brought to criminal liability only for those socially dangerous actions (inactions[s])…of which his guilt has been established." The Supreme Court has not directly ruled on the question of corporate criminal liability and the fundamental principles are inferred from the use of language suggesting that only natural persons can be prosecuted.

Legal persons are subject to administrative liability for violations of the Code of Administrative Offences. This is without prejudice to the criminal or administrative liability of the natural persons that manage or direct a legal person (CAO Art. 2.1(3)). CAO Article 15.27(4) makes it an administrative offence for an organisation or its officials to negligently fail to observe the AML/CFT law if such a failure results in ML or TF "established by an effective court sentence." This offence is mainly intended to punish compliance violations by intermediaries, as discussed under R.35, and does not track he ML crime the way the administrative offence on TF tracks that crime. This is a shortcoming. Further, the sanctions that may be imposed on a legal entity are a fine of RUB 1 million (approximately EUR13 385) or suspension of activities for up to 90 days. The potential fine is relatively low and a legal person's administrative liability appears contingent on a criminal sentence having been imposed on an unspecified, natural person for related ML.

Criterion 3.11 **–** There are a range of ancillary offences applicable to ML, including participation (CrC Art. 33(2)); commission by a group of persons or criminal organisation (conspiracy) (CrC Art. 35); attempt (CrC Arts. 29-30); and aiding and abetting, facilitating, and counselling the commission of crime (CrC Art. 33).

Weighting and Conclusion

There are minor deficiencies related to the criminalisation of ML on the basis of the Vienna and Palermo conventions, uncertainty regarding whether financial transactions involving only virtual assets can constitute ML, and limited administrative liability for legal persons with sanctions that are not fully dissuasive.

Recommendation 3 is rated largely compliant.

Recommendation 4 - Confiscation and provisional measures

In its last MER, Russia was rated compliant with these requirements.

Criterion 4.1 – Russia can confiscate, upon conviction, assets held by criminal defendants and third parties, if the person or entity that received the property knew or should have known that it derived from criminal activity (CrC Art. 104.1(1) and (3); CPC Art. 81(3.6)).[86] Confiscation of virtual assets (VA) is not yet possible under Russian law. Although Russia can investigate and trace VA, it can only seize or confiscate VA once converted into another type of property.

a) ***Property laundered*:** The means of commission of a crime are subject to confiscation under CrC Article 104.1(1)(d). This includes funds or other assets laundered. SC Order No. 32 (2015) emphasises the necessity of confiscation with respect to persons convicted of ML.

b) ***Proceeds, including income or other benefits derived from proceeds, and instrumentalities used in or intended for use in ML or predicate offences*:** Money, valuables, and other property received as a result of committing certain offences, and any income from that property, are subject to confiscation under CrC Article 104.1(1)(a). Russian law includes a list of offences the proceeds of which can be confiscated. The list contained in CrC Article 104.1(1)(a) includes the ML offences and a wide range of predicates within the FATF's designated categories. However, there are some exclusions of entire or partial predicate categories from this list, including fraud, migrant smuggling, illicit trafficking in stolen and other goods, robbery and theft, tax crimes, extortion, and insider trading and market manipulation. The proceeds of these excluded offences cannot be confiscated through the CrC unless a conviction is obtained for the laundering of the proceeds of such predicates (see also SC Order No. 17 (2018), para. 2, confirming that list of crimes contained in CrC Article 104.1(1)(a) is exhaustive).

   If there is no ML conviction, the proceeds of these excluded predicate offences can be confiscated using the CPC. According to CPC Article 81(3) proceeds and income derived from proceeds are first subject to return to their legal owner (i.e., restitution). Next, if there is no rightful owner or such a person is not identified, proceeds are "passed into the ownership of the state" (i.e., confiscated). The crimes excluded from direct proceeds confiscation under the CrC are those likely to cause financial harm to victims, such as fraud and

[86] The main criminal confiscation provision is situated in the CrC, but because it does not fully cover proceeds from all categories of predicate offences, Russia must also rely on its CPC to cover the excluded offences.

theft. Russia has prioritised restitution over confiscation; confiscation is a last resort if there are no legal owners to compensate.

The 2008 MER noted that reliance on both the CrC and the CPC was suboptimal. Russia was urged to change this dual system and to simply include all predicate offences in CrC Article 104.1 as giving rise to confiscation. Prior to the enactment of Article 104.1 in 2007, Russia relied on the CPC exclusively for confiscation authority, which was not judged to be a strong legal basis. This assessment team echoes the concern that "the procedural confiscation that is available in the [CPC] may be vulnerable to criticism by the courts and others" and that "there is no policy reason as to why confiscation should not apply to all offences that are committed for a profit motive" (3rd Round FATF MER, p. 46 (2008)). While the CrC and the CPC provisions largely satisfy c.4.1(b) when read together, the CPC confiscation authority is not as fulsome as that contained in the CrC (see c.4.1(d)). Therefore, confiscation is possible for the predicate offences excluded from the CrC, but minor gaps remain within this complicated system.

Assets into which proceeds have been fully or partly transformed and income therefrom are subject to confiscation under CrC Article 104.1(1)(b). According to CrC Article 104.1(2), when proceeds or income derived from proceeds are commingled with clean property, the part of the property representing the value of the proceeds may be confiscated.

Instruments, equipment, or other means of commission of any crime, when such instrumentalities belong to the accused, are explicitly subject to confiscation under CrC Article 104.1(1)(d) and CPC Article 81(3.1). Instrumentalities in the possession of third parties are implicitly subject to confiscation in that they form part of "the rest of the objects" in a criminal case which shall be "passed to the ownership of the state" if they cannot be returned to an identified lawful owner (CPC Art. 81(3.6)).

c) ***Property that is the proceeds of, used in, or intended or allocated for use in the financing of terrorism, terrorist acts, or terrorist organisations***: Money, valuables, and other property used or intended for use in financing terrorism, extremist activities, and an illegal armed formation or criminal organisation are subject to confiscation under CrC Article 104.1(1)(c). The proceeds of TF and acts of terrorism are subject to confiscation directly (CrC Art. 104.1(1)(a)). Federal Law 35-FZ (2006), Article 24(3), states that the property of an organisation liquidated for its participation in terrorism is subject to confiscation.

d) ***Property of corresponding value*****:** Monetary funds or other property subject to confiscation that have been used, sold, or are otherwise unavailable, may be substituted. Pursuant to CrC Article 104.2, "the court shall issue a decision on confiscation of the amount of money corresponding to the value of the given item," or, a "decision on the confiscation of other property whose value corresponds . . . or is comparable" to the property that should be confiscated if there are no funds available or if they are insufficient. Unlike in the CrC, there is no explicit corresponding value confiscation authority for assets confiscated using CPC Article 81. This creates a shortcoming with regard to

the ability to confiscate value corresponding to the proceeds of certain predicates described above in (b), although in practice, authorities do so.

Russia also has measures for non-conviction based confiscation related to corruption and terrorism. Federal Law 230-FZ (2012) provides that unexplained wealth held by some, but not all, Russian public officials may be subject to forfeiture in civil proceedings initiated by prosecutors when the public official fails to confirm that his or her assets were legitimately acquired (Art. 17). This confiscation power extends to real property, vehicles/vessels, securities, or shares (Federal Law 230-FZ, Arts. 2, 17). Additionally, LEAs may investigate the origin of assets "possessed by the close relatives, relatives, and intimates of the persons who [have] committed a terrorist act where there are sufficient grounds to believe that the given property has been obtained as a result of terrorist activity and/or represents the income derived from such property" (Federal Law 35-FZ (2006), Art. 18(1.2)). Such property may be subject to forfeiture in civil proceedings initiated by prosecutors; the burden of proof is shifted to the person to prove lawful origin. An organisation associated with terrorism, on the rare occasion that it is legally registered (e.g., an NPO), also may have its property confiscated. This is done without a criminal conviction, upon a court's decision to liquidate the organisation (Federal Law 35-FZ, Art. 24(3)).

Criterion 4.2 –

a) ***Identification, tracing, evaluation*:** Competent authorities are able to conduct covert criminal intelligence activity and overt criminal investigations to identify and trace property subject to confiscation. Criminal intelligence is conducted within the scope of each LEAs' jurisdiction for the purposes of, inter alia, discovering crimes and perpetrators and identifying property which is subject to confiscation (Federal Law 144-FZ (1995), Arts. 1-2). Article 6 of Law 144-FZ permits a range of measures to be taken by operational agents performing criminal intelligence activity—including measures enabling the identification and tracing of assets—such as examining items and documents, interrogating persons, making inquiries, and examining premises and means of transportation. During the public investigation, investigators are further required to identify and trace property subject to confiscation pursuant to CPC Article 73. The evaluation and appraisal of assets is conducted by LEAs, experts hired by LEAs, or the FASPM for assets in its custody.

b) ***Provisional measures*:** Provisional measures are provided for in CPC Articles 115, 115-1, and 116 to prevent any dealing, transfer, or disposal of property subject to confiscation as proceeds, instrumentalities, property laundered, and corresponding value. According to CPC Article 115(1), property may be arrested for the purpose of guaranteeing the enforcement of a judgment in a civil action, the collection of a fine, other property levies, or criminal confiscation. Although this provision does not explicitly authorize the seizure of corresponding value, and in fact refers only to property confiscatable under subsection 1 of CrC Article 104.1 (proceeds/instrumentalities) and not Article 104.2 (corresponding value), Russian authorities explain that corresponding value can still be restrained or seized in practice. This is

because Article 104.2 is interpreted as a discretionary power exercised by the court at the time of the court's final decision on criminal confiscation, and it is not interpreted as a freestanding confiscation power. In other words, turning to property of corresponding value is a way to confiscate, not a new type of confiscation. Thus, Article 115's broad reference to arresting property to guarantee the effectiveness of criminal confiscation is unaffected by any later decision by a judge to substitute clean assets for dirty assets that were sold or are unavailable or insufficient. In practice, assets of corresponding value, which can include non-proceeds and non-instrumentalities (i.e., property not linked to crime), are seized and restrained without obstacle because CrC Article 104.2 only modifies what can be ultimately confiscated in place of assets named in Article 104.1. To arrest corresponding value, LEAs cite in their court petitions the "criminal confiscation" prong of CPC Article 115(a) and case examples confirmed that corresponding value can be subject to pre-trial seizure.

c) The arrest of property under the CPC can comprise a prohibition, a requirement to dispose of property or hand it to the custody of another, the seizure (arrest) of property, a restraint, or a restriction (CPC Art. 115(2), (6), (7)). Any property belonging to the suspect or the accused may be arrested upon the articulation of specific circumstances by the investigator (CPC Art. 115(2)). Any property held by third parties may be arrested upon a finding of sufficient grounds to believe the property represents proceeds or instrumentalities (CPC Art. 115(3)). Seizure requires the investigator and prosecutor to petition the court; the judge must consider the petition within 24 hours (CPC Art. 165). Only the State may participate in the court session concerning the petition, so it follows that the seizure may initially be sought on an ex parte basis (CPC Art. 165(3)). In exceptional cases when seizure is urgently needed, an investigator or prosecutor may take the necessary action to arrest property without judicial permission, so long as a judge is notified within three days and validates the legality of the action (CPC Art. 165(5)).[87]

   During criminal intelligence or the "pre-investigation phase," authorities may also seize property as evidence, or because it is the subject of the offence, and take it into custody (CPC Art. 81). These seizures do not require court authorisation and would generally be used against instrumentalities, such as items found at the scene of the crime or in the possession of an arrested suspect. During the public investigation, the investigator will apply to the court to officially seize these assets, using CPC Article 115 to "formalise" the seizure (except if the property is held strictly for evidentiary purposes). Amounts seized during the pre-investigative phase and the public investigation are subsequently included in final confiscation or restitution judgments.

[87] Property is defined in line with the FATF definition, as: "any things, for instance amounts of money in cash and certificated securities; the non-cash funds available in accounts and deposits in banks and other credit institutions; the certificateless securities in respect of which rights are recorded in a register of holders of certificateless securities or a depositary; property rights, for instance rights of claim and exclusive rights" (CPC Art. 5(13.1)).

d) ***Preventing or voiding actions*:** The court has discretion in fashioning measures that ensure Russia's ability to freeze, seize, or recover property that is subject to confiscation. Restrictions on the possession, use, and disposal of property are envisioned (CPC Art. 115(3)). The CvC may also be used to void actions that prejudice Russia's ability to freeze, seize, or recover property. Under CvC Article 169, a court may void transactions and recover, for the benefit of the State, property received in transactions completed by persons who acted wilfully and in violation of a legal order. CvC Article 170 may also be used invalidate sham deals/fraudulent transactions.

e) ***Appropriate investigative measures*:** Aside from the investigative measures available to trace assets described in c.4.2(a), GPO Order No. 87 (2017), Article 1(11)-(12), requires those supervising investigations into ML and predicate offences to ensure that proceeds and funds involved in the offences are seized and that confiscation is recommended. In cases of potential damage to the State and in order to enable civil recovery by the State, Joint Order RFM No. 105(1) (2016) requires LEAs to identify property subject to confiscation; to request information from banks, registrars, property and tax offices, employers of a suspect, and other authorities; to request Rosfinmonitoring information establishing financial links and potential laundering transactions; and to promptly apply for seizure of property located in Russia or abroad, upon identification. Article 2 of Joint Order 105 requires prosecutors to supervise investigations by LEAs to ensure all necessary measures are taken to recover damages inflicted on the State as a result of crime.

***Criterion 4.3* –** Laws and other measures provide some protection for the rights of bona fide third parties. The assets held by a person or organisation other than the defendant can only be confiscated if the defendant transferred the property to that person or entity and the recipient knew or should have known that the property had been received as the result of criminal actions (CrC Art. 104.1(3)). SC Order No. 17 (2018) acknowledges that confiscation may restrict the right of citizens to private property, and, as such, confiscation shall be implemented in accordance with the Constitution, universally recognised principles and norms of international law and treaties of Russia, and the requirements of criminal law and procedure. Property subject to confiscation cannot be returned to its owner if the owner participated in the crime (SC Order No. 17, para. 4). Harm caused to a legitimate owner is required to be considered by a court deciding on confiscation of corresponding value (SC Order No. 17, para. 10).

CPC Article 115(8) requires that when property is seized from a person, an explanation of the right to appeal the judicial decision authorising the arrest of property, as well as the right to move the court to modify any property restrictions or lift the seizure, shall be provided. An inordinately long arrest of property owned by a third party may offend the Constitution (CPC, note to Art. 115(2)). There are also procedures in the CPC for appealing and seeking revision of court judgments, including those ordering confiscation. Persons may appeal a judicial decision insofar as it concerns their rights and legitimate interests and an appeal can be taken before a final judgment is rendered in judicial decisions on punitive sanctions and the arrest of property (CPC Arts. 389.1(1), 389.2(3), 389.4(1), 389.6(2)). An appeal against a sentence must be filed within 10 days (CPC Art. 389.4), and an unfair sentence or

incorrect application of criminal law may result in reversal or alteration of a judgment. Thus, appeals may be used by third parties to contest confiscation decisions (CPC Art. 389.15).

CPC Article 81(1), provides that the fate of instrumentalities and proceeds enclosed in the criminal case shall be decided by the court at sentencing. Proceeds and income shall be returned to legal owners, or, if not, they shall be confiscated (CPC Art. 81(3.4)). The "rest of the objects" in the criminal case, such as property not deemed to be proceeds or instrumentalities, shall be returned to lawful owners and "disputes on the ownership of demonstrative proof shall be resolved by civil court proceedings" (CPC Art. 81(3.6)).

Despite the above, there are no particular provisions in Russian law requiring notice of confiscation to persons who may have a legitimate interest in property not already seized (if the property were seized, there would have been notice per CPC Article 115(8)).

Criterion 4.4 – Russia has a variety of mechanisms in place for managing and, when necessary, disposing of property frozen, seized, or confiscated. Court-issued seizure orders may contain terms on use and disposal of property (CPC Art. 115(1)-(2)); they may also include provisions relating to storage, custodians, or the use of a "specialist" to assist in seizure (CPC Arts. 115(2), (5), (6), and 58). Article 82 of the CPC provides the legal authority to LEAs to manage complex assets or assets that are expensive to maintain pending the conclusion of a criminal case. Seized assets, including funds resulting from assets subject to interim sale, are preserved by the relevant LEA or turned over to the FASPM; confiscated assets are usually passed to the general revenue fund for use in federal budgets (GR 848 (2012)). Tasks such as asset valuation and contracting with insurance agencies can be undertaken by the FASPM, and expenses incurred are charged to FASPM's annual budget (GR 848). Numerous other mechanisms are relevant to asset management and disposal, including GR 311 (2003); Federal Laws 229-FZ, Art. 104; Laws 178 and 118; GRs 432 and 1041; and the Administrative Regulation of the FASPM.

Weighting and Conclusion

Russia's legislative measures for confiscation are sufficient, but the proceeds of important predicate offences are not included in the main confiscation provision of the Criminal Code. Instead, reliance is placed on the CPC to confiscate the proceeds of certain ML predicates, after restitution is decided, and the CPC does not explicitly allow for confiscation of corresponding value. There is also a minor gap in that there is no requirement to notify third parties if property they may have an interest in, and that was not previously seized, is to be confiscated. Finally, confiscation does not reach virtual assets.

Recommendation 4 is rated largely compliant.

Recommendation 5 - TF offence

In its last MER, Russia was rated largely compliant with these requirements. The main deficiencies were that the TF offence did not extend to the theft of nuclear material and the lack of criminal liability for legal persons. The former has been adequately

addressed and while fundamental principles of law still appear to preclude criminal liability for legal persons.

Criterion 5.1 – The TF offence is contained in CrC Article 205.1 ("contributing to terrorist activity"). There is a minor deficiency in the criminalisation of TF on the basis of the TF Convention. Russia does not cover adequately the full scope of terrorist acts, the funding of which should constitute a TF offence.

Russia's TF offence prohibits the financing of 15 listed crimes. One of these, CrC Article 205 ("act of terrorism"), is the broadest. It is an overarching offence, defining acts that should be considered terrorism. However, Article 205 requires proof that the perpetrator had a specific intent—either the purpose of destabilisation of the activities of public authorities or international organisations or the purpose of influencing their decision making (CrC Art. 205 and SC Order No. 1, para. 1 (2012)).[88] Intimidation of the population is presumed to be intended by the nature of the act of terrorism, broadly defined in CrC Article 205. SC Order No. 1 provides that explosions, arson, or acts of a similar nature should not constitute terrorist acts when committed for non-terroristic reasons, such as revenge, personal animosity, etc. (para. 11).[89] Therefore, TF is criminalised in line with TF Convention Article 2(1)(b), but there are issues with Article 2(1)(a) of the Convention.

All treaty offences and sub-offences are crimes in Russia's Criminal Code either as free-standing crimes[90] or pursuant to Russia's catch-all terrorism offence in CrC Article 205. However, some of the treaty offences which should be *per se* acts of terrorism seems to require an impermissible proof of the defendant's specific intent.[91]

Technical compliance

88 Article 205 must be read in conjunction with SC Order No. 1. Paragraph 1 of that Order informs courts that a terrorist purpose is required under Article 205, but advises that all facts and circumstances of the perpetrated act should be taken into account in proving whether the intent of the defendant was directed destabilisation, such as time, place, and manner of the act, the nature and impact of the event, and the conduct of the perpetrator before and after the act. The Supreme Court thus directs that the context of the act or event may be evidence of a terroristic purpose, but this purpose, or specific intent, must still be shown. Paragraphs 2 and 3 of Order No. 1 instruct that explosions, arson, or bombings are covered by Article 205 when they frighten and endanger the population; the Order goes on to provide some examples of acts comparable to explosions which would frighten and endanger the population. These paragraphs explain how facts and circumstances should be considered as to whether the act, by its nature, puts people in fear of harm to their life, limb, loved ones, or property.

89 These examples of intents which would not be sufficient to prove guilt under Article 205 tend to confirm the assessors' view that there is indeed a specific intent element, even if it may be proven through circumstantial evidence.

90 E.g., CrC Articles 211, 360, 206, 220, and 221 criminalise treaty offences incorporated in the annex to the TF Convention either with no specific intent or with a permissible specific intent.

91 For example, high-jacking is separately criminalised without requiring any terrorist intent, which satisfies the TF Convention's incorporation of the Convention for the Suppression of the Unlawful Seizure of Aircraft. But acts which should be offences under the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation and the Protocol for the Suppression of Unlawful Acts of Violence at Airports are covered by Russia's catch-all offence, so they are not criminalised as *per se* acts of terrorism because they require proof of specific intent, or a terrorist purpose, as described in CrC Article 205(1). The same deficiency applies to acts which should be offences under the International Convention for the Suppression of Terrorist Bombings. The acts which should be offences under the Protocol for the Suppression

Thus, there are some gaps related to criminalisation on the basis of Article 2(1)(a) of the TF Convention. SC Order No. 1 requires courts to consider the overall circumstances of the act when determining whether it was committed with the essential terrorist purpose, which helps, but does not cure the deficiency.[92]

Criterion 5.2 – The TF offence is primarily criminalised in CrC Article 205.1(1.1) and secondarily in Article 208(1) (financing of an illegal armed group) and Article 361(2) (specific acts of international terrorism). The wilfulness element of the offence is implicit. The actus reus of the crime is "providing or collecting funds or providing financial services" (CrC Art. 205.1, n.1). SC Order No. 1, para. 16, elaborates that providing or collecting funds includes not only monetary funds (cash or non-cash), but also material such as clothing, equipment, means of communication, medication, residential or non-residential premises, means of transportation, etc. The non-exhaustive nature of this list is sufficient to cover "funds or other assets" as defined in the FATF Glossary, a phrase encompassing financial assets, economic resources—including oil and natural resources—and property of every kind, however acquired.

To commit a TF offence, the perpetrator must have one of the following mental elements: (1) knowledge that the funds are intended to finance the organising, preparing, or committing of at least one act on a defined list of acts of terrorism; (2) knowledge that the funds are for the purpose of committing certain acts of international terrorism; (3) intent to finance (or provide other material support to) a person with the aim that he commits at least one act on a defined list of acts of terrorism; (4) intent to provide support to an organised group, illegal armed group, or criminal organisation formed or being formed to commit at least one act on a defined list of acts of terrorism; or (5) intent to finance an armed group. An armed group, as described in SC Order No. 1, is a band, squad, militia, or other armed group, not stipulated in law, created for the realisation of certain goals such as the perpetration of terrorist acts (herein it is understood as a terrorist organisation).

Criterion 5.2 requires that a person must commit the offence with the unlawful intention that the funds should be used, or in the knowledge that they are to be used, to carry out a terrorist act, or by an individual terrorist or terrorist organisation. Russian law, as it relates to the financing of acts, requires proof that the perpetrator provided or collected funds "*in the knowledge that they are intended to finance*" the commission of terrorist acts. Thus, the mental element with regard to providing/collecting funds to carry out a terrorist act could be understood to inquire into the perpetrator's knowledge of the recipient's intended end-use of the funds,

of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf are specifically criminalised as sabotage under CrC Article 281, but Article 281 not one of the 15 listed crimes the financing of which is illegal. The acts under this Protocol could also fall under CrC Article 205, as crimes occurring on the continental shelf can be considered to have occurred within the jurisdiction of Russia according to CrC Article 11, but, as mentioned, the catch-all offence would then import an impermissible intent requirement for crimes which should be *per se* terrorism.

92 The FATF Guidance on Criminalising TF (R.5), para. 17 (2016), makes clear that a "catch-all" provision like CrC Article 205 may not be sufficient to criminalise the 30+ treaty offences, under the TF Convention Art. 2(1)(a), as most do not require the act to be committed with any particular purpose.

instead of asking only what the perpetrator intended to occur.[93] Also, R.5, like the TF Convention, uses the word "or" to describe the two possible intents with which TF can be committed; the Russian offence allows for one (knowledge) and not the other (intention) when it comes to the financing of acts. "Knowledge that funds are intended to finance" an act of terror does not encompass the FATF standard's alternative intent: that the perpetrator simply have an unlawful intention that the funds should be used for a terrorist act. The distinction is one of hoping or desiring that the recipient uses the funds to carry out an act of terror, versus knowing that he or she will do so. Russian authorities state that the relevant phrase in original Russian means that the perpetrator "realises" or is "aware" that the funds could be used for terrorist acts. The authorities also point to the fact that TF can be proven by showing the defendant acted not just wilfully, but negligently, as permitted by CrC Article 25. Negligence means that the perpetrator foresaw the possibility of a dangerous consequence (act of terrorism) and did not wish it to occur, but consciously allowed it or treated the possibility with indifference (by funding a terrorist). The assessment team does find a technical gap, but weighs it lightly due to these two mitigating factors.

With respect to the financing of an individual terrorist for any purpose, Russia is mostly compliant, but the assessors' understanding was developed by reviewing case examples. Russia does not formally recognise judicial precedent, but these cases interpret the law as codified, per the civil law tradition. What must be shown under CrC Article 205.1, n. 1, is that the perpetrator provides or collects funds or provides other material support to a person "with the aim"—or intending—that this person commits at least one of a number of specified crimes. This formulation appears at first not to cover the financing of an individual terrorist for any purpose because there must be an "aim" that the recipient commits some "act." However, one of the acts criminalised in Russia is membership in a terrorist organisation. Essentially, since being a terrorist is criminalised, any limitation apparent upon a plain reading of the TF law is mitigated. Numerous judicial decisions on this issue were reviewed by the assessment team.[94] Even though the language of the TF offense appears to require the financier to furnish funds with the aim that the individual terrorist should commit at

93 FATF Guidance is also instructive on this point. Any knowledge that the terrorist financier may have had about how the terrorist organisation/individual terrorist was using or intending to use the funds or other assets is not relevant to the TF offence. Similarly, it is not relevant to the scope of the TF offence the purpose for which the financier intended the funds to be used by the terrorist organisation/individual terrorist. Either aspect would add an element unnecessary to proving the crime. See FATF Guidance on Criminalising TF (R.5), paras. 21-22 (2016).

94 Two examples illustrate how a defendant can be convicted of TF where he or she intends only to finance the commission of an individual's ongoing commission of the crime of being a member of a terrorist organisation. In one case, the financier sent funds to be used on medical supplies and to materially support an individual who was providing medical care to wounded ISIL fighters in Syria. In another case, the defendant transmitted funds abroad to benefit his brother, who joined ISIL and was fighting in Syria. Discussions between the financier and his brother showed that the money was intended to support the brother's subsistence in Syria, as well as the purchase of specific equipment. These examples demonstrated that the actual use of the funds was not relevant to the court's finding of guilt and that a court can convict without any evidence of the perpetrator's intention to finance a specific terrorist act by the recipient other than the act of merely being a terrorist. The transfer of funds to these individuals in Syria was illegal due to the recipients' mere association with a terrorist organisation, ISIL.

least one act in a list of specified acts, one of those acts is, simply put, being a terrorist.[95] This interpretation of the TF offense by Russian courts confirms that the financing of an individual terrorist for any purpose is covered. Prosecutors need not show evidence of the perpetrator's intent that the recipient individual should carry out a terrorist attack. In practice, cases in which a person is found guilty of supplying funds to "participants in the activities of a terrorist organisation," without intention to finance a terrorist act, make up the majority of TF convictions. The only caveats are that the terrorist organisation with which the recipient is affiliated must be one that is recognised as such by Russia[96] and the funds should not be intended to facilitate the disassociation with the organisation such that one's status as a "terrorist" would be extinguished (for example, if the money was intended to be used to buy a plane ticket home from the conflict zone).

Criterion 5.2bis – The TF offence under CrC Article 205.1 includes the financing of travel of individuals who travel to a state other than their states of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts, or the providing or receiving of terrorist training. The receipt of training for the purpose of engaging in terrorist activity is a separate offence under CrC Article 205.3 and it is one of the 15 crimes the financing of which is prohibited. The same is true for organising and participating in terrorist organisations or their activities (CrC Arts. 205.4 and 205.5) and the participation in an illegal armed group, "in the territory of a foreign state" (CrC Art. 208(2)). The provision of training as well as planning or perpetrating terrorist acts are covered collectively by these provisions. The financing of travel of individuals to take part in terrorist acts could also be considered the finance of "preparing" to commit an act of terrorism per CrC Article 205.1, n.1. There is no geographic limitation in the main TF offence, meaning that financing the plans or activities of a foreign terrorist fighter are covered by CrC Article 205.1.

CrC Article 361(2) contains a separate offence that specifically addresses the financing of acts of international terrorism occurring outside of Russia. This provision criminalises, among other things, financing, recruiting, or training a person for such acts. Under this provision, the financing of travel of a person to perpetrate, plan, prepare, or participate in a terrorist act outside of Russia is restricted to those acts which endanger citizens of Russia or are aimed against the interests of Russia (CrC Art. 361(1)). According to the Concept of Combatting the Financing of Terrorism, a national strategic document signed by the President in 2009, all international terrorism is recognised as a threat to the national security of Russia.

Criterion 5.3 – The TF offence extends to any funds or other assets whether from a legitimate or illegitimate source.

95 CrC Article 205.5(2) makes it a crime to participate in the activities of an organisation which is recognised as terrorist organisation with Russian Law. This straightforward offence has no other elements and it is one of the 15 crimes listed in Article 205.1, the financing of which is illegal.

96 This recognition requires no formal process, announcement, or listing. For example, although the Supreme Court issued an Order recognising ISIL as terrorist organisation, there were 58 cases prosecuted relating to crimes involving ISIL prior to the issuance of that Order.

Criterion 5.4 – The TF offence does not require that the funds or other assets were actually used to carry out or attempt a terrorist act or that the funds be linked to a specific terrorist act.

Criterion 5.5 – The knowledge required to prove the TF offence may be inferred from objective factual circumstances. Generally applicable provisions of the CPC establish that mental elements may be inferred from facts (see c.3.8 for a list of these provisions).

Criterion 5.6 – Proportionate and dissuasive criminal sanctions apply to natural persons convicted of TF. The TF offence is punishable by imprisonment for a term of 8 to 15 years with the possibility of a fine up to RUB 700 000 (approximately EUR9 640) or 2-4 years' salary (CrC Art. 205.1(1.1.)). A maximum sentence of life in prison is also possible for TF (CrC Art. 205.1(1.1)) and there are certain enhancements in the range of potential terms of imprisonment for organising TF, financing an act of international terrorism, and financing an illegal armed group (CrC Arts. 205.1(4), 208(1), 361(2)). A person who commits TF may receive a conditional sentence (leniency under CrC Art. 73) if he or she, through timely notice to the authorities or otherwise, assists in the prevention or suppression of the crime financed, unless the person's actions also constitute another crime (CrC Art. 205.1, n.2).

Criterion 5.7 – Legal persons do not face criminal liability in Russia. The Constitution and Criminal Code are cited for the fundamental principles of law that prohibit imposing criminal sanctions on legal persons (see c.3.10 for a full description of these provisions).

Legal persons are subject to administrative liability for violations of the CAO. This is without prejudice to the criminal or administrative liability of the natural persons that manage or direct a legal person (CAO Article 2.1(3)). CAO Article 15.27.1, which largely tracks the language of the criminal TF offence, makes it an administrative violation for a legal persons to provide or raise funds or provide financial services with the knowledge that they are intended to finance terrorism. The penalty for this offence is a fine of RUB 10 to 60 million (approximately EUR 138 320 to EUR 829 930). This sanction is proportionate and dissuasive.

Additionally, Federal Law 35-FZ (2006), Article 24, prohibits the establishment and activities of organisations whose goals or actions are aimed at support of terrorism or at committing certain enumerated crimes in Ch. 24 of the Criminal Code, including the TF offence under Article 205.1. Upon application of the Prosecutor General, such an organisation can be liquidated by court order and its property confiscated (Federal Law 35-FZ, Art. 24(2)-(3)).

Criterion 5.8 – Attempt to commit TF is punishable under CrC Articles 29-30. Participating as an accomplice in a completed or attempted TF offence can be punished as participation in a terrorist community under CrC Article 205.4 and SC Order No. 1, para. 22.5, or participation in a terrorist organisation under CrC Article 205.5 and SC Order No. 1, para. 22.7. Aiding and abetting, facilitating, and counselling the commission of crime are recognised as a basis for liability in CrC Article 33, as well as in the TF offence itself (CrC Art. 205.1, n.1.1). Organising or directing others to commit a TF offence is covered by CrC Article 205.1(4). Liability for participation in the commission of a crime (CrC Art. 33(2)) and commission of a crime by a group of persons or criminal organisation (conspiracy) (CrC Art. 35) apply to TF.

Criterion 5.9 – TF is designated as a ML predicate offence by virtue of Russia's "all crimes" approach.

Criterion 5.10 – The TF offence applies regardless of whether the person alleged to have committed the offence is in the same country or a different country from the one in which the terrorist or terrorist organisation is located or the one in which the terrorist act has occurred or will occur (CrC arts. 11-12; CrC art. 361).

Weighting and Conclusion

There are minor shortcomings in Russia's criminalisation of TF. While all offences listed in the Annex to the TF Convention are covered, some of these offences require proof of a specific terrorist purpose. Also, the TF offence inquires into the perpetrator's knowledge of the recipient's intent. The law does not unequivocally permit the mental element of the TF offence to be proven with evidence of the mere "intention (as opposed to knowledge)" that funds should be used to carry out a terrorist act. Finally, the text of law does not obviously cover the financing of an individual terrorist for any purpose, but repeated judicial interpretation has shown that the law is broad enough.

Recommendation 5 is rated largely compliant.

Recommendation 6 - Targeted financial sanctions related to terrorism and TF

In its last MER, Russia was rated partially compliant with former SR.III due to weakness related to the implementation of UNSCR 1373. The FUR concluded that Federal Law No. 134-FZ added the relevant provisions to the AML/CFT regime to implement the remaining elements of SR.III, bringing the level of compliance to largely compliant.

Criterion 6.1 – For designations under UNSCRs 1267/1989/2253 and 1988:

a) The MFA is responsible for proposing the listing and de-listing of persons or entities to the 1267/1989/2253 and 1988 Committees (art. 10.2(1) L115). Other competent authorities (e.g., Rosfinmonitoring, LEAs, FSB) are obliged to cooperate and exchange information with the MFA for executing its listing/delisting decisions (art.10.2 L115).

b) The mechanism for identifying persons or groups for UN designation is not referenced in law. Russia states that the submission of proposals for designation may be based on a review of the domestic list established pursuant to UNSCR 1373, as well as the list of the IAC. During the onsite, the assessment team reviewed a confidential internal instruction that outlines the designation process.

c) Designation proposals are approved by the MFA. Final decisions are co-ordinated with Rosfinmonitoring and other relevant authorities (art.10.2 L115). Russia states that the identification process is based on a standard of "reasonable grounds or reasonable basis" and that a criminal conviction is not necessary for proposing a designation to the relevant UN committee.

d) See (e) below.

e) During the last five years, Russia has successfully proposed twelve persons and four groups to the 1267/1989/2253 and 1988 UN Committees by using the UN standard form and following the applicable UN-approved guidelines. The obligation to follow these procedures is not explicitly stated in any internal document. Russia refers to the successful proposals approved by relevant UN Committees as evidence that Russia uses the correct UN templates and provides sufficient accompanying information to support its proposals for designation, including identifying information and a statement of case. Russia does not automatically disclose its status as a designating state, but considers such disclosures on a case-by-case basis.

Criterion 6.2 – With regard to designations pursuant to UNSCR 1373, requirements are established in L115, the Presidential Decree to implement 1373 UNSCR requirements (PD 6), the Decision of the Government no.804 of 2015 on "the endorsement of rules for defining the list of organisations and natural persons concerning which there is information on their complicity in extremist activity or terrorism" (GR 804) and the Decree of the President of Russia No. 562 of 2015 "On Interagency Commission on Combatting the Financing of Terrorism" (PD 562).

a) Rosfinmonitoring is responsible for the formation of the list of organisations and natural persons when there is information on their complicity in terrorism (art.2 GR804). The criteria for domestic designations is a finding that a person is suspected of committing a range of terrorist-related offences in the Criminal Code, including the attempt to commit terrorism (art.6 (2.1) sub para 3 L115), or a court decision or conviction (both domestic and foreign) related to terrorism. When there is a lack of grounds for such inclusion, the IAC CFT[97] sends further requests for information to relevant authorities (art.4 PD 562). The IAC CFT is responsible for analysing third party requests for designation (art.7.4 L115; art.3 PD 562).

b) Rosfinmonitoring receives information from the GPO, IC, MoJ, FSB, and MoI to identify targets for domestic designation (art.6 (2.1) L115; art.2 GR 804). The IAC CFT, in the absence of criminal prosecution for terrorism and TF, receives materials to identify targets for domestic designation from LEAs and BoR when there are grounds to suspect involvement in terrorist activity (art.4 PD 562). The IAC CFT is also responsible for receiving and considering foreign requests for designations (art. 5(c) PD 562).

c) Foreign requests for domestic designations are received by Rosfinmonitoring through bilateral channels and sent to the IAC CFT, which must render its decision within 30 days (may be extended for up to 120 days) (art.6 and 9 PD 562). Decisions taken by the IAC CFT are sent to Rosfinmonitoring for subsequent publication on its website as well as to the requesting third country (art.10 and 11 PD 562).

[97] The IAC CFT is comprised of high level representatives of Rosfinmonitoring, Ministry of Internal Affairs, Federal Security Service and Ministry of Foreign Affairs, and is chaired by the deputy head of Rosfinmonitoring.

d) The grounds for inclusion in the domestic list pursuant to UNSCR 1373 is the existence of a criminal prosecution for terrorism (art.6 (2.1) L115). With respect to the IAC CFT list[98], the ground for inclusion is "sufficient grounds to suspect their involvement in terrorist activities (including TF)" (art.7.4 L115; art.3 PD 562). This legal basis is also applied to third country requests. In the absence of a foreign conviction, the foreign request may be considered for designation to the IAC CFT List.

e) There are no legal provisions regarding outgoing requests, but both the general provisions on international co-operation (art.10 L115) and bilateral international agreements may be used. Co-operation is based on the principle of reciprocity.

Criterion 6.3 –

a) Both Rosfinmonitoring and the IAC CFT receive information from federal authorities, and third countries. The CFT Commission also has the authority to solicit information in order to meet the designation criteria (art.15 GR 804; art.5(c) PD 562).

b) Both Rosfinmonitoring and the IAC CFT operate without prior notice to the person or organisation identified for designation (art.4 L115).

Criterion 6.4 – Under the Constitution of the Russian Federation, international treaties (including UNSCRs) are a component of the legal system without the need for a separate act of implementation. However, the relevant UNSCRs do not include all the elements required to be enforceable means under the FATF Standards. The AML/CFT Law, while requiring immediate freezing, does not indicate the moment when such an obligation arises. Instead, it sets the deadline for the implementation of the relevant UNSCR requirements to the publication of UN decisions on the Rosfinmonitoring's website. This gives rise to a risk of delayed implementation of freezing obligations which is not in line with FATF requirements. Under such interpretation of the law, Russia implements TFS within two days. Rosfinmonitoring is required to publish its listing decisions on its official website "in the course of one working day" following the UN decision to list/delist, and immediately following domestic designations (art.20 GR 804). For IAC CFT domestic designations, the IAC CFT is required to inform Rosfinmonitoring on freezing decisions taken (art.10 PD 562 Regulation). Rosfinmonitoring is required to publish "immediately" such decisions on its official website (art.7.4 (2) L115).

FIs and DNFBPs are required to implement the freezing measures immediately, and *no later than one working day after the publication of the listing on the Rosfinmonitoring website* with respect to the UN1267/1988 and 1989 lists and domestic designations pursuant to UNSCR 1373 (art.7 (1) sub para 6 L115). For IAC CFT domestic designations, freezing obligations for FIs and DNFBPs must be implemented immediately and no later than one working day after publication on the website of Rosfinmonitoring (art.7.4 (2) L115).

98 The IAC CFT list deals with cases both coming from third country requests and in the absence of ground for the inclusion in the list of terrorist as per above mentioned points a) and b) because there is no criminal prosecution.

As a result of this two-step process, FIs and DNFBPs are required to implement TFS freezing measures within 48 hours following a designation (both at the UN and domestically) instead of within a matter of hours as defined in the FATF Glossary.

Criterion 6.5 –

a) FIs and DNFBPs are required to implement freezing measures of "monetary funds or other assets" immediately, and no later than one day, from the publication of the designation on the websites of Rosfinmonitoring (art.7.6 sub para 6) L115). These freezing measures must be conducted without prior notice (art.4 L115). These freezing requirements do not extend to all natural and legal persons. Russia refers to art.15 (4) of the Constitution[99] to establish an automatic incorporation of the relevant UN lists (1267/1989/1988) into domestic law. However, there are no provisions which explicitly provide for liability for infringing the prohibition by all natural and legal persons (other than FIs and DNFBPs). Russia states that it could use its TF offence to prosecute violations of the freezing requirements by natural persons, or its administrative offence for legal persons. However, neither offence has an affirmative freezing obligation. Instead, they prohibit the provision or collection of funds or the provision of financial services.

b)

i. The AML/CFT Law does not include a definition of "monetary funds or other assets". Russia states that several articles in different codes (CvC, CPC, Tax Code) and two laws (L39 of 1996 "on securities market" and L7 of 2002 "On environmental protection") broadly cover the FATF definition of "funds or other assets", and is applicable to L115. The freezing obligation in L115 extends to "funds and other assets belonging to" a designated person or organisation (art.7(6)), and does not cover funds or other assets "controlled", even though FIs and DNFBPs can suspend a transaction for five working days [extended to 35 days if needed (art.8 L115)] when a legal entity or natural person is acting on behalf of on the instructions of designated organisations or persons (art.7(10) L115). They are required to immediately supply information about the suspended operation to Rosfinmonitoring, which could convert the suspension into a permanent freeze (art.8 L115).

ii. FIs and DNFBPs must suspend the transactions and freeze accounts for five working days (extended to 35 days if needed) when a legal entity or natural person is suspected of being directly or indirectly under the ownership or control of designated organisations or persons (art.7(10) L115). They are required to immediately supply information about the suspended operation to Rosfinmonitoring, which could convert the suspension into a permanent freeze, if a positive determination is made (art.7(10) L115). When such a decision is taken, it remains valid until it is revoked (art.8 L115).

[99] Article 15.4 of the Constitution states that "the universally recognised norms of international law and international treaties and agreements of Russia are a component part of its legal system. If an international treaty or agreement of Russia establishes other rules than those envisaged by law, the rules of the international agreement shall be applied."

iii. The obligation to freeze funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons/entities is not referenced explicitly in law. However, any income derived from the funds of a listed person/entity becomes property covered by the existing freezing measures based on Russia's broad interpretation of art.15(4) of its Constitution.

iv. The obligation to freeze funds or other assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities is not required by legislation. However, FIs and DNFBPs must suspend the relevant operation for five working days (extended to 35 days if needed (art.7(10) L115) when a legal entity or natural person is acting on behalf of on the instructions of designated organisations or persons (art.7(10) L115). They are required to immediately supply information about the suspended operation to Rosfinmonitoring, which could convert the suspension into a permanent freeze, if a positive determination is made (art.7(10) L115).

c) FIs and DNFBPs are prohibited from carrying out transactions involving funds or assets (art.7 L115). This prohibition, read with articles 153 and 185 of the CvC, also prohibits FIs and DNFBPs from providing financial or other related services.

i. Russia does not have an explicit prohibition that applies to natural and legal persons beyond FIs or DNFBPs. Russia states that art.15(4) of its Constitution automatically incorporates the requirements of all UNSCRs into Russian domestic law, thereby establishing a prohibition for all natural and legal persons. However, no penalties exist for violation of UNSCRs by all natural and legal persons (other than FIs and DNFBPs). Furthermore, the UNSCRs place obligations on member states themselves, and not on natural and legal persons within those member states. Therefore, these requirements contained within the relevant UNSCRs are not legally enforceable.

ii. Russia also states that it could apply its TF offence in such circumstances, but the use of TF offences to enforce UNSCRs is considered inadequate by the assessment team. First, the TF offence requires the proof of intention by the defendant, whereas the prohibition on making funds or other assets available does not have a mens rea requirement. Second, the TF offence does not cover those who act on behalf of, or at the direction of, designated persons or entities. Third, as of the date of the onsite visit, judges were not instructed to automatically consider UN designated persons as terrorists in TF cases.[100] Even if it is possible to use the TF offence to enforce the prohibition, no such cases did so prior to the end of the on-site visit.

d) Rosfinmonitoring is required to publish changes to its consolidated list on its website within one working day after that the decision is taken (art.20

[100] However, in June 2019, an order on initiation of a criminal case noted that a person was a terrorist by virtue of their UN designation, and an additional establishment of proof was not required.

GR804), and on National Gazette, the Rossiyskaya Gazeta. Decisions taken by the IAC CFT must also be immediately published on Rosfinmonitoring website (art.7.4 L115). A notice is also issued on the main page of Rosfinmonitoring and organisations/individuals can subscribe to alerts via the Personal Account. The requirement to provide clear guidance to FIs and other persons or entities, including DNFBPs, is not referenced in L115 but it is part of both Rosfinmonitoring (PD 808) and BR powers (art. 77 L86), and both authorities have issued guidance.

e) FIs and DNFBPs must immediately inform Rosfinmonitoring on freezing measures taken, as per the procedures established by Rosfinmonitoring (art.7(6) L115). Attempted transactions must also be reported to Rosfinmonitoring (art.7(13) L115). These requirements state that organisations and individual entrepreneurs must "immediately" submit information on freezing to Rosfinmonitoring (art.3(c) and art.4(c) GR209).

f) The rights of bona fide third parties are protected under the L115 (art. 7.4 (5)).

Criterion 6.6 –

a) The MFA is responsible for forwarding listing and delisting requests to the relevant UN Committees (art.10.2(1) L115). Russia states that it applies the procedures set out in the relevant UNSCRs for potential delisting. Although, the procedures for Russia to submit delisting requests to the relevant UN committees are not referenced in law, Russia has successfully requested to remove a person from the UN 1267 list. During the onsite, the assessment team reviewed a confidential internal instruction that outlines the designation process and confirms the authorities' view.

b) A broad legal framework exists in order to delist persons and organisations from the domestic terrorist list (art.6 (2.2) L115). The IAC CFT can revoke a designation upon receipt of documents substantiating such cases. Every six months, the Commission verifies information on organisations and persons on whom decisions on freezing have been taken. On the basis of received written requests, the IAC CFT may amend decisions taken previously or revoke them (arts.14-16 PD 562). Such decisions are sent to Rosfinmonitoring for immediate publication on its website (art.15 PD 562) and includes a notice of changes to the list (para.6 RFM 232). An extract from the minutes of the meeting of the IAC CFT containing the decision taken is posted on the official website of Rosfinmonitoring immediately, and no later than the working day following the date of receipt, places any change into Personal accounts of the organisations, individual entrepreneurs and other persons, on the official website of Rosfinmonitoring (para.4 RFM232).

c) Decisions on designation taken by the IAC CFT and Rosfinmonitoring may be appealed by persons or organisations domestically designated (art.7.4(3) L115). The conditions for removal include the repeal of a sentence or of a court decision for the national list (art.6(2.2)).

d) In regard to UNSCR 1988 and the Al-Qaida Sanctions list, Russia states that it applies the procedure set out in the UNSCR for delisting, which is available on the UNSC website, which is hyperlinked on the Rosfinmonitoring website.

Moreover, the MFA has the explicit authority to submit delisting requests (art.10.2(2) L115).

e) See (d) above.

f) Persons or organisations which have been inadvertently affected by a freezing mechanism (i.e. false positive), may submit an application to Rosfinmonitoring, who must inform the applicant of its decision within ten working days. The MoJ, MoI, FSB must provide Rosfinmonitoring with specific information no later than five working days from the date of Rosfinmonitoring request (art.11 GR 804). The applicant may also appeal Rosfinmonitoring's decision in court (art.6 (2l.3) L115). Decisions taken by the IAC CFT may also be appealed in court (art.7.4 (3) L115).

g) The same procedure explained above applies [see c.6.5(d)].

Criterion 6.7 **–** Russia has measures in place to allow access to frozen funds or other assets that are deemed necessary for basic expenses, for the payment of certain types of fees, expenses and service charges, or for extraordinary expenses. This applies to both domestic lists (art.7.4 para 4 L115; and art.12 PD562) and the international UN list (art.6(2.4 and 2.5) L115). All transactions involving the access to funds by a designated person are subject to MCR obligations, and must be filed to Rosfinmonitoring (Art.6(2.4)(4)).

Weighting and Conclusion

Russia generally implements its TF TFS obligations through an automatic incorporation of the relevant UNSCRs though its Constitution and AML/CFT Law. However, two deficiencies exist: (1) it can take up to two days for FIs and DNFBPs to implement TFS, which is not considered as occurring "without delay"; and (2) there are no legally enforceable requirements that apply to all natural and legal persons (beyond FIs and DNFBPs) to freeze or prohibit the provision of funds/assets/services to designated persons or entities.

Recommendation 6 is rated partially compliant.

Recommendation 7 – Targeted financial sanctions related to proliferation

This is a new Recommendation that was not assessed in the last MER. The AML/CFT Law (L115) together with Guidelines issued in 2018 by the Government (GR 1277) apply.

Criterion 7.1 **–** Rosfinmonitoring is responsible for implementing PF-related TFS (art.1 GR 808). The grounds for including an organisation or natural person in Russia's list related to the proliferation of weapons of mass destruction is "provided for by Chapter VII of the Charter of the UN, the UN Security Council or by the bodies especially established by decisions of the UN Security Council" (art.7.5(2) L115). Guidelines on how to compile the national list of entities and individual designated by relevant UNSCRs was approved on October 2018 by the Government (GR 1277). FIs and DNFBPs must freeze and block monetary funds and other assets of the organisations or natural persons designated as involved in the proliferation of weapons of mass destruction immediately and no later than one working day after the publication of the relevant list on Rosfinmonitoring's website (art.7.5(5) L115).

under the Constitution of the Russian Federation, international treaties (including UNSCRs) are a component of the legal system without the need for a separate act of implementation. However, the relevant UNSCRs do not include all the elements required to be enforceable means under the FATF Standards. The AML/CFT Law, while requiring immediate freezing, does not indicate the moment when such an obligation arises. Instead, it sets the deadline for the implementation of the relevant UNSCR requirements to the publication of UN decisions on the Rosfinmonitoring's website. This gives rise to a risk of delayed implementation of freezing obligations which is not in line with FATF requirements. Under such interpretation of the law, as a result of this two-step process, FIs and DNFBPs are only required to implement TFS freezing measures within two days following a designation instead of within a matter of hours, as defined in the FATF Glossary.

Criterion 7.2 –

a) PF TFS must be implemented immediately, and no later than one working day, by FIs and DNFBPs after the publication on Rosfinmonitoring's website (Art.7.5(5) L115). This requirement does not extend to all natural and legal persons (other than FIs and DNFBPs). Similar to TF TFS, Russia refers to art.15 (4) of the Constitution to establish an automatic incorporation of the relevant UN lists into domestic law, however, this requirement does not extend to all natural and legal persons (other than FIs and DNFBPs) since there are no provisions which explicitly provide for liability for infringing the prohibition by all natural and legal persons (other than FIs and DNFBPs).

b) See below:

i. The AML/CFT Law does not include a definition of "monetary funds or other assets". Several articles in different codes (CvC, CPC, Tax Code) and two laws (L39 of 1996 "on securities market" and L7 of 2002 "On environmental protection") broadly cover the FATF definition of "funds or other assets" and applies to the AML/CFT Law. The freezing obligation does not cover the funds and assets under control of designated persons or entities. However, FIs and DNFBPs are required to suspend for five working days a transaction that involves a legal entity directly or indirectly owned by, or individuals and entities under control of or acting on behalf of, a UN listed individual or entity (art.7.5(8) L115). FIs and DNFBPs are required to inform Rosfinmonitoring, which may make a decision within five days (and may be extended for up to other 30 days) (art.8 L115). If Rosfinmonitoring does not take a decision within this timeframe, the transaction may occur, otherwise freezing measures are taken. Incoming funds are exempted from suspension (art.7.5(8) L115). This temporary administrative freeze may be extended by court order.

ii. The obligation to freeze funds and other assets wholly or jointly owned or controlled, directly or indirectly by UN listed persons and entities is not referenced in law. However, the same power to suspend as described above, applies under sub (ii).

iii. There is no reference in law to freeze the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities. However, any income

derived from the funds of a listed persons/entities becomes a property covered by freezing measures. The same power to suspend as described above, applies under sub (iii).

iv. The obligation to freeze funds and other assets of a person acting on behalf of, or at the direction of, listed persons or organisations is not referenced in law. However, the same power to suspend as described above, applies under sub (iv).

c) Russia does not have an explicit prohibition that applies to all natural or legal persons from making any funds or other assets, economic resources, or financial or other related services available, directly or indirectly, wholly or jointly, for the benefit of designated persons or entities; and persons and entities acting on behalf of, or at the direction of, designated persons or entities. Instead, Russia "blocks" FIs and DNFBPs from carrying out transactions involving funds or assets (Art.7 L115).

   Russia does not have an explicit prohibition that applies to natural and legal persons that are not FIs or DNFBPs. Russia states that art.15(4) of its Constitution automatically incorporates the requirements of all UNSCRs into Russian domestic law, thereby establishing a prohibition for all natural and legal persons. However, these requirements do not extend to all natural and legal persons, since there are no provisions which explicitly provide for liability for infringing the prohibition by all natural and legal persons (other than FIs and DNFBPs). Therefore, the requirements contained within the relevant UNSCRs are not legally enforceable.

d) Rosfinmonitoring informs FIs and DNFBPs about any decision taken by the UNSC by publishing on its website the changes to the lists no later than one day after the publication by the UN. Alerts are also circulated to FIs and DNFBPs through Rosfinmonitoring's Personal Account. Changes (listing, de-listing, amendment) are also included, once a month, in the Official Gazette, Rossiyskaya Gazeta (GR 1277). The requirement to provide guidance on TFS to FIs and DNFBPs is the responsibility of Rosfinmonitoring (PD 808) and the BR (art. 77 L86). The BR recently issued an informational letter from 29 December 2018 about identifying natural and legal persons which are related with PF TFS (BR 1284).

e) FIs and DNFBPs must immediately inform Rosfinmonitoring on freezing measures taken, under procedures established by Rosfinmonitoring and the BR depending on the nature of the institution that has taken freezing action (art.7.1.6 L115). Attempted transactions must also be reported to Rosfinmonitoring (art.7(13) L115). These requirements state that organisations and individual entrepreneurs must "immediately" submit information on freezing to Rosfinmonitoring (art.3(c) and art.4(c) GR209).

f) The rights of FIs and DNFBPs acting in good faith when undertaking freezing actions are protected (art.7(12) L115).

Criterion 7.3 – FIs and DNFBPs are required to check once every three months if their existing clients are designated and report the results to Rosfinmonitoring (art.7.5(6) L115).

FIs and DNFBPs who fail to comply, including the PF TFS obligations to freeze, may face civil, administrative, and criminal liability, and may have their licences revoked. Officials of FIs and DNFBPs may also be liable to administrative, civil or criminal sanctions (art.13 L115). Fines on officials range from RUB 30 000 to 40 000 (approx. EUR 467); on legal entities ranging from RUB 300 000 to 500 000 (approx. EUR 4 000-6 600); or the administrative suspension of activities for a period up to 60 days (art.15.27(2.1) CAO). Specific sanctions are established by several pieces of legislation for failure to comply with AML/CFT requirements. In particular, non-compliance:

- by credit institutions may result in revocation of the licence (art.20, 6.1 of L395-1);
- by consumer credit cooperatives can entail the imposition of prohibition to attract funds from members, admit new members and grant loans (art. 5(3)(7) L190); or liquidation (art. 5(3)(9)(c) L190);
- repeatedly breaching in one year by agricultural consumer credit cooperatives can entail the imposition of prohibition to attract funds from members, admit new members and grant loans (art. 40.2 (1)(10)(3) L193), or liquidation (art. 40.2 (1)(11)(4) L193);
- repeatedly breaching in one year by professional securities market participants, can result in licence cancellation (art.39.1 (1)(8) L39);
- by pawnshops can entail liquidation by a decision of the RF Court (art 2.3 (4)(6)(a-c) L196);
- repeatedly breaching in one year by microfinance organisations may result in removal from the government register (art.7(1.1)(3) L151).

Criterion 7.4 –

a) Rosfinmonitoring, in co-operation with MFA, is the central authority for submitting delisting requests to the Focal Point established pursuant to UNSCR 1730 (art.10.2(2) L115). Russia provides a hyperlink to the relevant UN sites on Rosfinmonitoring's website.

b) The AML/CFT Law permits "erroneously" affected natural and legal persons to submit a written application to Rosfinmonitoring, which must then must make a decision within ten working days. The decision of Rosfinmonitoring may be judicially appealed (art.7.5(4) L115).

c) The AML/CFT Law provides the possibility for listed persons and entities to submit via Rosfinmonitoring, requests to access frozen funds for both basic and extraordinary expenses. Requests are forwarded to the relevant UN bodies for approval (art.7.5(7) L115). Distinction between basic and extraordinary expenses is envisaged in presidential decrees for Iran and DPRK (art.5 PD 109; art.2 PD 665). Rosfinmonitoring must inform the petitioner and the institution that holds the frozen funds on the outcome of the request (art.7.5(7) L115).

d) De-listings are communicated to FIs and DNFBPs in the same manner as listings and amendments to the relevant UN lists (see c.7.2(c)).

Criterion 7.5 –

a) Provisions to permit the addition to accounts frozen pursuant to UNSCR 2231 (Iran) of interests or other earnings due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts were blocked are referenced in law (art. 3 and 4 PD109). Similar provisions with respect to UNSCR 1718 (DPRK) are also referenced in law (art. 7(8) L115).

b) The AML/CFT Law permits the "making of payments under agreements (contracts) made before the inclusion of the given organisation or natural person into the lists…connected with proliferation of mass destruction compiled by the UN Security Council." This article also states that such requests must be submitted in writing, by Rosfinmonitoring. The MFA is required to submit the request to the UN for consideration (art.7.5(7) L115).

Weighting and Conclusion

Russia generally implements its PF TFS obligations through an automatic incorporation of the relevant UNSCRs though its Constitution and AML/CFT Law. However, two deficiencies exist: (1) it takes up to two days for FIs and DNFBPs to implement PF TFS; (2) there are no legally enforceable requirements that apply to all natural and legal persons (beyond FIs and DNFBPs) to freeze or prohibit the provision of funds/assets/services to designated persons or entities.

Recommendation 7 is rated partially compliant.

Recommendation 8 – Non-profit organisations

In its last MER, Russia was rated partially compliant with the requirements relating to NPOs (former SR.VIII). As the requirements in Recommendation 8 have changed considerably since then, the previous analysis is no longer relevant.

The legal framework for NPOs consists of Federal Law No. 82 of 1995 "On public associations" (L82), Federal Law No. 7 of 1996 "On non-profit organisations" (L7), Federal Law No. 125 of 1997 "On freedom of conscience and religious associations" (L125), Federal Law No. 129 of 2001 "On the State Registration of Legal Entities and Individual Businessmen (L 129), and Presidential Decree No. 1313 of 2004.

NPOs are defined in law as organisations not having profit-making as their main objective and not distributing earned profit among the participants (art.2 L7). NPOs must be registered as a legal entity (art.3.1 L7); such registration can be denied if legislative requirements are not satisfied (art. 23 L129). NPOs can be created in the form of social or religious organisations, communities of the aboriginal minorities of Russia, Cossack communities, non-profit partnerships, institutions, autonomous non-profit organisations, social, charitable and any other funds, associations and unions (art.2 L7). Legislation makes reference to a possible prohibition for persons included in the consolidated terrorists list from acting in the capacity of NPO founders ((art.15(2)(2) L8; art.19(2)(2) L82; art 9(3)(3) L125). Furthermore, a person previously head of, or member of, the board of a public or religious association or other NPO, subject to a court decision (liquidation or prohibition of activity) cannot be the founder of a public association, religious and other organisation within ten years from the date of entry into force of the relevant court decision (art.15(1.2-1) L7; art.19 L82; art.9(3) L125).

Non-commercial organisations total around 643,000, of which approximately 212,000 are NPOs.[101] The MoJ is responsible for supervising the sector (art.1 PD1313).

Criterion 8.1 –

a) The 2018 TF NRA includes a section on the TF risks in the NPO sector, which states that the majority of NPOs are considered low risk due to the type of activities conducted. One relevant vulnerability was identified, which is when funds collected by NPOs are not credited to accounts, but kept in cash or credited to bank cards or other means of payment (e.g. electronic wallets, mobile phone accounts).

   A sectorial NPO risk assessment,[102] conducted in 2018 by Rosfinmonitoring in collaboration with LEAs and the MoJ, identifies the subset of organisations that fall within the FATF definition of NPOs as: NPOs (autonomous NPOs, foundations, private establishment, associations, Cossack society, minority communities), public associations (public organisations and social movements), religious organisations and charitable organisations.[103]

   The SRA reviewed the risks associated with each legal form of NPO, based on their legal form and structure, focusing primarily on risk mitigation through the presence of structural safeguards against misuse required by the law, and also based on the results of TF investigations of each form of organisation. The sectoral assessment did not assess how different NPOs within each legal form may be exposed to different levels of TF risk by virtue of their activities or characteristics (e.g. their objectives and funding sources; their operations and services, or their geographical scope), except for the vulnerabilities of using cash. The risk assessment does not have the level of specificity required by this criterion, and a more granular assessment should be conducted to identify the features and types of at-risk NPOs within those legal forms rated as medium-risk or higher.

b) Russia identified the nature of the threat posed by terrorists and terrorist entities and their potential abuse of high risk NPOs in its sectorial NPO risk assessment.

c) Russia reviewed the adequacy of measures that govern the whole NPO sector, and considered it effective in protecting NPOs from possible misuse for TF purposes, including measures aimed at mitigating TF risks. Nevertheless, the Russian authorities are considering, in the long-term, to adopt a new regulations on different ways to collect funds, including through money transferred to NPOs' bank accounts, as well as on how to identify persons involved in such transactions.[104] These measures are also included in Russia's CFT Action Plan.

d) The TF NRA concludes that further work should be done to assess the TF risks in the NPO sector. Since 2014, Rosfinmonitoring, competent authority for

101 From the ML NRA 2017-2018 non-public version (page 28).

102 The methodology for determining the level of risk was based on the methodology provided in the TF NRA.

103 The assessment of the risk in the NPO sector (2018).

104 The existing preventive mechanism provides an effective barrier to the creation of NPOs in order to finance terrorists and terrorist groups" (TF NRA 2017-2018)

coordination (art.5(16.1) RFMR) has submitted annual reports to the President of Russia on national security threats (see also c.1.1), which provide for regular updates on the respective risk assessments. Neither the TF NRA nor its methodology, however, include a reference to periodically reassess the risks faced by the NPO sector.

Criterion 8.2 –

a) NPOs are subject to government registration as legal entities (art.3.1 L7). Documents necessary to establish an NPO are also sent to the government registration authority (the local authority of the FTS) for inclusion in the USRLE. Information included in the register is publicly available through the FTS website, as well as on the MoJ's NPO Information Portal (art.19(4-5) L135).[105]

   All NPOs are required to maintain accounting and statistical records, and keep records of transactions with funds received from foreign sources. NPOs are also required to report on activities conducted, members of their management board and purposes for which funds are spent (art. 29 L82). This information is publicly available.

b) Rosfinmonitoring together with the ITMCFM and the Public Chamber, compiled a document entitled, "CFT Recommendations for NPOs", which includes the relevant FATF reports on how NPOs can protect themselves from potential TF abuse. The local offices of the MoJ have been instructed to inform NPOs about the public version of the TF NRA as well as on CFT Recommendations for NPOs, which are publicly available on the websites of Rosfinmonitoring, ITMCFM, MoJ and Public Chamber.

c) Every year, the NPO sector organises workshops, roundtables and working meetings where authorities engage directly with some NPOs. Since the public versions of the TF NRA and SRA of NPOs were published in 2018, additional events were held in different regions to highlight current trends, risks, and ways to prevent the use of NPOs for TF.

d) Specific instructions to the sector are included in the CFT Recommendations (section 4 (b)) in order to encourage conducting transactions via regulated financial channels.

Criterion 8.3 – Russia applies uniform TF risk mitigation measures on all NPOs, with additional measures applied to charitable organisations.[106] All NPOs are required to maintain accounting and statistical records; keep records of transactions with funds received from foreign sources; and report on activities conducted, members of their management board and purposes for which funds are spent. However, charities, which were identified as having a medium risk in the NPO sectoral assessment, must also submit further and detailed information (art.19 L135).

[105] Information on activities carried out by NPOs, on members of their management bodies, on how properties are used and funds spent, including funds received from foreign sources.

[106] The risk-oriented approach is envisaged by the law (art. 18 L294) in order to prevent violations of mandatory requirements, and it is not conducted for specific AML/CFT purposes.

MoJ on-site and off-site inspections are scheduled based on annual inspection plans approved by the GPO, taking into account reputational information and concerns raised by LEAs with respect to potential TF abuse. Ad hoc inspections may also be conducted if particular concerns are raised by other relevant authorities, including when TF concerns exist (art.32(4.2) L7).[107]

Criterion 8.4 –

a) As noted above, the MoJ is responsible for supervising the NPO sector. During onsite inspections, authorities monitor the application of the registration and accounting requirements, as well as screening founders and managers of NPOs against the consolidated list of terrorists. Funds and/or other assets transferred to a Russian NPO from foreign states, international and foreign institutions, foreign citizens and stateless persons, and when the NPO spends funds and/or other assets is subject to mandatory control, if the amount of the transaction is equal to or exceeds RUB 100 000 (approx. EUR1 340) (art.6(1.2) L115).

b) NPOs are subject to effective, proportionate and dissuasive sanctions for violations of their obligations. Depending on the violations, sanctions can include ineligibility, warnings, suspension of activity, imposition of administrative liability and liquidation (art.3.11 CAO; art.32(5.5) L7; art.42 L82; art.61(3) CvC).

Criterion 8.5 –

a) Within the IAC CFT, information on NPOs can be shared to ensure co-operation and coordination among competent authorities. Although the MoJ is not a member of the IAC CFT[108] it can be involved in its work, and may also propose freezing measures in relation to potential domestic terrorist designations (art.4 PD562).

b) LEAs have the expertise and capability to investigate TF and are able to use a wide range of investigative techniques for the investigation of TF (see R.31).

c) The MoJ can request administrative and executive documents, which are mostly publicly available. Restricted information (i.e. passport details) can be provided to government authorities, including LEAs, during an investigation.

d) The MoJ carries out its activity, including the supervision of the NPO sector, in co-operation with other federal executive bodies, executive bodies of the constituent entities, local self-government bodies, public associations and organisations (art.3(6) PD 1313), IAC CFT, and the National Antiterrorism Committee (NAC) that co-ordinates counter-terrorism activities (PD 116 and PD 664). If a suspicion arises that an NPO is involved in TF activities, or it is being misused for TF purposes, this information is referred to LEAs for investigation.

[107] A particular concern can be related to the breach of legislation in terms of, for example, registration, upon Prosecution's specific request, because the term with respect to an irregularity found during a previous inspection expired, etc.

[108] Members of IAC CFT are: Federal Security Service, Ministry of Internal Affairs of Russia, Ministry of Foreign Affairs of Russia and Rosfinmonitoring,

Criterion 8.6 – The AML/CFT Law provides the legal framework to respond to international requests with respect to all issues related to AML/CFT, including NPOs suspected of TF or involvement in other forms of terrorist support (art.10 L115). Rosfinmonitoring can obtain basic, financial or other information about NPOs from international counterparts. Such requests are made on the basis of MoUs, or on the principle of reciprocity (art.5(15) PD808). The GPO, the MoJ and Rosfinmonitoring are the focal points for responding to international requests depending on the request (i.e. mutual legal assistance, foreign justice counterparts, or foreign FIUs requests).

Weighting and Conclusion

Minor deficiencies relate to the lack of granularity of risk classification and to the fact that. neither the TF NRA nor the NPO SRA include a reference to periodically reassess the risks faced by the NPO sector

Recommendation 8 is rated largely compliant.

Recommendation 9 – Financial institution secrecy laws

In its last MER, the Russia was rated compliant with these requirements.

Criterion 9.1

Access to information by competent authorities

FIs are obliged to keep confidential the information on clients and transactions (Law 395, Art.26; Law 39, Art. 8.6 (1); CC, arts 857 (1) and 946). FIs would not breach secrecy laws if they provide information and documentation to the competent authorities in respect of transactions and for the purposes and in the procedure envisaged in the Law (L115, Art.7(8); Law 395, Art.26; Law 39, Art 8.6 (4); CC, Articles 857 (2) and 946). Law enforcement entities can also obtain information from CIs on accounts and deposits of natural and legal persons (Law 395, Art.26). The BoR holds the appropriate legal authority to override financial secrecy provisions (article 76.7 of Federal Law No. 86-FZ; Law 86, Art.57; Instructions on BR 147, Art.2.5.3; BR 151, paragraph 2.5.3). Roscomnadzor is also entrusted with the power to request and obtain the information required for taking decisions on the issues under its remit (Government Decision No. 228, Art.6.1).

Sharing of information between competent authorities

All federal and local governmental bodies shall provide Rosfinmonitoring information and documents required for the performance of its functions free of charge, for instance by providing automated access to databases (Art. 9, para 1, L115). There are also a number of national mechanisms established in order to share information between competent authorities at an operational level (e.g. Joint-Order No 207 on information exchange between Rosfinmonitoring and LEAs specifically on AML/CFT matters; Joint-Order 50-1, on information between the BoR, Rosfinmonitoring and LEAs regarding the detection and suppression of illegal financial operation of CIs and their clients; see more generally R.2). Information sharing takes place also at the international level (see R.40). No impediments are placed by financial secrecy laws.

Sharing of information between FIs

Financial institutions legislation does not place any secrecy obligations that would hinder the sharing of information between financial institutions for the purposes of R.13, 16 or 17. Personal data may be shared without individual consent, for the purpose of attaining the objectives envisaged by an international agreement of Russia or a law, for the realisation and execution of the functions, powers and duties vested in FIs (article 6, paragraph 1, sub-paragraph 2 of Federal Law No. 152). Information can be shared cross-border in accordance with the law to foreign countries that are party to the Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data and also of the other foreign states that ensure adequate protection in respect of the rights of personal data (Article 11, Federal Law No.152).

Weighting and Conclusion

All criteria are met.

Recommendation 9 is rated compliant.

Recommendation 10 – Customer due diligence

In the last MER, Russia was rated partially compliant with these requirements. The deficiencies were related to the: (i) lack a specific prohibition on maintaining existing accounts in fictitious names, (ii) lack of requirements to conduct CDD where there is a suspicion of ML/TF; for dealing with doubts about veracity of previously obtained customer identification data; to the timing of verification of identification and consequences of a failure to conduct CDD, for non-CIs, (iii) lack of clarity in respect of beneficial ownership requirements; in relation to ongoing due diligence; to establish nature and intended purpose of business relationship and regarding requirements related to SDD and EDD.

Criterion 10.1 – All FIs are prohibited from opening and maintaining a bank account for anonymous holders or in fictitious names (Art.7(1) and (5) L115).

Criterion 10.2 – FIs are required to conduct CDD measures when:

a) Establishing a business relation (art.7(1) L115; BR 499, paragraph 1.1; BR 444; paragraph 1.1; RFM 366, paragraph 8-14).

b) Conducting an occasional transaction regardless of threshold. While some exemptions to identification of a customer which is a natural person, the representative of the customer, beneficiary and BO are in place (Art.7.1.1 to Art.7.1.4), the thresholds are low (the highest is RUB 100 000 – around EUR 1 200 – i.e. usage of personified electronic payment means for the purchase of precious metals and stones, while the lowest is RUB 15 000 – around EUR 200 – i.e. for natural persons payments and insurance premiums) (art.7(1, 1.1-1.4) L115). These exemptions are not applicable if suspicion of ML/TF arises.

c) Carrying out occasional transactions that are wire transfers under R.16 (Art.10.1 -10.9 Law 161).

d) There is a suspicion of ML/TF, regardless of any exemption or threshold (Art.7.1; 1.1-1.4 L115).

e) There is doubt regarding the "credibility and accuracy" of previously obtained customer identification data (Art.7.1.3 AML/CFT Law).

Criterion 10.3 – FIs are required to identify their customers, either natural or legal persons (art.7(1)(1) L115; for CIs, see BRR No. 499, paragraphs 2.1 and respective annexes 1 and 2; for non-CIs, see BRR No. 444, paragraph 1.1; RFM 366[109], paragraph 9) by way of the provision of valid original documents or their certified copies (in this case, FIs must verify the original documents, BRR No. 499, paragraphs 3.1 and 3.2; BRR No. 444, paragraph 2.4). Reliability of documents must be confirmed in the course of customer identification by using a number of databases (i.e. USRLE), open access information (i.e. Single Interagency Electronic Interactions System) but also through FIs internal procedures (BRR No 499, paragraph 3.2.; BRR No. 444, paragraph 2.2.; RFM 366, paragraph 6).

Criterion 10.4 – The identification and verification of the customers' representative is required and the procedure conducted is the same as outlined in c.10.3. For natural persons, FIs should receive information confirming authority of the representative, which includes the name, date of issue, validity period, number of the document granting authorities to the customer representative (BR 444, Annex 1; BR 449, Annex 1; RFM 366, Annex I (15), Annex 2 (3)). It is also required to verify his/her authorisation to act on behalf of the customer who is a legal person or legal arrangement (article 7, paragraph 1, sub-paragraph 4 L115).

Criterion 10.5 – The definition of BO provided in article 3, paragraph 13, of the AML/CFT law[110] is in line with the FATF Glossary[111]. FIs must resort to reasonable and available measures in the existing circumstances to identify and verify the identity of the BO prior to establishing a business relation or conducting an occasional transaction (article 7(1)(2) L115) with a legal person, legal arrangement of if it suspects the customer is acting on behalf of somebody else. FIs are not obliged to identify BO at all times, notably if the identification or verification of identity proves to be a challenging enough effort for an FI to deem their application to be unreasonable or unavailable. FIs must cross-check a number of databases to confirm the reliability of the information regarding the BO (see c.10.3).

Criterion 10.6 – FIs are required to obtain information on the purpose and intended nature of the business relationship (art.7(1)(1.1) L115).

Criterion 10.7 – There are several obligations in place for FIs that taken together resemble on-going due diligence. These are re-assessment of purpose of economic

[109] RFM 366 applies to some FIs only (leasing companies, payment service providers, factoring companies; federal postal service operators).

[110] "Beneficial owner" for the purposes of this Federal Law means a natural person who directly or indirectly (through third persons) ultimately owns (has a predominant stake of over 25 per cent in the capital) a customer being a legal entity, or has the possibility to control the actions of the customer. The beneficial owner of the customer that is a natural person shall be deemed this person, except for the cases when there are grounds to consider that the beneficial owner is another person.

[111] The definition of "customer" encompasses legal arrangements. In addition, the natural person who ultimately owns a legal person or controls the customer will not be deemed the BO if there are grounds to consider that it could be a different person.

activity on a regular basis; financial standing of the customer and its business reputation; regular updating of CDD information (art.7(1)(1.1, 2 and 3).

a) FIs must scrutinize transactions undertaken throughout the course of a business relationship to ensure they are consistent with their knowledge of the customer, its business and risk profile and its source of funds (L115, article 7 (1) (1.1); BR 375, paragraph 5.2; BR 445, paragraph 5.5; GR667, paragraph 16-23).

b) Information collected under the CDD process must be kept up-to-date, relevant and accurate to all customers, including higher risk categories (article 7, paragraph 1, subparagraph 3 L115).

Criterion 10.8 – For legal persons and legal arrangements, FIs should take appropriate measures to understand the ownership, control structure and obtain information on the nature of customer's business (L115, Art. 7, paragraph 1, subparagraph 1.1, 2, 3; BR 499, para 1.6 and 2.1; BR 499, Annex 2, para 1.2, 1.3, 1.8, 2.1 – 2.9; BR 444, para 1.5 and 2.1; BR 444, para 1.2, 1.3, .8, 2.1- 2.7; RFM 366, paragraphs 8, 9, annex 2 – paragraphs 1.7, 2.4 and 2.6)).

Criterion 10.9 – For legal persons, FIs are required to identify the customer and verify its identity through the following information (article 7, paragraph 1, subparagraph 1, and paragraph 5.4 L115):

a) Name, form of incorporation and taxpayer identification number or code of foreign organization.

b) FIs are required to collect information and documentation regarding the bodies of a legal person, including the structure and personal composition of its management bodies (For CI see BR No. 499, annex 2, paragraph 2.4, by way of article 7, paragraph 5.4 of AML/CFT; for non-CIs, see BR 444, annex 2, paragraph 2.1; RFM366, paragraphs 8, 9, annex 2 – paragraphs 1.7 and 2.4), which is more limited than individuals holding a senior management position. There is no requirement to establish the powers that regulate and bind the legal person.

c) No requirement is established regarding the principal place of business, where different from the address of registration. There is nonetheless a requirement on FIs to record the residence address or the address of stay (BR 499, Annex 1, BR 444, Annex 1; RFM366, paragraphs 8, 9 and annex 1 and 2).

Regarding legal arrangements, FIs are required to identify the customer and verify its identity through the following information (article 7, paragraph 1, subparagraph 1 L115):

a) Name, registration number of the state of incorporation;

b) For non-CIs, there is no requirement to establish the powers that regulate and bind the legal arrangement. On senior management positions, FIs are required to collect information and documentation regarding the bodies of foreign structures without forming a legal person, including the structure and personal composition of its management bodies (BR No. 499, annex 2, paragraph 2.4, by way of article 7, paragraph 5.4 of AML/CFT; BR 444, annex 2, paragraph 2.1; RFM366, paragraphs 8, 9 and annex 2 – paragraphs 1.7 and

2.4), which is more limited than individuals holding a senior management position.

c) The place of exercising its principal activity.

Criterion 10.10 – For customers that are legal persons, the identity of the beneficial owners must be identified by adopting reasonable measures and not at all times and verification of identity encompasses an obligation for FIs to conduct a reliability check of documents received (see c.10.5) (article 7, paragraph 1, subparagraph 1 and paragraph 5.4 L115). This includes: a natural person who directly or indirectly (through third persons) owns at least 25% of the capital or has the possibility of controlling the actions of the customer; and, the case where there is doubt over who the BO is. When the determination of the natural person(s) is not possible, the executive body of the legal person may be deemed BO (art.7(1)(2) and art.7(5.4) L115). According to article 65.3 (3) of the CvC, a sole executive body is a director, director-general, chairman, etc. Both a natural person and a legal person may act as a sole executive body of a corporation, and Russian legislation does not clarify that FIs need to identify as BO the natural person holding the position of senior managing official.

Criterion 10.11 – The definition of "foreign structure without forming a legal entity" includes trusts and other types of legal arrangements. In relation to these types of arrangements, FIs are required to identify and verify the identity of the founders (settlors) and the trustee (trust manager), beneficiaries[112] and BO - Article 7, paragraph 1, subparagraph 2 and paragraph 5.4 of AML/CFT Law. Deficiencies in criterion 10.5 apply.

Criterion 10.12 – CDD measures applicable to customers and representatives, including the updating requirements, are also applicable to beneficiaries at the moment of the establishment of a business relationship. Although no specific requirements exist to verify the identity of the beneficiary at the time of the payout, the update of the identification process must occur when doubts arise regarding the credibility and accuracy of information received earlier, within seven working days following the day when such doubts occurred. If the beneficiary cannot be identified and verified before onboarding the customer because the beneficiary of a transaction could not be determined, such determination must occur within seven business (BR 499, paragraph 1.5, for CIs; BR 444, paragraph 1.4, for non-CIs). Payment of premiums up to the amount of RUB 15 000 (EUR 200) are exempted from the application of such measures except if ML/TF suspicion arises.

Criterion 10.13 – There is no specific reference to include beneficiaries of life insurance contracts as a relevant risk factor when determining whether EDD is required at the time of pay-out. Requirements mentioned in 10.12 and 10.17 apply.

Criterion 10.14 – FIs are mandatorily required to verify the identity of the customer and beneficial owner prior to the establishment of a business relation or conducting an occasional transaction (Article 7, paragraph 1, subparagraph 1; paragraph 5.4

[112] For the purposes of the AML/CFT Law, "beneficiary" means a person (both natural and legal) for whose benefit a customer is acting when conducting transactions in funds and other assets, *inter alia*, under a brokerage contract, agency contract, commission contract and fiduciary management contract.

L115 Law; BRR 499, paragraphs 2.1., 2.2., 3.1. and 3.2; BR444, paragraph 2.1, 2.2, 2.4; RFM366, paragraphs 6, 8, 9, 14, 29, 30 and 33).

Criterion 10.15 – Since neither a business relation is established nor is an occasional transaction conducted without verification of identity, this criterion in not applicable.

Criterion 10.16 – FIs are required to apply CDD measures to existing customers by way of updating previously obtained information (i.e. identification, purpose and character of business, financial standing and business reputation of customers, origin of funds and property of customer) depending on their risk profile (updating takes at least once a year; within seven business days if doubt arise on the credibility or accuracy of information) – Article 7, paragraph 1, subparagraphs 1.1 and 3; paragraph 5.4 L115; RFM 366, paragraph 26; BRR 499, paragraphs 1.6; BR 444, paragraph 1.5).

Criterion 10.17 – A general requirement exists that CDD measures may vary according with the level of risks (Article 7, paragraph 1, subparagraphs 1.1 and 3 of AML/CFT Law; BRR 375, paragraphs 4.1, 4.9.). FIs must also pay "high attention"[113] to the transactions of high risk customer[114] (Art. 18 of GR №667), which does not properly substantiate the difference between SDD, CDD and EDD in terms of the scope, depth and intensity of measures taken under each regime. Nevertheless, certain EDD measures are foreseen in BoR regulations (BR375, paragraph 5.2, for CIs and BR445, paragraphs 5.2, 5.3, for non-CIs).

Criterion 10.18 – SDD measures can only be applied regarding natural persons (see art. 3 L115 for definition). SDD is permitted in determined situations (see c. 1.8), unless a ML/TF suspicion arises (art. 7, paras 1.1, 1.2, 1.4, 1.4-2 and 1.11 L115). The conditions whereby SDD measures are applicable resemble objective characteristics of potentially low-risk relations and have been defined with due regard of the findings and conclusions of earlier risk assessments.

Criterion 10.19 – For the purposes of this criterion, Russian legislation does not encompass all the elements of CDD, only capturing identification and verification of identity. The system is also characterized by a mix between prohibition and entitlement to refuse to establish a business relation and an occasional transaction: "Entitlement" conveys the idea of "right to refuse" as opposed to "duty to refuse", as required. As such, CIs are prohibited to establish a business relationship if the customer or his/her representative fails to provide the information and documents necessary for identification (art.7, para 5 L115). No similar provision exists for occasional transactions. These deficiencies are partly mitigated by the fact that CIs are entitled to: (i) refuse to establish a business relation if they have an ML/TF suspicion (article 7, paragraph 5.2 L115); and, (ii) refuse to carry out a customer instruction to carry out an occasional transaction of a legal arrangement, if the required documents have not been submitted or on ML/TF concerns (art.7, para 11 L115). CIs are required to file an STR in both situations (art.7, paras 11, 13 and 13.1 L115). Non-CI are only covered by the requirements regarding occasional transactions (art.7, para 11 L115). Regarding BO, if determination is impossible due to lack of submission of information

[113] Increased attention means the adoption of enhanced measures of monitoring and control in relation to the customer and related transactions (GR 667, paragraphs 13-15; BR 375, chapter 4, for CIs; BR 445, chapter 4, for non-CIs; see also criterion 1.7).

[114] A high-risk customer is a customer who is assigned a high level of risk by the FI based on the implementation of the customer risk assessment program, which must foresee a number of factors that are taken into account in the process.

or documentation, then the entity also has the right, not the obligation, to refuse to conduct a transaction or enter into a business relation (art.7(1)(2) and art.7(5.2 and 5.4) L115; for CIs, see BRR No. 499, paras 1.2., 2.1, 2.2., 3.1 and 3.2.; for non-CIs, see BR444, para 1.1.1, para 1.5, subpara 1 and 2, paras 2.2, 2.3 and 2.4).

Criterion 10.20 – When FIs form a suspicion of ML or TF and reasonably believe that performing CDD measures will tip off the customer, there is no provision allowing the FI to elect not to pursue CDD and requiring it instead to file an STR.

Weighting and Conclusion

The Russian legal system broadly complies with Recommendation 10 and the above stated deficiencies are minor. Notably, FIs have a right, not an obligation, to refuse the establishment of a business relation or carrying out an occasional transaction when unable to comply with CDD measures. EDD enforceable regime could be clearer and more developed. Also, when forming a suspicion of ML or TF that could reasonably lead FIs to believe that performing CDD measures would tip off the customer, there is no provision allowing the FI to elect not to pursue CDD and filing an STR instead.

Recommendation 10 is rated largely compliant.

Recommendation 11 – Record keeping

In its last MER, Russia was rated largely compliant with these requirements. Deficiencies were related with account files and business correspondence not having to be kept for a minimum of five years from the termination of the account or the business relationship. In addition, timely access was not required by law or regulation. R.11 sets out that the principle that the requirement for FIs to maintain certain records should be established in law. The AML/CFT Law provides a range of measures that embody the referred principle.

Criterion 11.1 – There is an extensive list of transactions FIs are required to keep records of for a period of not less than five years, after its execution – art.7 (1), sub-paragraph (4); art. 7 (2) (3) (4) L115. There is, however, no obligation on FIs to maintain the necessary records on all transactions.

Criterion 11.2 – FIs are required to keep all records obtained through CDD measures for at least five years, beginning from the day of termination of the business relationship or after the date of the occasional transaction (art.7(1)(1) and (1.1); art.7(4) L115), accounting files (Law 402, Art.29(2)), business correspondence (GR No. 667, paragraph 33(g)), analysis of unusual or suspicious transactions (joint reading of GR No. 667(21), (22), (33)(c)), and article 7(4) L115).

Criterion 11.3 – FIs are required to obtain a range of information regarding individual transactions which permits reconstruction, namely their type and purpose; their date and amount; information on the identity of natural or legal persons requesting the transaction; information relating the identity of the representative conducting the transaction on behalf of the customer; information relating to the beneficiary (art.7, para 1, subpara 4 L115). This information can be made available to all State bodies in the context of a legal proceeding (art.857, para 2 CC. See also, art 7, para 1, subpara 5 L115; art. 26 of Banking Law).

Criterion 11.4 **–** FIs are required to provide CDD information and information on transaction records and beneficial ownership to Rosfinmonitoring immediately or from one business day to no later than 5 business days after completion of transaction (Art.7(1)(5)(10) L115; GR No. 209, paragraph 3, indents a), b), f) and g), BR 600, Para 1 and Annex, paragraph 9). CIs have an additional requirement to provide transaction records to a number of competent authorities (article 26, paragraphs 2, 4, 5 and 6 of the Banking Law). Securities market participants can provide information to a wide array of institutions, namely other public agencies with investigative duties and courts (L39, article 8.6 (4)). BoR also has the right to obtain all information necessary to conduct inspections (L86, article 73, for CIs, article 76.5, for non-CIs; and art. 2.5.3 BR147; see c.27.3). LEAs can obtain information from FIs (see c.30.1). Legal provisions are in place regarding the provision of CDD information to Rosfinmonitoring (article 7, paragraph 1, subparagraph 5 of AML/CFT Law; BR 600, Annex, paragraph 9, for CIs. GR 209, for non-CIs).

Weighting and Conclusion

There is no requirement to maintain records on all transactions, despite the extensive list of legally defined transactions subject to record-keeping obligation. Non-CIs are not obliged to disclose CDD information and transaction records to a wide array of domestic competent authorities.

Recommendation 11 is rated largely compliant.

Recommendation 12 – Politically exposed persons

In its last MER, Russia was rated partially compliant with these requirements. Deficiencies were related to the definition of PEPs, which did not extend to those who have been entrusted with public functions; lack of requirement to obtain approval from senior management for existing customers found to be PEPs; a lack of clarity relating to establishing source of wealth and no enhanced on-going due diligence and beneficial ownership obligations.

Criterion 12.1 **–** When considering whether a customer falls within the category of foreign PEP, the determination should be made in accordance with the FATF Recommendations (Art.7.3, para 4 L115). However, it cannot be considered as a substantial national implementing measure and doubts arise whether this technique introduces clarity and certainty in the Russian legal system.

In relation to foreign PEPs, FIs are required to take additional measures besides CDD. In this context, FIs are required to:

a) Put in place risk management systems to determine, by taking reasonable and possible measures, whether a new or existing customer is a foreign public official (article 7.3, paragraph 1, subparagraph 1 L115; Paragraph 3.2, subparagraphs 1 and 6 of BR No. 375 for CI; paragraph 3.2., subparagraphs 1 and 5 of BR No. 445 and GR 667, paragraph 11, for non-CI). All FIs are required to determine whether any foreign PEP would be the beneficial owner of a customer (BR 375, paragraph 4.4; BR445, paragraph 4.2 and Annex 2; RFM 57 – Methodological Recommendation – part III; RFM 59 – Methodological Recommendation – part II).

b) Obtain head or deputy-head of the FI approval before the establishing business relationships with foreign public officials (article 7.3, paragraph 1, subparagraph 2 L115). This legal provision does not encompass existing customers.

c) Take reasonable and possible measures to identify the source of funds or other assets (i.e. wealth) of foreign public officials (art.7.3, paragraph 1, subparagraph 3 L115). If a foreign public official is identified as beneficial owner, this conduct is applicable to all FIs.

d) To pay special attention (see deficiencies in c.10.17) to transactions conducted in the course of the business relation by foreign public officials (art.7.3, para 1, subpara 5 L115). FIs are also entrusted with the duty to update on a regular basis the information available of the source of funds and other assets (art. 7.3, para 4, subpara 3 L115).

The requirements established in paragraph 1 of the referred article 7.3 are not to be applied by CIs, unless there is a suspicion of ML/TF, when (i) conducting operations up to the amount of RUB 40 000 (approximately EUR 550) or equivalent amount in foreign currency, if related to the purchase or sale of foreign currency in cash by natural persons, and (ii) conducting transactions up to the amount of RUB 15 000 (approximately EUR 200) or equivalent amount in foreign currency which are related to with transfers of monetary funds on the instructions of natural persons without opening a bank account.

Criterion 12.2 **–** FIs must take reasonable and possible measures to determine whether a new or existing customer is a domestic PEP or an official of public international organisations (art. 7.3, paragraph 1, subparagraph 1 L115; Paragraph 3.2, subparagraphs 1 and 6 of BR No. 375 for CI; paragraph 3.2., subparagraphs 1 and 5 of BR No. 445 and paragraph 11 oh GR 667 for non-CIs). Different from foreign PEPs, there is no equivalent reference to using the FATF Recommendations to determine whether a person falls into the category of domestic PEPs. Domestic PEPs would be considered persons entrusted with governmental functions of Russia; members of the board of directors of the BoR; federal state civil service functions to which people are appointed and dismissed by the President or its Government functions in the Central Bank and state corporations and other organisations established by Russian law that are included in the lists of functions determined by the President, and officials of international organisations. Judicial and military officials are covered because they are appointed by the President. Regarding senior politicians and important political party officials, since they are not appointed by the President, are only considered as domestic PEPs insofar as they hold any governmental (executive) or Federal Assembly (legislative) positions. In consistency with the Glossary, PEPs should be as such considered by focusing on the prominence of function rather than by presidential power of appointment. A consolidated list is enacted and frequently updated by the President– see Presidential Decree No. 32.

Measures and legislation referred in c.12.1(a) apply: in cases where a transaction is identified as high risk, the measures criterion 12.1 (b) to (d) must be applied (Art.7.3, paragraph 3). This legal requirement is not totally aligned with the present criterion, since it focuses on the transaction being qualified as high risk rather than on the business relationship with the customer. However, regulations clarify that FIs customer risk assessment must take into account whether the customer is considered

a domestic public official (BR 375, paragraphs 4.3 and 4.4, for CIs; BR 445, paragraph 4.2 and Annex 2, for non-CIs). Deficiencies of criterion 12.1 apply.

Criterion 12.3 **–** EDD measures apply to immediate family members of foreign and domestic public officials. Transactions on behalf of these people is also covered. (art. 7.3, para11, subpara 5, and para3 L115). However, EDD requirements do not apply to close associates of foreign and domestic public officials. Deficiencies in c.12.1 and 12.2 apply.

Criterion 12.4 **–** CDD measures applicable to customers and its representatives, including the updating requirements, are also applicable to beneficiaries at the moment of the establishment of a business relation. As such, FIs must determine whether the beneficiaries are PEPs, conduct enhanced scrutiny on the business relationship with the policyholder and consider making a suspicious transaction report, should higher risks be identified. If the beneficiary cannot be identified by FIs before onboarding the customer due to the absence of determination of who the beneficiary is in operations scheduled by the customer, such process must occur within a time period not exceeding seven business days from the date the operation is carried out (BR 499, paragraph 1.5, for CIs; BR 444, paragraph 1.4, for non-CIs). However, there is no provision requiring FIs to assess whether the beneficial owner of the beneficiary is a PEP. There are also no specific requirements for FIs to inform senior management before the pay-out of the policy proceeds.

Weighting and Conclusion

Regarding foreign PEPs, Russia as chosen to make a direct reference to the FATF Recommendation when assessing whether or not a person can be as such considered. As for national PEPs, there is a national list, regularly updated by Presidential Decree. However, eligibility of persons to be as such considered mostly rely on having been appointed by the President rather than on the prominence of functions, which is found to be rather formalistic thus providing little flexibility for reporting entities to make their own appraisals. EDD measures do not apply to close associates of any kind of PEP. There is no provision requiring FIs to assess whether the beneficial owner of the beneficiary of life insurance policies is a PEP. There are also no specific requirements for FIs to inform senior management before the pay-out of the insurance policy proceeds.

Recommendation 12 is rated partially compliant.

Recommendation 13 – Correspondent banking

In the last MER, Russia was rated partially compliant with these requirements. Deficiencies were related to there being no specific requirement to: (i) understand the nature of respondent's business and determine quality of supervision; (ii) make a judgement on the effectiveness of respondent AML/CFT system, and (iii) to ascertain if respondent has been subject of ML/TF investigation. The new FATF Recommendation adds a specific requirement concerning the prohibition of correspondent relationships with shell banks.

Criterion 13.1 **–** Credit institutions must implement a specific identification procedure regarding the establishment of cross-border correspondent banking relationships with foreign banks and other credit institutions that are not foreign

banks (BRR No. 375). There are no binding provisions neither on other similar relationships nor to non-CIs.

a) When establishing cross-border correspondent banking relationships, credit institutions are required to gather sufficient information about the respondent institution to understand the nature of the respondent's business, determine the reputation of the institution, and other information (paragraph 2.5 BRR 499). However, there is no requirement on the necessity of understanding the quality of supervision.

b) Required to collect information on the AML/CFT measures applied by respondents. However, there is no requirement to assess the respondent institution's AML/CFT controls;

c) Prior the establishment of CB relationships, obtain approval of the chief executive officer or an officer authorized by the chief executive officer.

d) No requirement exists regarding the understanding of the respective AML/CFT responsibilities of each institution in the context of the CB relationship.

Criterion 13.2 **–** The legal framework does not foresee the setting up of payable-through accounts.

Criterion 13.3 **–** CIs are prohibited from establishing and maintaining correspondent banking relationships with non-resident banks that do not display permanently operating managing bodies in the countries or jurisdictions where they are registered (art.7, paragraph L115). They are also required to take measures to prevent the establishment of business relations with non-resident banks that allow such entities to operate their accounts (art.7(5.1) L115). The requirements that must be met to establish a bank in Russia, as set out by the Banking Law, effectively prohibit shell banks from operating in the country.

Weighting and Conclusion

Russia complies with Recommendation 13 to a large extent. Noted deficiencies are related to the fact that financial institutions are neither required to understand the quality of supervision of the respondent, to assess the respondent institution's AML/CFT controls nor the AML/CFT responsibilities of each institution. Also, legal requirements only apply to CIs.

Recommendation 13 is rated largely compliant.

Recommendation 14 – Money or value transfer services

In the last MER, Russia was rated non-compliant with these requirements. Deficiencies related to the lack of effectiveness in ensuring compliance; insufficient attention was devoted to the existence of and risks presented by illegal alternative remittance systems; payment acceptance service providers were not covered by supervisory regime until November 2007 (effectiveness could not be determined); implementation of R.5-8, 10, 13-15, 22 and 23 in the MVTS suffered from the same deficiencies as those that applied to banks; and Roscomnadzor lacked effective sanctioning powers.

Criterion 14.1 – MVTS operators are required to obtain a banking licence pursuant to Law No.395, or in the case of postal communication operators under Law No 126. Other operators engaged in payments' acceptance must be registered with Rosfinmonitoring (GR No.58) including payment agents (Art.4, paragraph 5 of Law No. 103).

Criterion 14.2 – Illegal money transfer systems in the Russia – operating without a licence from the BoR and Roscomnadzor – is a criminal offence under with proportionate and dissuasive sanctions (Article 172 of the CC) - (i) a fine of an amount ranging RUB 100 000 to RUB 300 000 (from around EUR 1 300 to EUR 4 000) or in the amount of the salary or any other income for a period from one to two years; (ii) with compulsory labour for a period of up to four years; (iii) deprivation of liberty for a period of up to four years, with a fine in the amount of up to RUB 80 000 (around EUR 1 000) or in the amount of the wage or salary, any other income for a period of up to six months, or without any fine. MVTS operating without a licence are also subject to deprivation of the whole amount obtained as well as a fine at double of the said amount. The BoR is also entitled to bring a liquidation action against such a legal person (article 13, paragraph 8, of Banking Law). Natural persons carrying out banking operations illegally are liable to civil, administrative or criminal proceedings (article 13, paragraph 9, of Banking Law). Preliminary investigation of criminal cases is carried out by police.

Criterion 14.3 – Credit institutions (bank and non-bank), telecommunication operators, the federal postal service and operators engaged in payments' acceptance, including payment agents, are subject to AML/CFT Law and are supervised regarding these requirements by relevant competent authorities (art.7(9) L115), namely BoR, Roscomnadzor, and Rosfinmonitoring.

Criterion 14.4 – MVTS providers are required to maintain a current list of agents with the addresses of all the places where operations are performed. The latter are obliged to provide the former with information necessary to be included in the list. MVTS providers are only required to provide this list to FTS on demand (article 14, paragraph 19 of Law No. 161-FZ; article 4, paragraph 3 of Law No. 103-FZ) and not to competent authorities in other countries in which the MVTS provider and its agents operate.

Criterion 14.5 – MVTS providers are obliged to monitor their agents compliance with the AML/CFT Law requirements (Article 14, paragraphs 20 and 24 of Law No. 161-FZ). There is no provision requiring MVTS providers to include their agents in their AML/CFT programmes.

Weighting and Conclusion

Minor deficiencies exist as there is no obligation for MVTS providers to provide a list of its agents other than to Russian competent authorities. There is also no requirements for MVTS providers to include their agents in the AML/CFT programme.

Recommendation 14 is rated largely compliant.

Recommendation 15 – New technologies

In the last MER, Russia was rated partially compliant with these requirements. Deficiencies were related to the requirements for new technologies being limited to internet banking and no requirements were in place for non-face-to-face transactions except for CIs.

Criterion 15.1 – Requirements for risk assessment provided for all obliged entities under the AML/CFT Law are applicable to all transactions and types of services (article 7, paragraph 2, L115), including to new technologies. ML/TF risks associated with the development of new products are also assessed by working groups and in the framework of other consultative mechanism. The Advisory Council under the Interagency Commission on AML/CFT has decided that its members shall provide information to Rosfinmonitoring regarding the development of work related to the risk reduction of the opening of remote accounts for legal entities as well as the use of digital signature for identification purposes. Pursuant to GR 1104, some FIs are part of a pilot project related to the use of electronic documents for registration of legal entities and individual entrepreneurs and to open their accounts using a special secure automated system in a pre-defined period of time (two years, extendable). The goals of the experiment are (i) development of the automated system, (ii) identification of technical possibilities of the automated system and (iii) identification of the financial effectiveness of the system and the ease of usability of the mentioned technology for legal entities and individual entrepreneurs. The BoR has also established the Interagency Expert Council for implementing innovative financial services and technologies (composed by both Chambers of Parliament, relevant Ministries and Rosfinmonitoring (see BR Order No. OD-849). This Expert Council considers issues pertaining to the use of innovative products, services and technologies in the financial sector. Modelling of the processes related to this use are conducted through assessment of risks, including ML/TF risks. As exemplified by Russian authorities, FIs analyse new products, business practices and the use of new technologies in new and existing products in order to identify and assess ML/TF risks. Rosfinmonitoring is entrusted with task to update the national evaluation of ML/TF risks, in co-operation with federal executive governmental bodies, other state bodies and organisations, the Central Bank and with the participation of FIs (see PD No. 808, paragraph 5, subparagraph 16.1). The 2018 ML NRA includes two sections on the risk of abusing electronic means of payment and virtual currencies and the TF NRA contains a section on the risks of raising funds for the purpose of financing of terrorism via Internet.

The assessment team considers that Russia demonstrates that it "identifies and assesses the ML/TF risks" that arise from new technologies. Also, the general clause of the AML/CFT Law is considered to encompass the obligation as stated in this criterion, despite the non-existence of a specific obligation for FIs to assess risks associated with the development of new products and new business practices and the use of new or developing technologies to both new and pre-existing products.

Criterion 15.2 – FIs are required to develop ML/TF risk management programs in order to implement their AML/CFT internal controls, meaning risk assessment and risk mitigation run in tandem (See BRR No. 375 and BRR No. 445 – both in chapters 4, specially paragraphs 4.1; GR No. 667, specially paragraphs 13-16). These are conducted prior to the launch of new products, practices and technologies and are

applicable to them concerning risk management and mitigation. Mitigating requirements are also set out in the recommendations of a number of supervisory authorities.

Weighting and Conclusion

All criteria are met.

Recommendation 15 is rated compliant.

Recommendation 16 – Wire transfers

In the last MER, the Russia was rated partially compliant with these. Deficiencies pertaining to these requirements related to the fact that full originator information was not always required; no requirements were in place for beneficiary FIs to adopt a risk-based procedure for wire transfers, and incoming transfers were not covered at all; the requirement to refuse transactions without full originator information could not be implemented; batch transfers were not specifically mentioned in law; shortcomings were identified under other Recommendations, namely regarding sanctions and monitoring and supervision; and, effectiveness of the then-new system could not be measured. Screening for TFS related to terrorism and terrorist financing is not explicitly covered in R.16.

The AML/CFT Law establishes two types of operations for the purpose of Recommendation 16: funds transfer from a bank account and funds transfer without opening a bank account.

Criterion 16.1 –

a) For cross-border wire transfers above RUB 15 000 (around EUR 200), FIs are obliged to ensure that they are accompanied by the following information regarding the originator (see Article 7.2, paragraphs 1, 1.1, 7 and 12 L115): (i) first name, surname and patronymic (for natural persons) or denomination (for legal person); (ii) bank account number (for both natural and legal persons) and a unique transaction reference number (not required for funds transfer from a bank account); (iii) address of residence (for natural persons) and tax identification number (for both natural and legal persons).

   While the law requires credit institutions to ensure available and complete information for compliance with this information, the assessment team considers that the wording is enough to capture the sense of "accuracy", as required by the standard. In fact, the identification and verification process is conducted prior to the transfer of funds (via a bank account or not) thus allowing for confirmation of adequacy (see c.10.2)

b) There is no legal provision requiring FIs to ensure that cross-border wire transfers are always accompanied by information on the name of the beneficiary or on the beneficiary account number or a unique transaction reference.

Criterion 16.2 – The AML/CFT Law does not specifically foresee "batch files", although it allows "package transfers", i.e. transfers from one sender combined into a batch file for transfer to recipients. The rules governing individual wire transfers,

namely Art.7.2 of the AML/CFT Law, equally apply to package transfers and deficiencies in c.16.1 apply.

Criterion 16.3 – For cross-border wire transfers below the threshold defined in Russian Law – RUB 15 000 (around EUR 200) – the requirements set out above (criterion 16.1) do not apply (article 7.2. (12) L115).

Criterion 16.4 – Whenever there is an AML/CFT suspicion, pursuant to the application of internal control policies and procedures, FIs are required to obtain additional information and documentation regarding a certain customer or transaction (BRR No. 375, paragraph 5.2.; BRR No. 445, paragraph 5.3; GR No. 667, paragraphs 23 and 24).

Criterion 16.5 – The AML/CFT Law does not distinguish between domestic and cross-border wire transfers for the purpose of originator information that must accompany transfer from ordering institutions, thus deficiencies in relation to cross-border wire transfers apply equally to domestic ones (see c. 16.3).

Criterion 16.6 – The same measures and, thus, deficiencies apply as indicated in 16.5. There are no requirements to provide information on beneficiaries to beneficiary financial institutions. FIs must provide information on transactions to Rosfinmonitoring on demand within three working days (GR No. 209, paragraphs 4, indents a) and b)) or by their own initiative if there is suspicion of ML/TF (in this case within one business day counting from the day in which the suspicion arose) – article 7, paragraph 5 and article 7.2 of AML/CFT Law. LEAs can promptly access information related to accounts, deposits and transfers (article 26 of Banking Law).

Criterion 16.7 – The ordering FI is required to retain all originator information collected for at least five years (art.7, paras 1 and 4; article 7.2, paras 1 and 7 L115). Regarding beneficiary information, there is no specific provision similar to that of the originator. However, article 7, paragraph 1 AML/CFT Law, obliges FIs to collect beneficiary information as required by R. 16, except for the beneficiary account number or, in the absence of an account, a unique transaction reference number.

Criterion 16.8 – Ordering FIs are required not to execute wire transfers that do not comply with the requirements set out above in criteria 16.1 to 16.7 only regarding originator information (article 7.2, paragraphs 2 and 8 L115).

Criterion 16.9 – Intermediary FIs are required to ensure that all originator information accompanying a wire transfer is kept with the transfer (article 7.2, paragraphs 4 and 9 L115). Deficiencies on lack of beneficiary information accompanying the wire transfer apply (c.16.1).

Criterion 16.10 – The AML/CFT Law does not make any distinctions regarding the obligation imposed on intermediary FIs to keep records of information received. As such, record-keeping obligations apply to all transfers, including the ones where technical limitations prevent the necessary information from accompanying the transfer, regardless of deficiencies identified above on the obligations regarding information accompanying the wire transfer (c.16.1 b) and information collection (c.16.7).

Criterion 16.11 – Intermediary FIs are obliged to ensure inalterability – which means that the information received by the beneficiary must be of the same content as received from the originator – of the information contained in received documents

(article 7.2, paragraphs 4 and 9 L115). This obligation does not amount to the proper check of existence of the required originator and beneficiary information to accompany the wire transfer. Notwithstanding, intermediary FIs that conduct funds transfer without opening a bank account are bound to check if the required information under the AML/CFT Law (see c16.1) accompanies the wire transfer. They must forward data on the transaction to the authorized body if the referred information is missing (art. 7.2, paragraph 11 L115). Deficiencies of c.16.1 apply.

Criterion 16.12 **–** Intermediary FIs conducting funds transfers without opening of a bank account are obliged to check if the required information under the AML/CFT Law (see c.16.1) accompanies the wire transfer. They must forward data on a transaction to the authorized body if: (i) the referred information is missing and (ii) there is ML/TF suspicion (article 7.2, paragraph 11 L115). Intermediary FIs are required to reject performing a wire transfer if the referred information is not received (article 7.2, paragraph 8 L115). The general duty of implementation of internal control AML/CFT policies and procedures applies to both to funds transfers without opening of a bank account and funds transfers from a bank account.

However, this does not amount to a specific risk-based policy and procedure for determining when to execute, reject or suspend a wire transfer that lacks the required information on the originator and the beneficiary. On the contrary, it amounts to a rigid and prescriptive set of rules that determines a legally defined outcome as follow-up action. Deficiencies of c.16.1 apply.

Criterion 16.13 **–** Beneficiary FIs are required to detect whether all required information on the originator accompanies wire transfers (see article 7.2, paragraphs 5 and 10). There are no requirements to detect whether beneficiary information is missing.

Criterion 16.14 **–** Beneficiary FIs must identify and verify the identity of the beneficiary of the wire transfer through general provisions of the AML/CFT Law (art.7, paragraph 1 L115), regardless of the type of transfer and to keep the information in accordance with R.11 (article 7, paragraph 4 L115).

Criterion 16.15 **–** The general duty of implementation of internal control AML/CFT policies and procedures applies. Beneficiaries FIs are not required to have a specific AML/CFT risk-based policy and procedure for determining when to execute, reject or suspend a wire transfer that lacks the required information on the originator and the beneficiary.

Criterion 16.16 **–** The MVTS under the AML/CFT legislation, including payment agents, are required to comply with the wire transfer requirements as described above. Deficiencies identified throughout R. 16 apply.

Criterion 16.17 **–** There are no specific requirements for a MVTS provider controlling both the ordering and beneficiary side of a wire transfer to take into account all the information from both sides in order to assess whether to file an STR or not. Nonetheless, regarding funds transfer without opening of a bank account, article 7.2, paragraph 11, AML/CFT Law requires that if a certain wire transfer (i) is not accompanied by the information referred in criterion 16.1 or (ii) raises ML/TF suspicion, FIs must forward data on the transfer to Rosfinmonitoring. This implies that FIs must take into account all information at their disposal (from both sides of the wire transfer). Concerning funds transfer from a bank account, paragraph 6 of

article 7.2 restricts the scope to the "credit institution where the recipient's bank account is opened". This implies that while making a decision to file an STR a MVTS provider controlling both the ordering and beneficiary side of a wire transfer is only obliged to take into consideration the information held by one of the sides of the wire transfer (the beneficiary's side).

In both cases, deficiencies in c.16.1 apply. The AML/CFT Law applies to branches and representative offices, as well as subsidiaries of institutions carrying out transactions with monetary funds or other assets located outside Russia, if this does not contradict the legislation of the country of their location (article 2). However, this does not amount to an explicit obligation to file an STR in any country affected by the suspicious wire transfer.

Criterion 16.18 – FIs shall impose measures for freezing (blocking) wire transfers immediately and, in any case, not later than one day from the publication of the listing (article 7, paragraph 6 L115).

Weighting and Conclusion

There are no requirements on ordering and intermediary FIs to ensure that information on the beneficiary accompanies cross-border wire transfers, which ultimately affects beneficiary FIs. For cross-border wire transfers under a certain threshold, the information required by the Standard is not available. For a MVTS provider controlling both the ordering and beneficiary side of a wire transfer, only for funds transfers without opening of a bank account is there an implicit obligation to take into account the information from both sides in order to assess whether to file an STR or not. Applicability of this obligation to their branches, representative offices and subsidiaries is also an issue.

Recommendation 16 is rated partially compliant.

Recommendation 17 – Reliance on third parties

In the last MER, Russia did not allow FIs to rely on intermediaries or third parties. Therefore, these requirements were deemed not applicable. Legal provisions regulating such activity now exist.

Criterion 17.1 FIs can rely on third parties to perform elements (a)-(c) of the CDD measures set out in R.10 only for natural persons and in three circumstances: 1) CIs and federal post when conducting money remittance without opening a bank account and electronic payments (article 7, paragraph 1.5 L115); 2) CIs and microfinance companies granting of consumer credit (article 7, paragraph 1.5-2 L115); 3) Professional participants in the securities market, investment funds management companies, unit investment funds and managing company of non-state pension funds when carrying out activities on non-state pension provision (article 7, paragraph 1.5-1 L115). In these cases, the referred entities:

a) Are required to immediately or no later than three working days obtain all information on identification (article 7, paragraph 1.9 L115);

b) Are not legally obliged to satisfy themselves on the availability of relevant CDD documents from the third party, upon request, without delay. However, third parties have a legal obligation to transfer the information received

during the CDD process in its entirety to the FI, immediately but no later than three working days from the date of receiving such data (L115, article 7 (paragraph 1.9);

c) All entities that can be entrusted with carrying out elements (a)-(c) of the CDD measures set out in R.10 are under the remit of AML/CFT Law (paragraph 9 of article 7) and, thus, are regulated and supervised. There is, however, no measure for the reliant FI to satisfy itself that third parties have measures in place to comply with CDD and record-keeping obligations.

Criterion 17.2 – The AML/CFT Law does not allow FIs to rely on third parties based outside of Russia to perform CDD measures. All third parties need to be supervised by a Russian competent authority (article 7 (9) L115).

Criterion 17.3 – The AML/CFT Law only allows FIs to rely on third parties that are not part of the same financial group to perform CDD measures (article 7, (1.5) (1.5-1) (1.5-2) L115).

Weighting and Conclusion

Recommendation 17 is broadly not applicable. However, in the situations where FIs are able to rely on third parties there is no measure for the reliant FIs to satisfy themselves that third parties have measures in place in order to be able to adequately comply with CDD and record-keeping obligations.

Recommendation 17 is rated largely compliant.

Recommendation 18 – Internal controls and foreign branches and subsidiaries

In the last MER, Russia was rated partially compliant with these requirements. Deficiencies were related to the internal control procedures governing terrorism financing lacked a comprehensive treatment of CFT, focusing almost exclusively on a "list-based" approach; training programmes of FIs focused too heavily on legal requirements under the AML/CFT Law, rather than on practical case studies of ML and TF, diminishing the effectiveness of the programmes; screening programmes were not broad enough, did not cover all personnel and did not focus on country specific risks, diminishing the effectiveness of the programmes; Russia Post could not demonstrate effective implementation of internal control programmes at all branches.

Criterion 18.1 – FIs must elaborate internal control rules for AML/CFT compliance (Article 7 and article 3, paragraph 8, paragraph 2 L115,). Internal control rules need to take account of the size, nature and complexity of the business.

a) The internal control rules on AML/CFT foresee the setting up of an AML/CFT system (BR No. 375, paragraph 1.6, for CIs; BR No. 445, paragraph 1.7, for non-CIs). The persons assigned with the function of implementing AML/CFT controls shall be a member of the executive body (see BR No. 375, paragraph 1.8, for CIs; see BR No. 445, paragraph 1.9, for non-CIs).

b) FIs special officials (people responsible for implementation of internal control rules) are required to comply with certain requirements, namely higher education qualifications or relevant work experience (see GR 492; for

CIs, BR No. 1486; for non-CIs, BR 3470).These requirements apply to all employees of the structural unit for AML/CFT (BR1486, paragraph 1; BR3470, paragraph 2). However, there is no screening procedure to ensure high standards for other employees.

c) FIs are required to provide on-going AML/CFT training to special officials and relevant staff (see BR No. 1485 for CIs; for CIs, except professional securities market participants, see RFM No. 203; BR No. 3471 for non-CIs);

d) An independent program for verifying the implementation of internal control systems is required (for CIs see BR 375, paragraphs 1.8 and 1.9; for non-CIs see BR 445, paragraph 1.9 and 1.10; GR 667, paragraphs 31 and 32).

Criterion 18.2 – FIs that are part of a financial group are required to implement group-wide programmes that are applicable to all branches and majority-owned subsidiaries or to accede to internal control rules as developed by their parent company (article 7, paragraph 2.1, sub-paragraphs 2 and 3 L115). These include the measures set out in c. 18.1.

a) Regarding policies and procedures for sharing information and documentation on CDD identification of customer, customer's representative, beneficiary and beneficial owner, updating such information, the conditions upon which FIs that are members of the same banking group or bank holding group[115] are authorized to exchange information within the group are overly restrictive. For example, these include the customer's written consent to exchange and use the information about him/her by other FIs of the same group (article 7, paragraph 1.5-4 L115). While the FATF Standards provide for the possibility for certain restrictions to be introduced based on the sensitivity of information and its relevance for AML/CFT risk management, the conditions in Russian law could be at odds with relevance for AML/CFT risk management. In addition, there is no margin of discretion left to FIs to make a determination on the sensitivity of CDD information gathered.

b) There are no provisions permitting (with or without restrictions) the exchange of information on customer information unrelated to CDD as well as account and transaction information for AML/CFT purposes, including the information and analysis of transactions or activities which appear unusual. Moreover, FIs that are members of a banking group or a bank holding company are prohibited from sharing the referred information and documents with other members of the same banking group or the same bank holding group if these are registered outside Russia (article 7, paragraph 1.5-5 L115).

c) There are no provisions to establish adequate safeguards on the confidentiality and use of information exchanged, apart from the Law 149, articles 2 (7) and 3 (7) – regarding the needed personal consent to share confidential information, and Law 152, articles 5-13 – on principles and conditions to process personal data.

[115] For the purpose of the AML/CFT Law, "Banking group" and "Bank holding group" are understood as defined in the Banking Law, which does not restrict the concept to banking institutions, encompassing all FIs.

Criterion 18.3 – The AML/CFT Law is applicable to branches, representative offices and subsidiaries (article 2, paragraph 2), thus making its requirements a minimum standard. Article 7, paragraph 5.3 of AML/CFT Law requires that if branches and subsidiaries of FIs are located in a state or territory that hinders its implementation or of other specific provisions, FIs must inform Rosfinmonitoring and also the body in charge of supervision of the relevant area of activity. FIs are not specifically required to apply additional measures to managed ML/TF risks in case the referred implementation is undermined.

Weighting and Conclusion

Financial groups are required to implement group-wide programmes specifically for ML/TF. However, there are several legal restrictions that may frequently and effectively impede CDD information sharing within financial groups, which are not in line with the standards. There are no provisions permitting (with or without restrictions) customer information unrelated to CDD as well as account and transaction information for AML/CFT purposes. FIs are not required to apply enhanced measures to manage ML/TF risks in case a state or territory where their branches and subsidiaries are located hinders implementation of the AML/CFT Law.

Recommendation 18 is rated largely compliant.

Recommendation 19 – Higher risk countries

Criterion 19.1 – The legislation does not explicitly require that FIs apply EDD to business relationship and transactions from countries for which this is called for by the FATF. Nevertheless, the application of EDD depends on the level of ML/TF risk and, when determining the risk of a client, FIs are required to take into account the level of compliance with FATF Recommendations of the client's country (BR No. 375, paragraph 4.3 and 4.5; BR No. 445, paragraph 4.2. and Annex 2). On that basis, FIs can tailor the measures according to the risks. This framework is complemented by RFM 103, stating that transactions with countries that do not comply with FATF Recommendations should be regarded as suspect and, therefore, filed to Rosfinmonitoring as an STR. A list regarding jurisdictions that fail to comply with FATF recommendations is determined by the Government of Russia with regard to the documents issued by the FATF and is published (Article 6, paragraph 1, subparagraph 2 L115; GR No. 667, paragraph 8, indent d), by Rosfinmonitoring (GR No. 173; RFM No. 361).

Also, any transaction above a certain threshold (RUB 600 000, around € 8.000) and related to remittances, loans, and securities where one of the parties is registered, resides or is located in a jurisdiction that "fails to comply with the FATF recommendations" – or if the stated transaction involve the use of an account in those jurisdictions – is subject to "mandatory control". As such, the FI should automatically report this transaction to Rosfinmonitoring. Below that threshold, such transactions are considered to be unusual (code 1304 of annex 3 of BR445; code 1304 of the annex to BR375) which entails further analysis. In addition, CIs have the right to (i) refuse to establish a business relationship or (ii) terminate it if at least two decisions have been taken in a calendar year on the refusal to comply with customers instructions due to lack of documentation to verify information and if there is an ML/TF suspicion (Article 7, paragraph 5.2 AML/CFT Law). However, (i) the automatic reporting of the

transaction to Rosfinmonitoring does not necessarily imply the application of enhanced due diligence proportionate to the risk, and (ii) CIs are entitled – not obliged – to refuse to establish or terminate a business relationship in the cases relevant for this criterion.

Criterion 19.2 – Russia applies countermeasures, such as the systematic reporting of financial transactions associated with natural or legal persons registered, resident or located in states that do not comply with FATF Recommendations (article 6, paragraph 1, AML/CFT Law), in accordance with the list referred to in c. 19.1.

Financial institutions are also required to pay enhanced attention to any transactions involving funds or other assets carried out by or on behalf of the referred natural or legal persons from those states or in the interests of such persons or entities, and with the use of an account of a bank registered in such a state (Article 7 (5.5.) L115). As noted in 19.1, FIs also have the right, not the duty, to refuse to establish a business relationship of in case of ML/TF suspicion.

Criterion 19.3 – Information on the results of mutual evaluations conducted by the FATF and FSRB is posted on Government websites[116]. Although posting the referred results online conveys the overall picture of a country's strengths and weaknesses, it should not be considered a substitute for indicating specific concerns on weaknesses of other countries' AML/CFT system. The BoR issues information letters advising CIs on certain AML/CFT risks emanating from specific countries (BR 168; BR 4609). FIs are also advised of the FATF public statements concerning higher risk countries, which they receive through the personal account.

Weighting and Conclusion

Russia largely complies with Recommendation 19 as few shortcomings exist. Particularly, the automatic reporting of the transaction to Rosfinmonitoring does not necessarily imply the application of enhanced due diligence proportionate to the risk. Moreover, CIs do not have an obligation to refuse to establish or terminate a business relationship in the cases relevant for this criterion. Also, financial institutions could be more frequently advised of specific concerns about weaknesses in the AML/CFT systems of other countries.

Recommendation 19 is rated largely compliant.

Recommendation 20 – Reporting of suspicious transactions

In its last MER, Russia was rated largely compliant with the former R.13 and partially compliant with the former SR.IV. Deficiencies related to the lack of power to report STRs based on the suspicion that a transaction might involve funds generated by insider trading and market manipulation (neither offence was criminalised); attempted transactions by occasional customers were not subject to a reporting obligation; and TF-related suspicious transaction reporting was limited due to shortcomings in the criminalisation of TF.

Criterion 20.1 – Where employees of financial institutions have suspicions that any operation is being performed for the purpose of legalising (laundering) illegal

116 http://fedsfm.ru/documents/international-statements.

earnings or TF, the obliged entity must send information within three working days from the date of identifying such operation to the "authorised body" (art.7 (3) AML/CFT Law). The legal obligation extends to reporting transactions even in case of a suspicion that the funds are the proceeds of crime due to the broad definition of money-laundering offence (see R.3) and as confirmed by legal practice (Order of the Plenary of the Supreme Court of Russia of 07.07.2015 N 32 (HC 32)). Rosfinmonitoring has been designated as the "authorised body" to receive STRs (Art. 3(5) and 8(1) AML/CFT Law; Art.3(b) GR No. 209). The requirement to report STRs within three working days from the date of detection of suspicion is assessed as sufficiently prompt.

Internal control programmes must include a wide range of indicators to assist financial institutions to detect unusual transactions, including lists of indicators on unusual transactions that could give rise to ML/TF suspicions, procedures for qualifying operations as suspicious, and taking further action (Art. 5.2, BRR 375 and BRR 445). The regulations also identifies the signs of unusual transactions – both in general terms and specific elements of ML schemes and certain risk factors related to geography (e.g. country risk), products (e.g. cash, loans, wire transfers), delivery methods (e.g. e-banking), including on TF. When there are reasonable grounds to suspect ML/TF and the STR is not disclosed to RFM such failure to comply entails administrative responsibilities (Article 15.27 parts. 1 and 2 of Code on Administrative Offences). The Russian authorities indicated that the STR can be submitted even in the absence of a specific operation (e.g. a dormant account) as the formation of a suspicion is not limited to the moment of the transaction but can be formed at subsequent time on the basis of additional information obtained (for example during on-going due diligence).

Criterion 20.2 – All suspicious transactions must be reported, regardless of the amount. FIs are required to report attempted transactions that are aborted at the customer's own initiative and which give rise to ML/TF suspicions within three days (AML/CFT Law, Art.7, para 2-3; RFM 103, Code 1124; BRR 375, Annex; and BBR 445, Annex 3). Reporting entities are required to report within one day to Rosfinmonitoring transactions and business relationships that are aborted at their own initiative due to suspicions (Art. 7(10) and Art. 7.5(8)) or refusal (Art.7(5.2) and (11)).

Weighting and conclusion

All criteria are met.

Recommendation 20 is rated compliant.

Recommendation 21 – Tipping-off and confidentiality

In its last MER, Russia was rated partially compliant with old R.14 as financial institutions and their directors were not covered by the safe harbour provision and the tipping-off prohibition.

Criterion 21.1 – Providing information on STRs and on other transactions to be reported by a financial institution or their heads and employees in compliance with the AML/CFT Law is not considered to be "*breach of service , banking, tax, commercial or communication secrets*" (Art.7(8) L115). Consequently, as long as an STR is made

"*for the purpose and in the procedure envisaged*" by the AML/CFT Law, the financial institution and its staff will be protected from both criminal and civil liability.

Criterion 21.2 – Tipping-off customers is strictly prohibited. Any reporting entity, including their heads and employees, is prohibited from informing the customer about any relevant information provided to Rosfinmonitoring (L115, Art. 7, paragraph 8). In addition, it is forbidden to inform customers and other persons on the measures taken to combat ML, TF, PF with the following exceptions: freezing of funds and other assets, suspension of a transaction, refusal to follow the customer's instruction on making transactions, refusal to open a bank account (deposit) and termination of a contract of bank account (Art.4 L115). Tipping-off provisions would inhibit the sharing of information as established under R.18, which requires information on transactions or activities which appear unusual (if such analysis was done) (see R.18).

Weighting and Conclusion

FIs and their directors, officers and employees are protected from criminal or civil liability in discharging their duty to submit STRs. Tipping-off provisions prevent FIs, their directors, officers and employees from tipping off customers; however they create some limitations to the sharing of information as established under R.18.

Recommendation 21 is rated largely compliant.

Recommendation 22 – DNFBPs: Customer due diligence

In the last MER, Russia was rated partially compliant with former R.12. Deficiencies – similar or in addition to the ones identified with regard to financial institutions under former FATF R. 5, 6 and 8-11 – related to, *inter alia*, insufficiently clear or missing requirements for beneficial ownership, ongoing due diligence, simplified and enhanced due diligence, timing of verification etc. (with regard to casinos, real estate agents and dealers in precious metals and stones); as well as limited CDD and record keeping requirements etc. (with regard to lawyers, notaries and accountants).

Compliance regime for DNFBPs

The AML/CFT Law sets up two different regimes of compliance for the subjects of the law. The first regime applies to all financial institutions and some DNFBPs (designated under Art. 5, for which this report uses the term "obliged entities" or "Article 5 entities"), particularly those involved in the gaming industry, the trade in precious metals and stones, and the real estate sector, which are subject to all relevant requirements set out in the law. The second regime applies to advocates, notaries, as well as to independent legal professionals and accountants (designated under Art. 7.1, for which this report uses the term "lawyers, notaries and accountants", or "Article 7.1 entities"), which are subject to the requirements on customer identification, internal control and record keeping[117], as well as on STR reporting[118] (subject to the professional legal privilege[119], as stipulated by the FATF Recommendations) whenever they prepare to carry out certain transactions on behalf or at the

[117] As set out in Article 7, Paragraphs 1, 2 and 4.
[118] As set out in Article 7, Paragraph 3.
[119] As set out in Article 7.1, Paragraph 5.

instruction of their clients. This second regime additionally applies to auditors regarding the STR reporting obligation only (Art. 7.1, Para. 2.1).

Criterion 22.1 **–** DNFBPs are required to comply with CDD requirements in the manners set out below. Minor deficiencies identified in R.10 equally apply here. All CDD-related provisions for the obliged entities set out in the AML/CFT Law, as well as in RFMO №366[120] on customer identification and in GR No. 667 on internal control rules[121] are identically applicable to casinos, DPMS, and real estate agents as Article 5 entities (see the preamble of the analysis for R.22), with certain specifics for lawyers, notaries and accountants as Article 7.1 entities (see the details under letter (d) below).

a) *Casinos* – Casinos must conduct CDD when customers engage in financial transactions. There is no specific requirement to conduct customer identification at the entry to a casino, and to ensure that the casino is able to link CDD information for a particular customer to the transactions that the customer conducts in the casino (the notion of mutually "linked" or "related" transactions). Nevertheless, the cash desks (Law on Gambling Activities, Art. 4, Para. 19-21) must be used for conducting any financial transactions – including acceptance of stakes, provision of chips/ tokens and payment of winnings (Art. 1(1), 2.1, 3 and 8(8)) – at which point the casino is obliged to identify the customers and is able to link identification information to the transactions conducted by them in the casino. There is no monetary threshold on financial transactions, thus encompassing situations broader than those set out in c.22.1(a).

b) *Real estate agents* – Companies and individual entrepreneurs providing intermediary services in transactions of purchase/sale of real estate (real estate agents) qualify as subjects of the AML/CFT Law in relation to any transaction. There is no express obligation to comply with the CDD-related requirements with respect to both the purchasers and the vendors of the property. Nevertheless, whenever the real estate agent is involved in a transaction for a client concerning the buying and selling of real estate, i.e. whenever a purchaser has been found for the property of the vendor that is the client of the real estate agent (or vice versa), both parties become the clients of the real estate agent, for which it has to comply with the CDD-related requirements.

c) *Dealers in precious metals and dealers in precious stones* – Applicable legislation does not specify a monetary threshold on cash transactions with the clients whereat DPMS would qualify as subjects of the AML/CFT Law, thus *encompassing situations broader than those set out in c.22.1(c).*

d) *Lawyers, legal professionals, notaries and accountants* – Lawyers, notaries and accountants, when performing the activities described under c.22.1 (d), are under an obligation to comply with certain CDD requirements set out in R.10,

120 As of the on-site visit, some provision of the RFMO №366 were redundant/ in conflict with – and nevertheless overridden by – the AML/CFT Law as amended in March 2018; however, the authorities advise that a new regulation endorsed by RFMO №199 of July 2019 has dealt with this issue.

121 Which comprise CDD-related elements such as obtaining and updating customer identification information.

with the exception of activities related to the creation, operation or management of legal arrangements (trusts) under foreign law. This is not considered a major deficiency as there is no evidence that Article 7.1 entities in Russia involved in such activities to a significant extent. Lawyers, notaries and accountants are required to identify customers and their authorized representatives (AML/CFT Law, Art. 7, Para. 1(1)), as well as of beneficial owners (Art. 7, Para. 1(2)); obtain information on the purpose and intended nature of the business relationship, take regular measures for establishing the purposes of financial and business activities, the financial standing and the business reputation of customers and, where necessary, take measures for establishing the sources of funds and/or other property of customers (Art. 7 (1.1)); as well as report STRs (Art. 7.1, Para. 2). These obligations apply whenever they prepare or carry out transactions on behalf or at the instruction of their clients, except if such information is subject to professional legal privilege, in line with the FATF Recommendations (Art. 7.1, Para. 5).

e) *Trust and company service providers* – The legislation does not regulate the provision of trust and company services separately from other economic activities. Legitimate company services, including their formation, operation and management, occurs under a tightly regulated regime whereby the registration of companies follows an intense scrutiny by the Federal Tax Service, and any representative must act in line with a power of attorney or a legitimate authorisation. In addition, providing false information on the real managers and owners is a criminal offence (CrC, Art.170.1, Art.173.1), and the legal address of a company must correspond to the place of the location of its permanent executive body or, if there is no permanent executive body, of other body or the person authorised to act on behalf of the legal entity (L.129, Art.8, para 2). Trusts cannot be formed in Russia, and Russia does not provide legal recognition to property held in trust, which may discourage the provision from Russia of services to any trust with property in Russia. Lawyers that are attested by the bar to represent clients in court proceedings, as well as notaries and accountants are not able to provide such services due to their specific sectoral legislation prohibiting this,[122] and their involvement in the provision of trust services would constitute violation of applicable sectoral laws (in case of lawyers, also of the relevant code of ethics) entailing administrative and disciplinary liability. Nevertheless, the law does not explicitly prohibit persons (individuals or companies), other than Article 7.1 entities covered by the AML/CFT Law, from providing trust and company services for profit, thus leaving a small gap as these persons are not covered by the requirements of R.22.

Criterion 22.2 – The provisions related to recordkeeping set out in the AML/CFT Law, RFMO No. 366 on customer identification and GR No. 667 on internal control rules[123] for financial institutions are identically applicable to casinos, DPMS and real estate

[122] L63, Articles 1 and 2 for lawyers; L4462-1, Articles 1, 6 and 35 for notaries; L307, Article 1 (6) for accountants.

[123] Which comprise elements related to the compliance with record keeping requirements regarding some financial institutions and DNFBPs, as well.

agents as Article 5 entities (see preamble above). These provisions apply equally to lawyers, notaries and accountants (L115, Art. 7.1, Para. 1). Minor deficiencies in R.11 apply here.

Criterion 22.3 – The provisions related to PEP requirements set out in the AML/CFT Law, RFMO 366 on customer identification and GR 667 on internal control rules[124] for financial institutions are identically applicable to casinos, DPMS and real estate agents as Article 5 entities (see preamble above). As for lawyers, notaries, and accountants, the AML/CFT Law (Art. 7.1, Para. 1) requires that these Article 7.1 entities comply with some of the PEP requirements defined by the law for Article 5 entities, particularly with those stipulated under Paragraph 1 (Sub-Paragraphs 1, 3 and 5), 3 and 4 of Article 7.3. This exempts them from the obligation to obtain senior management approval before establishing a business relationship with foreign PEPs, as well as to update on a regular basis the information available on their foreign PEP clients. This is not considered to be a major deficiency as most of these Article 7.1 entities are sole entrepreneurs, and foreign PEP clients would be very rare. Deficiencies in R.12 apply here.

Criterion 22.4 –The provisions related to new technologies set out in the AML/CFT Law, RFMO 66 on customer identification and GR 667 on internal control rules[125] for financial institutions are identically applicable to casinos, DPMS and real estate agents as Article 5 entities (see preamble above). As for lawyers, notaries and accountants, the AML/CFT Law (Art. 7.1, Para. 1, with further reference to Art. 7, Para. 2) requires that these Article 7.1 entities comply with risk assessment requirements defined by the law for Article 5 entities. See also the analysis for R.15.

Criterion 22.5 – The law does not permit DNFBPs to rely on third party to perform elements of CDD set out in R.10 (to identify the customer or the beneficial owner; to understand the nature of the business; or to introduce business) (L115 Art. 7, Para. 1.5-1.10).

Weighting and Conclusion

There are shortcomings with regard to lawyers, notaries and accountants (no CDD obligation when they prepare for or carry out transactions on behalf of a client concerning creation, operation or management of legal arrangements under foreign law; and no obligation to obtain senior management approval (in case they act not as sole entrepreneurs but as firms) before establishing a business relationship with foreign PEPs; no obligation to update on a regular basis the information available on their foreign PEP. There are also a shortcoming in that persons (other than the DNFBPs specified by the AML/CFT Law) providing trust and company services for profit are not covered by AML/CFT legislation. Deficiencies identified under the analysis for R.10, 11 and 12 bear an impact on the rating for R.22. Considering that most of the requirements are fully met, and that the provision of services to companies and trusts is tightly regulated and monitored, the shortcomings appear to be of a minor nature. **Recommendation 22 is rated largely complaint.**

[124] Which comprise elements related to the compliance with PEP requirements regarding some financial institutions and DNFBPs, as well.

[125] Which comprise elements related to the compliance with new technologies requirements regarding some financial institutions and DNFBPs, as well.

Recommendation 23 – DNFBPs: other measures

In its last MER, Russia was rated partially compliant with former R.16. Deficiencies related to, *inter alia*, lack of STR reporting requirement for attempted transactions by occasional customers, limited reporting obligation due to inappropriate criminalisation of TF, non-coverage of obliged entities and their directors by the safe harbour provision and the tipping off prohibition, as well as shortcomings in implementation of internal controls and counter-measures against high risk countries.

Criterion 23.1 – Reference is made to the description in the preamble of R.22 (the section entitled "Compliance regime for DNFBPs") on the two different regimes of compliance for the subjects of the law with, *inter alia*, STR reporting requirements. DNFBPs must report suspicious transactions subject to the following conditions:

a) *Lawyers, notaries and accountants* – STR reporting requirements apply to lawyers, notaries and accountants whenever they qualify as subjects of the law (see c.22.1 (d)). These categories are required to inform the FIU whenever they have "any grounds to believe" in the potential presence of ML/TF "not later than within three business days following the day, when the relevant transaction (operation) is detected"(RFMO №110, Art. 5.3 and GR №82, Art. 3). This is assessed as sufficiently prompt. The reporting obligation does not extend to information subject advocate's secrecy (L115, Art. 7.1, Para. 5), nevertheless the professional legal privilege is applied in compliance with the FATF Recommendations as there is case law[126] sanctioning lawyers (and notaries) for the failure to implement internal control rules as set out in GR №667[127] and these categories do in practice submit STRs to the FIU (see IO.4).

b) *Dealers in precious metals and stones* – The legislation does not specify for DPMS a monetary threshold on cash transactions with the clients (see c.22.1 (c)), and the general STR reporting obligation[128] set out in the AML/CFT Law with regard to Article 5 entities applies to DPMS (see preamble to R.22).

c) *Trust and company service providers* – See c.22.1(e).

Criterion 23.2 **–**The provisions related to internal controls set out in the AML/CFT Law and in GR 667 on internal control rules for financial institutions are identically applicable to casinos, DPMS and real estate agents as Article 5 entities (see the preamble to R.22). Lawyers, notaries and accountants must comply with internal control requirements (AML/CFT Law, Art. 7.1, Para. 1) as well as with qualifications of compliance officers and training requirements (RFM 203 and GR 492). Deficiencies identified in R.18 apply here.

126 Case No. 33a-9255/2018 resolved on December 27, 2018; Case No. 5-446/2018/92 resolved on 19 February 2019.

127 Which provides for the obligation to identify (Art. 4(d)) and report (Art. 24(d)) suspicious transactions.

128 As opposed to the specific STR reporting obligation set out in the AML/CFT Law with regard to the subjects of the law designated under Article 7.1 (i.e. lawyers, notaries and accountants, see the analysis for c.23.1 (a)).

Criterion 23.3 **–** The provisions related to higher risk countries set out in the AML/CFT Law and in GR No. 667 on internal control rules for financial institutions are identically applicable to casinos, DPMS and real estate agents as Article 5 entities (see the preamble to R.22). As for lawyers, notaries and accountants, the legislation does not set out additional specific provisions relevant for the compliance with AML/CFT requirements under R.19. Deficiencies identified in R.19 apply here.

Criterion 23.4 **–** The provisions related to tipping-off and confidentiality set out in the AML/CFT Law for financial institutions are identically applicable to casinos, DPMS and real estate agents as Article 5 entities (see the preamble to R.22). As for lawyers, notaries and accountants, the legislation does not set out additional specific provisions with requirements under R.21. Deficiencies identified in R.21 apply here.

Weighting and Conclusion

There are minor shortcomings for lawyers, notaries and accountants who are not subject to AML/CFT requirements when they prepare for or carry out transactions on behalf or at the instruction of their clients concerning creation, operation or management of legal arrangements under foreign law. Deficiencies identified in c.22.1(e) as well as deficiencies identified in R.18, R.19, and R.21 bear an impact on the rating for Recommendation 23.

Recommendation 23 is rated largely complaint.

Recommendation 24 – Transparency and beneficial ownership of legal persons

In the last MER, Russia was rated partially compliant with these requirements. The main deficiency was related to the fact that none of the existing systems achieved adequate transparency regarding BO and control of legal persons.

Commercial and non-commercial organisations can be set up in Russia (see Chapter 1). Legal persons operating in special economic zones are subject to the same registration and information requirements of other companies as per L.129 and L.115 (L.116, Art.6). [129]

Criterion 24.1 **–** The CvC sets out the different types and forms of legal persons in Russia (article 48 et seq., namely article 50) as well as their basic features (*e.g.* article 52, on the constitutive documents of legal persons; article 53, on the legal persons' bodies). Law No. 129-FZ states in a detailed and thorough manner a set of basic information that legal persons need to file. Information that identifies and describes the different types, forms and basic features of legal persons in the country is available on the internet.[130] Law No. 129-FZ outlines a thorough process for the creation of legal persons in Russia and for obtaining of basic information. Regarding BO information, the AML/CFT Law obliges legal persons to have and keep information on the BOs as well as update it on a regular basis (at least once a year) (Art.6.1).

Criterion 24.2 **–** Russia's ML NRA presents a specific section on the topic of transparency and the BO of all legal persons. This assessment was based on the analysis of several information sources. Although Russia conducted a comprehensive information gathering and analysis exercise, additional data-sets could have been

129 http://economy.gov.ru/minec/activity/sections/sez.
130 www.nalog.ru/create_business/ul/creation/.

used to determine in more granularity the risk associated with legal persons (see IO.5). The TF NRA approaches legal persons risk in accordance with the stages of the TF process, through which the means of raising, moving or using funds are determined. However, it does not specifically assess this risk in relation to all types of legal persons. A separate assessment of the TF risks in the non-commercial sector was carried out. According to the results of this assessment, the types of non-commercial organisations were distributed by risk level, specific TF vulnerabilities and risks were identified.

Criterion 24.3 – All legal persons are required to be registered in the USRLE (article 48, paragraph 2 CvC). Legal persons acquire legal personality after registering with this State register (CvC, Art.49(3)). The USRLE must record basic information of all legal persons (to include name of the legal person, the original or a copy of the founding documents attested by a notary – which include basic regulating powers, legal form and status, address of the registered office, directors) (Law No.129, Art.5(1)). The information is required to be publicly available (article 51, paragraph 2 CvC and article 6, paragraph 1 of Law No. 129-FZ).[131]

Criterion 24.4 – Legal persons operate upon charters, except for business partnerships (which operate under a constitutive agreement, concluded by its founders, and which are subject to the rules in the CvC on the charters legal persons) and state corporation (that operate under the federal law on such corporation) (CvC, Art.52). These charters must include type and number of shares or members as well as associated voting rights (Article 12 of L14, for LLCs; article 11 of L208 for JSC) which must be approved by its founders/members. These contain the information mentioned in criterion 24.3. More detailed provisions and requirements for retention of information on shareholders or members by legal persons, depending on their legal forms and types, are set out in the laws governing the activities of the respective legal persons (regarding LLCs, see article 31.1 of Law 14; on JSC see article 44 of Law 208; on securities holders, see article 8 of Law No. 39,). Bearer shares are not allowed in Russia since a share is defined as being an inscribed security (Art.2, Law No. 39).

The address of the legal person must be communicated to the State register (CC, Art.54 (3)). The location of a legal person is determined based on the place of its government registration, which is conducted at the location of its permanent executive body or, if no such body exists, at the location of other body or a person entitled to act in the name of a legal person without power of attorney (Article 54 of the CC; Article 8 of Law No. 129-FZ). Most documents required under c.24.4 must be kept in Russia by the FTS, the USRLE and the legal persons themselves. However, there is no explicit obligation on a Russian legal entity to maintain the information on shareholder/members and of directors in Russia in all cases (e.g. where the legal person is not tax resident in Russia).

131 Simple Partnerships and Investment Partnerships do not constitute a separate legal person and need not register with the Uniform Register as such. They are registered for tax purposes with the Tax Office. See http://www.eoi-tax.org/jurisdictions/RU#latest. According to article 1041 of the CvC only individual entrepreneurs and/or commercial organisations may be the parties to the contract of partnership. Therefore, information about the participants of such a partnership is contained in the USRLE and is accessible to the competent authorities.

Criterion 24.5 – Any change to information recorded in the USRLE – relevant for c.24.3 and c.24.4 – shall be reported by legal persons to the USRLE within three business days following such changes (article 5, paragraph 5 of Law No. 129-FZ). Prior to registration of a legal person or of any other new data, USRLE is obliged to verify reliability of the information (CvC, Article 51, paragraph 3). The FTS verifies the conformity of the form and the data contained in the provided documents in the case of applications for registration as well as when there are reasonable doubts about veracity of information (Article 9, paragraph 4.1 of Law No. 129-FZ and Order of the FTS No.MMV-17-14/72) and can refuse the registration for inconsistency of the identification details and documents (Article 23, paragraph 1 of Law No. 129-FZ). JSCs and LLCs are obliged to ensure maintenance and keeping of the register of shareholders (article 44, paragraph 1 of Law No. 208-FZ; article 31.1 of Law No. 14-FZ). Regarding securities holders, the holder of the register bears responsibility for the completeness and reliability of information (article 8, paragraph 3.9 of Law No. 39-FZ).

Criterion 24.6 – Any legal person created under Russian legislation is required have information on its BOs[132] (L115, Art.6.1). Natural and legal persons who are founders or participants of the legal person or otherwise control it are obliged to provide the legal person with the necessary information to determine the BO (L115, art. 6(5)). The managers as well as the legal person can be sanctioned with an administrative fine (form RUB 30 000 to RUB 40 000 for managers (approximately from EUR 400 to EUR 530) and RUB 100 000 to RUB 500 000 for legal entities (approximately from EUR 1 300 to EUR 6 700)) if the legal person does not comply with the requirement to obtain, update and provide BO information to the authorities on request (Art.14.25.1 CAO).

In addition to the requirement to have BO information available by all legal persons created under Russia law, BO information is also collected by FIs and DNFBPs when establishing a business relationship (see criteria 10.5, 10.10, and 22.1, where deficiencies apply; see GR No. 913, paragraphs 1 and 2, read in tandem with article 6.1. and article 7, paragraph 1, sub-paragraph 2, and paragraph 14 L115). BO information is also available information on companies listed on a stock exchange (see GR No. 913, paragraphs 1 and 2, in tandem with article 6.1. and article 7, paragraph 1, sub-paragraph 2 L115).

Criterion 24.7 – The AML/CFT Law provides that BO information be updated, but not necessarily to the extent that it is as up-to-date as possible. Legal persons must update BO information on a regular basis, and at least once a year (L115, Art. 6.1(3)). According to Russian authorities, "on a regular basis" means that in the case of changes in the share of the charter capital of at least one of its founders or changes in the ownership structure, a legal person is obliged to request information from individuals and legal persons that are the founders or participants of the legal person or otherwise control it, necessary to establish their BOs (paragraph 4 of article 6.1 L115). There is no obligation on the owners to inform the Russian legal person of a BO change, which means that the Russian legal entity may not be aware of a change in the charter capital. FIs/DNFBPs who collect BO information on legal persons for

[132] For the purpose of this provision, a BO is defined as an individual that ultimately, directly or indirectly (via a third party) owns a legal entity (has a dominant participation in the capital of more than 25 percent) or can control its activities (L115, article 6.1 (8)).

the purpose of CDD must update information on at least once a year or in case they have doubts about the credibility and accuracy of information received earlier (see c.10.7 b), which is not fully in line with the requirement to have information as up-to-date as possible (for example, if the BO changes without the reporting entity being aware of it). For those legal persons that have a relationship with an FI/DNFBP in Russia, accuracy of BO information is ensured by FIs/DNFBPs who must take reasonable measures to verify the information received. Regarding the information collected by the company itself, there is no provision (such as verification of the information received) that ensures the accuracy of BO information.

Criterion 24.8 – There are sufficient measures to ensure that legal persons cooperate with competent authorities. All legal persons are required to collect information on their BOs and share it with the FTS and Rosfinmonitoring (article 6.1, paragraph 4 to 6 L115 and GR No. 913, paragraph 1). The head of the legal person or other authorised to act on its behalf must be authorised by the company for providing all basic information and available BO information in electronic form (see article 6.1, paragraph 6 L115 and GR No. 913, paragraphs 5 and 6). Failure to provide information to FTS and Rosfinmonitoring is subject to sanctions (see c.24.12). LEAs can access information from FTS and Rosfinmonitoring (on the basis of co-operation agreements and/or Joint Order RFM 207 new).

Criterion 24.9 – JSCs and LLCs are required to keep records of basic information (article 50, paragraph 1 of Law No. 14-FZ, for LLCs; article 89, paragraph 1 of Law No 208-FZ, for JSCs). Other types of entities are also required to do so by way of keeping information present on their charters (article 52 (4) CvC), including business partnerships (article 9 (2) of Law 380). FIs/DNFBPs are required to keep record of their customer's information and related documents for a period of at least five years from the moment of termination of business relationship (article 7, paragraph 4, L115). BO information is required to be kept by legal persons for a period of at least five years from the moment of receipt (article 6.1, paragraph 3, L115), which is not fully in line with the requirement that records be maintained for at least five years from the date on which the legal person is dissolved. Information must be kept by competent authorities for 15 years after termination of activities (Order of the Ministry of Culture of Russia of 25.08.2010 No. 558) and after liquidation (Order No 15 of MoF, 2013). Access to documentation by a liquidation commission is possible (article 23, paragraph 10 of Law 125-2).

Criterion 24.10 – Basic and BO information can be directly accessed by all competent authorities (PD No. 808, paragraph 5.1; article 6.1, paragraph 6 L115; Law No. 3; article 4, paragraph 2.1 of Law No. 2201-1-FZ; article 31 of the Tax Code; article 6.1, paragraph 6, L115, article 7, paragraph 1, sub-paragraph 3 of Law No. 403-FZ; BR No. 147, article 2.5.3; Law No. 86-FZ, article 73; article 7, paragraph 14, AML/CFT Law; GR 228, paragraph 5.1.1.2.5; L126, article 27, paragraph 8 (1); GR 1052; L41, article 13). Rosfinmonitoring can provide information on BOs to LEAs pursuant to inter-agency co-operation agreements concluded with the GPO, MoI, FSB, FCS, and IC.

Criterion 24.11 – The issuance of bearer securities is admissible in the cases established by law (article 143 (5) CvC. All securities must be registered (Article 2 of L39), therefore, the issuance of shares to the bearer is not possible. Registration and transfer of securities is carried out by a professional securities entity, which is

covered by AML/CFT law (article 8 of L39).[133] Paper securities may transferred for keeping to a person entitled by law and/or keep record of the rights of securities (art. 148.1 CvC). The rights of the owners to the issued securities of the documentary form of issue shall be attested by certificates (if certificates are held by the owners) or by certificates and records in the special custody accounts in depositories (if certificates have been put in custody in the depository) – article 28 of the L39. Therefore, when a bearer security in immobilized, the rights of the owners will be kept by a security professional. The law does not regulate share warrants, so their issuance would not have any legal value.

Criterion 24.12 – Nominee shares and nominee directors are not recognized in Russia's legal system, and any representative of owners/directors must receive proper authorisation. The provision of nominee services without authorisation would lead to criminal prosecution for providing false information on the true managers and owners (CrC, Art.170.1, Art.173.1). It is possible that shares be held by someone on behalf of someone else by establishing a "Discretionary Management Agreement" (DMA) (trust of estate, article 1012 (1) CvC).[134] A trust of estate is established by contract, which must identify the property and the name of the legal person or the individual in whose interest the trust of estate is exercised (article 1016 (1) CvC). Securities can be held by the professional intermediary under a "depository agreement" (paragraph 1 of article 8.2 and paragraph 1 of article 8.3 of the L39).

Criterion 24.13 – Even if there is a wide range of sanctions for violations of the requirements under R.24, the sanctions are not fully proportionate and dissuasive. There a number of administrative sanctions, such as: failure to store data (fines from 2.500 to 5 000 RUB (EUR 30 to EUR 60)) on natural persons and from RUB 200 000 to 300 000 (EUR 2 500 to EUR 4 000) on legal persons) (CAO, art.13.25); engaging in business activities without registration (fine of RUB 500 to 2 000 (EUR 7 to EUR 27)); refusal to provide information or inaccurate or untimely information (fine from RUB 1 000 to RUB 2 000 (EUR 26 to EUR 32) on the official person responsible (Article 14.25); failure to comply with the AML/CFT legislation (fine from RUB 30 000 to RUB 50 000 (EUR 400 to EUR 670 on natural persons and from RUB 300 000 to 500 000 (EUR 4 000 to EUR 6 500) on legal persons) (Article 15.27); failure to obtain, update and provide BO information to the authorities (fine from RUB 30 000 to RUB 40 000 for managers (approximately from EUR 400 to EUR 530) and RUB 100 000 to RUB 500 000 for legal persons (approximately from EUR 1 300 to

[133] Depositary activity means the rendering of services in the custody of certificates of securities and the record-keeping of securities and the transfer of rights to them (art. 7 of L39). The certificate of security is a document issued by the issuer and certifying the totality of rights to the number of securities specified in the certificate.

[134] A DMA is an arrangement by which one party (settler) shall transfer estate in discretionary management to the other party (administrator) for a determined period, while the other party shall undertake to administer this estate in the interests of the seller or the person indicated by him (beneficiary). The object of the DMA may include enterprises, real estate, securities, rights certified by non-documentary securities, exclusive rights and other property (article 1013 (1) CvC) and cash, in certain instances provided for in law (art.1013 (2) CvC). The trust of estate administrator can be either a natural or legal person (e.g. a non-profit organization, an individual entrepreneur or a commercial organization, with the exception of a unitary enterprise) – article 1015 (1) CvC. The transfer of estate does not involve the transfer of ownership rights to the discretionary manager (administrator).

EUR 6 700)) (Art.14.25.1 CAO); breach of the rules for keeping register of securities holders (art.15.22). failure to register the name of securities owners (fine ranging from RUB 30 000 to RUB 50000 RUB (EUR 400 to EUR 670) or disqualification for a period of one to two years on natural persons and from RUB 700 000 to RUB 1 000 000 (EUR 9 500 to EUR 13 500) on legal persons. Violation of registration requirements (L.129) may lead to liquidation by a court ruling (art. 25 CvC). Compensation for losses may also be ordered if the required information to the register of legal entities is not provided, is not provided timely or is unreliable (article 51, paragraph 2 CvC).

There are criminal sanctions for in the CrC: provision of false information to the USRLE, register of securities holders or depository record-keeping system (art. 170.1) (fine from RUB 100 000 to RUB 300 000 (EUR 1 250 to EUR 4 000) or imprisonment for a period of up to two years; illegal establishment (creation, reorganisation) of a legal person (article 173.1 (1) (fine from RUB 100 000 - 300 000 (EUR 1 250 to EUR 4 000) or imprisonment up to three years, with aggravating factors if the offence is committed in an official capacity or in an organised fashion (art. 173.1 (2)); illegal use of documents for establishment (creation, reorganization) of a legal person (art. 173.2 (1)) (fine from RUB 100 000 to 300 000 (EUR 1 250 to EUR 4 000) or corrective labour for up to two years. The amount of the fine is determined by a court taking into account the gravity of the crime and the property status of the convicted person and family, as well as the convicted person's ability to receive a wage or any other income (art. 43, 46(3) CrC). On administrative and criminal liability, the applicable pecuniary sanctions are neither proportionate nor dissuasive, especially given the low minimum and maximum amounts. Ancillary sanctions are dissuasive. Although the imprisonment sanction is potentially dissuasive, it may not be proportionate given the types of offences at stake.

Criterion 24.14 – Competent authorities, including Rosfinmonitoring, the FTS, the GPO, the MoI, IC and the FSB), co-operate at the international level in order to exchange relevant information at their request or on their own initiative (art.10 L115). This is a general co-operation clause and thus includes basic, BO and shareholder information. However, there is no legal reference requiring them to act rapidly (see also R.37 and R.40).

Criterion 24.15 – Pursuant to receiving information from a foreign FIU on BO, Rosfinmonitoring's database is uploaded with it. In accordance with paragraph 4.1.3 of the Temporary Procedures for Conducting Electronic Cases of Financial Investigations and Forming a Database, approved by the Director of Rosfinmonitoring No. 01-00-08 / 16121 of July 2017, the "Inquiry Statement on the Primary Examination of Material" is formed, where the types of information received are indicated, including on BO.

In order to inform foreign FIUs about the quality of international co-operation, Rosfinmonitoring fills in the relevant questionnaires on the quality of international co-operation sent by foreign partners in accordance with the requirements of the Group Egmont on a quarterly basis.

Weighting and conclusion

Russia largely complies with R.24 as few shortcomings exist. The TF NRA does not specifically assess each type of legal person. BO information needs to be updated, but not necessarily to the extent that it is as up-to-date as possible. FIs/DNFBPs who collect BO information on legal persons for the purpose of CDD must update information on a risk-sensitive basis. Sanctions are neither sufficiently proportionate nor dissuasive.

Recommendation 24 is rated largely compliant.

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

In the last MER, these requirements were considered to be not applicable to Russia, since the legal system did not allow for the creation of trusts and the legal concept of trust did not exist. The FATF Recommendations have since been revised such that some elements of R.25 apply to all countries. Even though express trusts and other similar legal arrangements cannot be created under Russian law, nothing prevents a person in Russia from setting up or managing a legal arrangement created under foreign law.

Criterion 25.1 –

a) Express trusts or other comparable legal arrangements cannot be established in Russia, therefore this sub-criterion is not applicable.

b) Same as (a) above.

c) The law does not require persons acting as professional trustees of a foreign trust to maintain basic or BO information of the trust. TCSPs are not obliged entities under the AML/CFT legislation. When a trust created under foreign law uses the services of FIs/DNFBPs, the FI/DNFBP is obliged to identify the parties to the trust (AML/CFT Law, Art.7, paragraph 1, (1), 14; Art.7.1), including the trustee. FIs and legal professionals are required to conduct CDD in relation to customers (including a foreign trust), when providing a certain number of services but not in a situation where they act as trustees of a foreign trust (see c.22.1d). Lawyers that are attested by the bar to represent clients in court proceedings, notaries and persons providing accountancy services who, in general, are more likely to act as trustees, are not able to provide such services due to their specific sectorial legislation who prohibits this (see c.22.1).

Criterion 25.2 – FIs and most DNFBPs must conduct due diligence and identify the parties to a foreign trust when a foreign trust is a customer. However, it is not clear that FIs/DNFBPs must conduct CDD and therefore identify the parties to a trust when acting as a trustee (see c.25.1c). FIs must update CDD information (L115, Art.7, paragraph 1, sub-paragraph 3) on their customers. Professionals subject to article 7.1. of the AML/CFT Law do not have an obligation to keep information updated (as provided for article 7, paragraph 1, sub-paragraph 3).

Criterion 25.3 – There are no specific obligations for trustees to disclose their status to FIs/DNFBPs. FIs/DNFBPs are required to identify foreign customers that are not

legal persons, and so may identify a trustee, request documents attesting his/her status, and refuse the business relationship in case the FIs/DNFBP cannot identify and verify the identity of the trustee. Customers are also required to provide necessary information for the execution of the AML/CFT Law (L115, article 7, paragraph 14).

Criterion 25.4 – Since Russian legislation does not allow for the creation of legal arrangements, persons acting in Russia as trustees of foreign trusts would not have enforceable means to oppose the provision of information on the trust (including assets held or BO information) to domestic or foreign competent authorities, FIs or DNFBPs.

Criterion 25.5 – Competent authorities have the powers to access information from reporting entities, including on trusts (article 5, article 7 paragraph 1, subparagraphs 1 and 5 of L115). The FTS and LEAs can also access information directly from FIs/DNFBPs (article 26 of Law 395, see R.31). Credit institutions have the obligation to provide information on transactions and accounts of legal persons as well as information on transactions, accounts and deposits of natural persons to investigators responsible to conduct criminal intelligence and detective operations and responsible for detecting, preventing and disrupting crime at their requests (article 26 of the Law 395-1, c).

Criterion 25.6 – Competent authorities, including the FTS, cooperate at the international level in order to exchange relevant information at their request or on their own initiative (Art.10 L115). This is a general co-operation clause and thus includes basic, BO and shareholder information.

Criterion 25.7 – Legal professionals can provide trustee services and do not have an obligation to keep and provide information on the trust in such situations. As such, it is not possible to make trustees legally liable for non-compliance and to apply sanctions accordingly.

Criterion 25.8 – There are sanctions for failing to grant competent authorities access to information on a trust. Failure to comply with a lawful request from LEAs is an administrative offence, punishable by fine or suspension of business activity (CAO Art.17.7). Failure to provide information to Rosfinmonitoring on customer transactions and BOs by an obliged entity can result in a fine ranging from RUB 30 000 to 50 000 (EUR 400 to 670) on natural persons and RUB 300 000 to 500 000 (EUR 4 000 to 6 500) on legal persons (art.15.27 CAO). However, since there is no obligation for the professionals referred to in c.25.1 and 25.2 to provide Rosfinmonitoring with information on the trust except in the case of an STR submitted, such sanctions are not applicable to them.

Weighting and conclusion

Russia partially complies with R.25 as major shortcomings exist. FIs and DNFBPs are not obliged to conduct CDD when they act as a trustee. There are no specific obligations for trustees to disclose their status to FIs or DNFBPs. TCSPs are not obliged entities under the AML/CFT legislation. Legal professionals do not have an obligation to keep information updated, including regarding trusts, and are not required to keep information on the trust when providing trustee services.

Recommendation 25 is rated partially compliant.

Recommendation 26 – Regulation and supervision of FIs

In the last MER, Russia was rated partially compliant with former R.23. Main deficiencies derived from: no provisions to prevent criminals from becoming major shareholders in a non-banking financial institution; inadequate provision regarding persons having a controlling interest with respect to a credit institution; and no fit and proper requirement regarding leasing companies, MVTS providers, the members of the board of a life insurance company or an insurance broker.

Criterion 26.1 - Russia has designated supervisors with responsibility for regulating and supervising all types of FIs. BR has been designated as the regulator and AML/CFT supervisor of credit institutions (and of bank groups), and non-credit FIs (Article 4 para. 9 and article 76.1 of the BoR Law (L86)). Roscomnadzor is the AML/CFT supervisor for federal postal communication and telecommunication operators (GR228, part 5.1.1.2.5). Rosfinmonitoring has the power to register and supervise any other financial institution not otherwise supervised (PD808, part 5-1.1; GR58 article 1; L115, Art.7, para 9).

Criterion 26.2 - FIs are required to be licenced or registered from designated authorities before conducting financial business. Core Principles FIs are required to be licenced by BoR L395, article 1, 12 and 13; L39, article 39); L4015, article 4.1, para.2, article 6, para.1, and article 32; L156, article 2, para.2, article 38, para.3, article 44, para. 1 and 2; L75 article 2, para.1). Federal postal services is licenced by Roscomnadzor (GB228, art.5.1.4). Other FIs are required to be registered with the USRLE and maintain the registration with BoR: Microfinance Organisations (L151, art. 4); Credit Cooperatives (L190, art. 5, par. 2(4)); Agricultural Consumer Credit Cooperatives (L193, art. 40.2). Purchase and sale of foreign currency both in cash and in non-cash form refers to banking operations, which can be carried out only by CIs under BoR licence (art.5, L 395) and the decision on licensing requires that a legal entity with a physical address in Russia, providing constitutive agreement, charter, business plan, and meeting the "fit and proper" standards (L395, art. 14). These requirements in practice prohibit shell banks from operating within Russia.

Criterion 26.3 - Supervisors take various regulatory measures to prevent criminals and their associates from holding a significant controlling interest or a management function in a financial institution. For CIs, BoR exercises "fit and proper" tests (such as including higher education, working experience, as well as integrity requirements including business reputation and no conviction for intentional crimes) to refuse a board or managerial position, or other controlling position. For directly or indirectly (through the third party or by a group of people) acquisition of more than 1% of the shares of a CI, BoR will need to be notified; if more than 10% is acquired, BoR needs to give prior consent (L395-1, art. 11 and art.16)). Supervisors for all FIs must verify fit and proper requirements of managers and major shareholders in FIs, including by checking whether a person has outstanding convictions willful crimes (L4015, art.32.1 and L281, para 1 and para 6.1; L156, art.38 and 38.1; L75, Art.4.1 and 6.2; L151, Art.1 and Art.1.1-1) or for crimes in the field of economic activities or crimes against the state (L39, art. 10.1 para.1; for credit cooperatives, L190, Art.15 para.4; L164, art. 5, para.5). "Russia Post" is a state enterprise and the director is appointed by the Government. Payment operators are required to register with Rosfinmonitoring and criminal records are checked only at the application stage. BR has the power to replace the management for all FIs. Minor shortcoming relates to

criminal record checks not clearly covering criminal associates and the wider array of criminal offences.

Criterion 26.4 -

a) Regulation and supervision for banking activities are largely in line with the core principles, and were assessed by the IMF during the FSAP process in June 2016. BoR supervision of AML/CFT issues is intensive and has a track record of enforcing AML/CFT requirementThe supervision for AML/CFT purposes is applicable to consolidated group, except that greater attention is needed in consolidated supervision with respect to groups that have foreign establishments and specific requirements are needed for management of country risk and transfer risk.[135] Supervision is generally risk-based, however, insurance regulation and supervision is still largely rules-based, and there is space for building BR's specialized insurance expertise.

b) Other FIs, including the FIs that provide MVTS, are all within the scope of AML/CFT supervision. Supervisors have issued regulations on the supervisory processes that are applied to these FIs. Currency exchange services can only conducted by CIs on the basis of the relevant licence, thus are covered under AML/CFT supervision as CIs.

Criterion 26.5 - The frequency and intensity of AML supervision of FIs or groups is generally determined on the basis of the conclusion about the ML/TF risks and internal controls rules of the entities or groups. The risk of each institution is determined taking into account various aspects including the results of the NRA and of the SRAs, the diversity of the scale of the entity's activities, the business focus, the individual characteristics of each entity and their compliance with the AML/CFT legislative requirements. Planned on-site inspections are conducted in a 2-year cycle as part of prudential supervision (para.1.4 BR147), and if it is decided to include AML/CFT component, then the scope and intensity of the planned inspection is determined on the risk profile and the internal control rules and applications of institutions. Unscheduled inspections can be triggered solely based on AML/CTF issues, of which risk profile and the state of internal control are also considered when determining the scope and intensity of the inspection. Off-site monitoring is conducted based on information in suspicious transactions and activities, potential AML/CFT breaches spotted by Rosfinmonitoring, as well as reviews of internal controls rules of CIs and NCFIs, and other information. However off-site supervision and unscheduled inspections can only be carried out on the ground of potential violation of the AML/CFT legislation, and not on the basis of other risk considerations.

For FIs other than banks, factors that determine the frequency and intensity of checks include the financial condition and prospects of activity of the NCFI, exposure to risks, the quality management of the NCFI including evaluation of risk management and internal control, reliability of its reporting and results of previous inspections (para.4.1 of BR151-1). Rosfinmonitoring and Roscomnadzor conducted on-site and off-site inspection on payment operators and postal services based on the risks profile including considering the NRA, the application of internal control rules and the characteristics of entities.

[135] See IMF Financial Sector Assessment Program (FSAP), June 2016.

Criterion 26.6 - BoR reviews the ML/TF risk profile of a FI or group at least quarterly as part of the assessment of quality of Bank's management, of the vulnerabilities and the risks of involvement in conducting of suspicious transactions, and the risk of non-compliance (Chapter 1and 4, BR 4336 for CIs; BR 4922 for NCFI). Generally, risk profile is also reviewed before inspections of CIs and NCFIs. On-site inspection taking into account the result of off-site review, is another way to understand the ML/TF risks including non-compliance risk of institutions. Besides, the BoR assesses the economic situation of banks including assessing the indicators of the state of internal control of CIs (BR4336 for CIs, BR4922 for NCFIs).

There is no explicit requirement on reviewing the assessment of the ML/TF risk profile of a financial institution or group where major events or developments in the management and operations (beside the above suspicious operations) happen, while changes in financial sustainability, economic status, financial condition and business prospects (including the quality of the management) of FIs are the basis for carrying out unscheduled inspection (BR149, para.4.1 and BR156, para.4.1) that will enable supervisors to update the knowledge of ML/TF risks. No information was provided on Roscomnadzor implementation of this criterion.

Weighting and Conclusion

Most criteria are met, but there are shortcomings in the market entry requirements mostly relating to criminal record checks that do not clearly address criminal associates and the wider array of criminal offences. There is no explicit requirement on reviewing the assessment of the ML/TF risk profile of a financial institution or group where major events or developments in the management and operations happen, though unscheduled inspection on some circumstances may make up some requirements.

Recommendation 26 is rated largely compliant.

Recommendation 27 – Powers of supervisors

In the last MER, Russia was rated partially compliant with former R.29. Deficiencies included: limitation on the BoR for conducting on-site AML/CFT inspections and limited powers to sanction FIs.

Criterion 27.1 - The BoR is a regulatory and supervisory body for AML/CFT issues of credit institutions and non-credit FIs (including professional participants in the securities market, insurance companies and organisations managing investment funds, etc.) (Art. 56 and 76 BR Law; art. 7 AML/CFT Law). Roscomnadzor controls and supervises communication service providers and is responsible for the AML/CFT supervision of federal postal service (AML/CFT Law). Rosfinmonitoring controls and monitors AML/CFT compliance of other FIs and relevant individuals where no other supervisor exists (art.5 PD 808).[136]

Criterion 27.2 - BoR has the authority to conduct inspections of CIs (and their affiliates) and non-credit FIs (Art.73 and 76.5 BR law). Rosfinmonitoring and

[136] Leasing companies, payment-acceptance operators, commercial institutions which conclude the contracts as financial agents for financing at assignment of a monetary claim

Roscomnadzor have the legal basis to conduct checks on its regulated entities (part II PD808; art.5.1.1.2.5 of GR 228, art. 50 of Order No. 213).

Criterion 27.3 - BoR has the right without any restrictions to receive any information relevant to monitoring compliance, including all documents and information, access to the software and hardware, request explanations concerning the information received as well as information and documents from third parties, customers and shareholders (art. 73 and 76.5 of L86, para. 2.5 of L147-I, L151-I; sub-clause 2.7.3 of L147-I and Para. 2.7 of L151 ;Para. 2.8 of L147-I, Para. 2.5 of L151;art.57 of BOR Law; art.44 (7) L39; art.30(5.4); art.55 (13) L156); art. 34 of L75; art.30 of L4015-1; art.14 of L151; art.5 of L190; art.40.2 of L193; art.2.3 of L196. Rosfinmonitoring has the right to request and receive any information related with implementation of requirements of AML/CFT legislation from entities it supervises (para.7 RFM191, para.6 PD 808). Roscomnadzor has the power to request and receive information and documents which are necessary for inspection (art.27(8) L126) and has the right to request information concerning the verification of compliance with AML/CFT requirements (art.53.2 (9.14) of L213). The exercise of these powers is not contingent upon supervisors obtaining court orders.

Criterion 27.4 - The BoR can impose a range of sanctions, including warning, administrative fines on individuals, suspension of activities (art.15.27 CAO), restrictions on individuals conducting financial activities, and restrictions on the scope of operations. BoR also has power to require CIs to eliminate any identified breaches, impose fines, restrict specific transactions, or impose a ban on individual banking operations (Art. 74 L86). BoR has the power to withdraw the licence of FIs in cases of repeated AML/CFT breaches (art.20 L395; art.39.1(8),44(4) L39; article 7, para.1.1(3) of L151; (Para 5 of Art. 32.6, Para 2 Art. 32.8 L 4015-1). BoR can apply to court for liquidation of a credit cooperative in case of multiple violations of federal laws and regulatory legal acts (art.5, para.3(9c) L190), and as well agricultural credit cooperative (subpar. 11 of art.40.2 of L193) and pawnshop (subpar.6, part 4 of art.2.3 of L196).

Roscomnadzor can issue warnings, suspend the licence for failure eliminate the identified violation, and revoke the licence for failure to eliminate the circumstances that caused the suspension of the licence, within the established period (Art. 37, Art. 39 L126). Roscomnadzor is also empowered to consider cases of administrative offences for failure to comply with AML/CFT Law (art.23.44 CAO). Sanctions are not in line with the standards set out in R.35. Rosfinmonitoring is empowered to consider cases of administrative offences under parts 1-3 of Art. 15.27 of the Administrative Code (art.23.62).

Weighting and Conclusion

Most criteria are met, however there remain minor deficiencies in that sanctions are not fully in line with R.35.

Recommendation 27 is rated largely compliant.

Recommendation 28 – Regulation and supervision of DNFBPs

In the last MER, Russia was rated partially compliant with former R.24. Deficiencies related to a lack of AML/CFT licensing regime for casinos, monitoring of lawyers, lack of details of specific AML/CFT monitoring of notaries, and TCSPs were not covered.

Criterion 28.1 -

a) Gambling houses including casinos are required to be authorised/licenced before conducting activities by the governance body (the FTS) of the gambling zone (art. 13 L244) and can be opened exclusively in gambling zones (art. 5 L244, there are five in Russia).

b) Legal entities whose founders (shareholders, including directly or indirectly owns not less than 10 percent share in charter capital or voting shares) are persons having an outstanding conviction for crimes in the field of economy or deliberate crimes of medium gravity, grave crimes or especially grave crimes cannot act as organisers of gambling activities (Art.6(2) L244). However, there are no legal or regulatory requirements to prevent criminal associates from being the BO (besides the above mentioned person) of a significant controlling interest, or holding a management function, or being an operator of a casino.

c) The FTS exercises control and supervision over AML/CFT compliance of organisations carrying out gambling (art.5.3.8 GR506), including all casinos (art.4 para.12 L244).

Criterion 28.2 - The following institutions are responsible for the regulation or supervision of the AML/CFT compliance of the obliged DNFBPs:

- **Real estate agents:** Rosfinmonitoring is responsible for registration (para.2 GR58) monitoring, conducting visits and imposing sanction (art.7 RFM 191).
- **DPMS:** Assay Chamber oversees compliance of DPMS, jewellery made by them and scrap thereof with the AML/CFT legislation (article 15, 16.8 and 19.27 of RF Finance Ministry Order No.687; Chapter VII of L41)
- **Notaries:** Notarial Chambers (SRBs), exercise the AML/CFT control over the discharge of professional duties by notaries (art.34 L4462-1). The Notary Code requires all notaries to be members of a regional Notary Chamber.
- **Accountants (auditors):** Self-regulatory bodies of auditors (which are supervised by MoF, subpar. 5.3.30 GR329) are responsible for monitoring the activities of their members and carrying out external work quality controls of operations of auditors (art. 9 L315, art. 10 L307). The Federal Treasury (art. 10.1 of L307) conducts external quality assurance review of the work of auditors conducting mandatory audit (art. 5 para.3 L307). The scope of external work quality control is the observance of the requirements set out in the present Federal Law (art. 10, para 3 L307), including AML/CFT regulations.
- **Attorneys (barristers/solicitors):** The chambers of lawyers is responsible for AML/CFT control over lawyers (The decision of the Council of the Federal chamber of lawyers of Russia dated 04.12.2017).

- **Legal Professionals:** There is no specifically appointed AML/CFT supervisor for legal professionals. Russia indicated that the General Prosecution Office (GPO) exercises AML/CFT supervision of this sector under its general responsibility for monitoring observance of the Constitution of Russia and execution of the laws in Russia, and governing bodies and heads of commercial and non-profit organizations (art. 21 L2202-1). However, the GPO's supervision is general and aims at overseeing the implementation of laws by government bodies and heads of commercial and non-profit organizations, and not specifically for AML/CFT supervision on legal professionals.
- **TCSPs:** Services to trusts and companies not regulated for AML/CFT purposes (see c.22.1(e) and therefore there is no assigned supervisor..

Criterion 28.3 - Russia identifies other categories of business and entities subject to the AML/CFT Law. Pawnshops are regarded as non-credit FIs, and the BOR is responsible for monitoring compliance with AML/CFT requirements. FTS exercises AML/CFT control and supervision over organizations conducting lotteries, sweepstakes, bookmakers and other risk-based games. Rosfinmonitoring is responsible for registration and exerting controls over the fulfilment of AML/CFT requirements on organisations which carry out transactions in amounts of money or other property (GR58 article 1 and PD808 part 5-1).

Criterion 28.4 -

a) Rosfinmonitoring, the Federal Treasury and SRBs have adequate powers to supervise DNFBPs, including to monitor compliance (article 10, para 2(1) L307; article 9, para.1 of L315). RFM191 art. 7; Article 26 and 26.1 of L41; article 7 and 33.1 of L4462-1; article 9, para.1 of L315; chapters 9 and 10 of the Code of professional ethics of notaries).

b) There are some measures to prevent criminals from being professionally accredited, or holding significant ownership or controlling positions in for lawyers, notaries, accountants, DPMS, auditors and real estate agents. This is achieved by excluding persons with outstanding convictions for any, or a selection of, crime (art.3, 4, and 18 of L307; article 2 of L4462; article 9, para.2, and art.17 para 1(4) of L63-2); GR 1052, para 9, sub para c and para 13 "e"; art. 22.1 L129; para.19 RFM 33). Rosfinmonitoring receives electronically information from MoI, however, there is no mechanism in Rosfinmonitoring to check the criminal record in a timely basis when owners, BOs, or controlling position change. There are no mechanisms to accredit legal professionals or to prevent them from being owned or controlled by criminals.

c) Supervisors of DNFBPs have sanctions available to them in line with R.35 to deal with violations of AML/CFT requirements (arts 13 and 20 L307; art.17, art.33 (7) of L63-2, art.4 of L64, art.18(6) Code of professional ethics para.9 and 10 of the Code of Professional Ethics of Notaries; art.15.27 (1-3), art. 23.1(1), art. 28.3(5) CAO; para.57 RFM191).

Criterion 28.5 - Authorities supervising DPMS, gambling organizations (including casinos) and intermediaries in the real estate market, use risk assessment models that take into account many criteria (such as characteristics and activities and numbers of the entities, the types of operations, and the level of implementation of preventive measures). Supervisors of notaries, lawyers, and auditors, alone or jointly with

Rosfinmonitoring, conducted SRAs, which have determined a series of unscheduled AML/CFT inspections, and supervisors of auditors issued guidelines for monitoring compliance of audit organizations using RBA. In order to determine the frequency and intensity of AML/CFT supervision these DNFBP supervisors use, when relevant, the results of national and SRAs, but mainly information on possible violations identified through documentary verification or from Rosfinmonitoring. There is no risk-based AML/CFT supervision of legal professionals.

Weighting and Conclusion

With the exception of TCSPs and legal professionals, DNFBPs are subject to regulation and active supervision by the competent authorities and SRBs. Deficiencies include a lack of provisions establishing or measures conducting the risk-based approach in supervision especially for lawyers and notaries.

Recommendation 28 is rated largely compliant.

Recommendation 29 - Financial intelligence unit

In the last MER, Russia was rated largely compliant with former R.26. Deficiencies included: a limitation in the reporting obligation for STRs; lack of a requirement to report on attempted suspicious transactions by occasional customers; and no STR requirements in cases involving insider trading and market manipulation (these two offences were not included as predicated offences).

Criterion 29.1 - Rosfinmonitoring is responsible for countering ML, TF, and PF, and participates in activities to counter corruption (art.1 PD808; art.5(4.1) PD808 for corruption). Rosfinmonitoring is the "national centre for assessment of the threats to national security arising from the performance of transactions in monetary funds or other property, and the elaboration of measures for countering these threats" (art.1 PD808). It is responsible for receiving and analysing STRs, MCRs, and other information relevant to ML, predicate offences and TF (art.5 (4-6) PD808). It is also authorised to disseminate (proactively or upon request) the results of its analysis to LEAs, if there are sufficient grounds to believe that a transaction is linked to ML and TF (art.5 (17) PD808). Similarly, it is authorised to disseminate information on transactions to counter corruption (art.5 (17.5), and inform the MoJ about a NPOs' failure to comply with its financial obligations (art.5. (17.4)

Criterion 29.2 - Rosfinmonitoring is the central agency for the receipt of disclosures filed by all reporting entities, including:

a) STRs filed in accordance with R.20 and 23 (art. 7(2) and (3); art.7.1(2) and (2.1) L115).

b) Rosfinmonitoring receives other disclosures from reporting entities on transactions subject to mandatory control reporting, including: cash transactions equal to or exceeding RUB 600 000 (approx. EUR 8 000), including transactions in foreign currencies (art.6(1) L115); bank account transactions, including transactions related to an account owned or controlled by a person or entity linked to a higher risk country as identified by the FATF; opening a bank account for a third person while making a deposit in cash; transactions in moveable assets, including the placement of

precious metals and stones, jewellery and scrap of jewellery or any other valuables in a pawnshop and the transfer of money by non-credit institutions upon a customer's request; transactions in immovable assets which results in the transfer of ownership, if the amount is equal to or exceeds RUB 3 000 000 (approx. EUR 40 000); transactions to NPOs from foreign states and citizens if equal to or exceeding RUB 100 000 (approx. EUR 1 340); and further reports as outlined in Article 6 L115.

Criterion 29.3

a) Rosfinmonitoring is able to obtain and use additional information from reporting entities (art.5 (5.1) PD808). BoR further expands on the information that can be obtained from FIs, which captures information on CDD, and supporting information (BR600). Penalties exist for non-submission of the requested information by Rosfinmonitoring, ranging from RUB 30 000 to 50 000 (EUR400-670) for natural persons, and RUB 300 000 to 500 000 (EUR4 000-6 700) for legal persons (art.15.27(2.3) CAO). Two regulations (applying to organisations, individual entrepreneurs and pension funds) issued in 2014 further establish the requirements to submit information to Rosfinmonitoring (GR209 and GR630).

b) Rosfinmonitoring (including all regional departments) has access to a vast range of information and intelligence to properly undertake its functions. In addition to the wide-breadth of information that must be submitted to Rosfinmonitoring [see c.29.2(b)], as well as the information that must be provided upon request [see c.29.3(a)], Rosfinmonitoring has direct access to the databases related to criminal justice and law enforcement, statistical reporting, and various registries including the NPO and reporting entities registries.

Criterion 29.4

a) Rosfinmonitoring is authorised to conduct operational analysis based on information received from reporting entities and other available information, in order to identify instances of ML/TF (art.5 (4-7, 12) PD808).

b) Rosfinmonitoring is authorised to conduct strategic analysis, specifically, to "organise and/or support scientific and scientific-research activities in the area of ML and TF…" (art.5(24.2) PD808). Furthermore, Rosfinmonitoring is empowered to evaluate ML and TF risks, and disseminate the results of its analysis, as well as conduct analysis and forecasts to counter ML and TF (art.5(16.1 and 12.1) PD808).

Criterion 29.5 Where there is reason to believe that a transaction relates to ML or TF, Rosfinmonitoring forwards all relevant information, with disclosure of banking secrecy, to LEAs (Federal Law 115-FZ, Art. 8). Rosfinmonitoring can also respond to LEA requests without disclosing banking secrecy (Federal Law 115-FZ, Art. 9); these reports summarise material and permit the LEA to conduct additional investigative steps.

Rosfinmonitoring uses dedicated, secure and protected channels for dissemination (art.5 GR630). Employees of Rosfinmonitoring must protect information and may be liable if such information is disclosed publically (art.22 GR209).

Criterion 29.6

a) Employees of Rosfinmonitoring "must observe the principle of non-disclosure of the information classified as service, banking, tax, commercial secret or secret of communication" that comes to their knowledge in connection in fulfilment of their functions. The penalty for such disclosures range from "a fine in the amount of up to RUB 500 000 (EUR 6 840) or in the amount of the convicted person's wage/salary or other income for a period of up to one year, or by corrective labour for a term of up to one year, or by compulsory labour for a term of up to two years, or by imprisonment for the same term." (art.183 CrC; art.8 L115). This prohibition is mirrored in other regulations (e.g. art.23 GR209).

   Russian law provides for the protection of confidential information and information constituting state secrets (art.16 L149; art.4 L5485-1). General provisions exist to restrict access to sensitive information, "to prevent unauthorised access to information and/or transfer of information to persons have no right to the access to information". L115 contains specific requirements on employees of Rosfinmonitoring to observe the principle of non-disclosure of classified information obtained in the course of its activities (art.8 L115).

b) Legislation exists related to provision of security clearances to all Russian public servants to access state secrets, which is "carried out by the security bodies at the location of organisations and of their territorially detached units" (art.8 GR63). Russia has general provisions to protect information constituting state secrets and confidential information (art. 9 and 15 L149; art. art. 6 pars. 2 and 4 L152; art.25 L5485-1). Moreover, the Federal Service for Technical and Export Control issued an Order to protect data in IT systems that do not constitute a state secret (FSTEC17).

c) Personalised access privileges to the buildings and databases of Rosfinmonitoring are used to implement differentiated access to confidential information so that employees can only use those components of the system that are relevant to their official duties. Requirements are applied to technical devices, program components, and a unified key-card is used to access office space and computers.

Criterion 29.7-

a) Rosfinmonitoring is "a federal executive governmental body" responsible for AML/CFT and participating in the countering of corruption (art.8 L115; art.1 PD808). The Director of Rosfinmonitoring is appointed by the President of Russian, and the FIU performs its activities directly and/or through its territorial bodies, or in interaction with other federal executive power bodies, local self-government bodies and public entities (art.10 and 4(1-2) PD808).

   This Presidential Decree states, "the activity of [Rosfinmonitoring] is guided by the President of Russia". However, the decree further states that the Director of Rosfinmonitoring is personally responsible "for the exercise of the powers" entrusted to the FIU (art.10 PD808). Russia's primary AML/CFT legislation does not place conditions on Rosfinmonitoring, or include reference to a role of the President in the activities of the FIU. Instead, art.8

states that Rosfinmonitoring "…shall be a federal executive body for which the tasks, functions and powers in the field of countering the legalisation (laundering) of proceeds from crime, financing of terrorism and financing of proliferation of mass destruction weapons are established under the present Federal Law". Furthermore, an additional regulation states that federal executives "enjoy independence in discharging functions and powers vested in it by federal laws and legislative acts…" (para 1.3 GR30).

b) Rosfinmonitoring is able to make arrangements or engage independently with other domestic competent authorities or foreign counterparts on the exchange of information (art. 5 (15-16) and (21); art.6(10.1) PD808).

c) Rosfinmonitoring is a federal executive body and not located within any existing structure (art.1 PD808).

d) Rosfinmonitoring has its own resources, including financial and human resources to carry out its functions. The Director is responsible for approving the structure and resources of the central apparatus of Rosfinmonitoring and its territorial bodies (art.10 (8-10) PD808). The Director is also responsible for submitting budget proposals to the MoF for consideration in the draft federal budget (art.11 (8 and 11) PD808).

Criterion 29.8 - Rosfinmonitoring became a member of the Egmont Group in June 2002.

Weighting and conclusion

All criteria are met.

Recommendation 29 is rated compliant.

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

In the last MER, Russia was rated largely compliant with these requirements. Deficiencies related to effectiveness, although the report noted that some law enforcement authorities lacked sufficient knowledge of the ML provisions.

Criterion 30.1 – Various LEAs can identify and investigate ML offences including MoI, FSB, and the IC, which have ML units or dedicated experts within central, regional, territorial, or specialised departments. The operational units of the MoI that are authorised to perform criminal intelligence are mainly responsible for the investigation of ML, associated predicate offences, and TF investigations (CPC Art. 151(2), paras. 2-3).

The investigators of MoI are primarily responsible for investigating ML (CPC Art. 151(2), para. 3), although a preliminary investigation of ML may be undertaken by the investigators of the LEA which detects it (CPC Art. 115(5)). Other LEAs, such as the IC, may pursue an ML investigation under the theory of "alternative jurisdiction" whereby the LEA charged with investigating a certain predicate offence would also take on the ML investigation associated with it. The FCS may also render assistance in ML or TF investigations related to crimes falling under its jurisdiction or items moved across borders (Federal Law 311-FZ (2010), Art. 12).

Regarding TF, pre-investigations and public investigations are the responsibility of the FSB. The IC,[137] which does not conduct criminal surveillance, may conduct TF investigations once they are formally initiated (see CPC Art. 151(2) and Federal Law 40 (1995), Arts. 9.1 and 10, relating to the anti-terrorism and crime control missions of the FSB).[138] MoI also plays a role in suppressing TF (Order No. 340) and may detect violations of CrC Article 205.1, the main TF offence.

For ML, associated predicate offences, and TF, GPO prosecutors supervise the activities of operational agents and investigators (Federal Law 144-FZ (1995), Art. 21; CPC Art. 37; Federal Law 2202-1 (1992), Art. 30).

Criterion 30.2 – Operational agents that detect predicate offences and conduct criminal surveillance measures in the pre-investigation phase, as well as LEA investigators, are empowered to pursue related ML or TF offences and to conduct financial investigations regardless of where the predicate offence occurred (CPC Art. 38; Federal Law 144-FZ, Art. 6; Art. 2). An investigator looking into a criminal offence is also authorised to conduct a parallel financial investigation, assuming there is a financial element present.

All operational and investigative agents are expected to perform financial investigations. This diffusion of responsibility may result in fewer pro-active financial investigations if generalist investigators are not appropriately trained or incentivised to conduct parallel financial investigations or pursue ML related to predicate offences. Still, the operational units that detect ML would present their files to the investigators in an advanced state and they may be requested to conduct additional steps to shore up financial aspects by obtaining additional information. Powers of parallel investigation are available to investigators, and both operational agents and investigators work often with Rosfinmonitoring, which conducts the most intensive financial investigations and provides expertise, leads, and link/tracing analysis to LEAs.

While there is no law requiring a financial investigation in all scenarios in which proceeds may be generated, there is ample policy.

A prosecutor has the authority to transfer a criminal investigation from one preliminary investigation agency to another (CPC Art. 37(2), para. 12) and investigators may accept referrals or pass them on (CPC Art. 38). Investigators may also work in groups if a criminal case is complex. The decision to initiate a group and its composition is taken by the head of the investigative body (CPC Art. 163). The groups envisioned under Article 163 can be cross-agency or multi-disciplinary and may include investigators specialised in financial or asset investigations. PD 567 (1996) states that the various LEAs shall co-ordinate, including at the interregional level, including by establishing teams to conduct investigations into particular criminal offences and by sharing the capacity and capability of LEAs for joint training and workshops.

Criterion 30.3 – All operational field agents and investigators are competent to expeditiously identify, trace, and initiate freezing and seizing of property that is, or

[137] Federal Law 403-FZ (2010) lays out the structure and responsibilities of the Investigative Committee, the main federal body for criminal investigation.

[138] Prior to March 2015, CFT functions were exclusively assigned to the General Department for Combatting Extremism of the Interior Ministry.

may become, subject to confiscation or is suspected of being proceeds of crime. Federal Law 144-FZ states that the goals of operational search activities include identifying property subject to confiscation (Art. 2). The same law authorises the collection of information on assets held by the associates of persons who have committed terrorist acts and the proceeds of terrorist activity (Art. 7.6, para. 8). Article 6 of Law 144 permits a range of measures to be taken in the course of performing operational search activity—including measures enabling the identification and tracing of assets—such as examining items and documents, interrogating persons, making inquiries, and examining premises and means of transportation. The foregoing provisions empower all LEAs to perform criminal intelligence and surveillance operations.

Criterion 30.4 – Although tax authorities are not considered part of law enforcement, they do interact and exchange information with investigative bodies responsible for the investigation of ML, as well as Rosfinmonitoring (Federal Law 115-FZ, Art. 8). According to CPC Article 144(7), non-tax investigators who discover potential tax evasion offences must send a report to the superior tax authority within three days accompanied by relevant documents and a preliminary estimate of uncollected taxes. Within 15 days of receiving the report, the tax authority must affirm the tax crime violation and relevant amounts, state that inspection is still ongoing, or deny that there has been a crime committed in light of a lack of evidence (CPC Art. 144(8)). The investigator thereafter and within 30 days shall decide, based on the response from the tax authority or other information indicating the commission of an offence, whether to institute a criminal case (which may also examine the laundering of the proceeds of tax crimes).

Criterion 30.5 – The IC, which operates as Russia's anti-corruption LEA, is capable of investigating ML and TF related to corruption offences, including bribery and had powers to identify, trace, and freeze assets. Since the body that detects ML may pursue it—in addition to the departments of the MoI—the IC would have jurisdiction to investigate ML related to those offences within its jurisdiction (CPC Art. 151(2.1(a)) and (5)). TF investigations are also within the purview of the IC (CPC Art. 151(2.1(a)).

Weighting and Conclusion

Russia has designated LEAs responsible for conducting ML and TF investigations and they have the authority to develop financial investigations and pursue criminal and terrorist assets. The responsibility to conduct financial investigations is widespread, and without a policy urging competent authorities to conduct financial investigations in all appropriate circumstances, this diffusion may leave opportunities to properly investigate ML on the table.

Recommendation 30 is rated largely compliant.

Recommendation 31 - Powers of law enforcement and investigative authorities

In the last MER, Russia was rated compliant with these requirements.

Criterion 31.1 - LEAs have the power to use compulsory measures in the areas below and a variety of additional operational search activities are enumerated in Federal Law 144-FZ (1995), Article 6. Complying with investigative demands is obligatory for natural and legal persons (CPC Art. 21(4)) and failure to comply is an administrative offence (CAO Art. 17.7).

a) *Production of records held by FIs, DNFBPs, and other natural or legal persons* – Records pertaining to the existence, status, and balance of accounts belonging to natural persons and information on the transactions of legal persons can be obtained pursuant to Federal Law 395-1 (1990), Article 26. The head of an investigative body conducting a preliminary investigation may obtain this information without a court order (same if there is a criminal case open). For more detailed financial records, court authorisation must be obtained. An investigator must apply to a judge for permission to seize objects or documents containing information about citizens' deposits and accounts at banks and other credit institutions (CPC Arts. 29(2), para. 7; 183). Motions for a seizure order are heard in a closed session and without notice to the affected entity or customer (CPC Art. 165). In urgent circumstances, an investigator may issue a resolution to seize records, which must be ratified by the court within three days of the obtaining the records (CPC Art. 165(5)).

   Banks and CIs are obliged to provide information about assets seized or restrained in response to an inquiry from the court or an investigator with the appropriate judicial authorisation (CPC Art. 115(7)). Bank secrecy is no obstacle to the production of specified records (Federal Law 395-1, Art. 26). Records held by non-bank or credit entities or natural persons may be searched for and seized by investigators according to the procedures detailed in Chapter 25 of the CPC if they are not provided voluntarily upon request (e.g., CPC Art. 182(5), (9)).

b) *Search of persons and premises* – A search of premises is provided for under CPC Articles 182 and 183. Some searches can be conducted on an investigator's resolution, such as the search of a business premise, but the search of a home requires a court order in accordance with CPC Article 165. The search of persons is authorised by CPC Article 184. A crime scene, and items found there, may also be examined (CPC Art. 176).

c) *Taking witness statements* – Interrogations of persons may be conducted pursuant to CPC Ch.26. Witnesses are summoned by writ (CPC Art. 184) and interrogations may be recorded (Art. 185). Records of statements are signed by both sides (CPC Art. 190).

d) *Seizing and obtaining evidence* – Instruments, equipment, means of crime, objects, documents, valuables which may prove to be of importance to the criminal case, property received as a result of the commission of a crime, and other items which may serve as the means to expose the crime and to establish facts and circumstances, may be searched for and seized in

accordance with CPC Ch. 25. Information and documents held by the state shall be accessible to competent authorities (Federal Law 115-FZ, Art. 9).

Criterion 31.2 **–** Competent authorities are able to use a wide range of investigative techniques for the investigation of ML, associated predicate offences, and TF. An investigator may give written orders to operational agents, to be executed without fail, about conducting criminal intelligence and performing of specific investigative actions (CPC Art. 38, para. 4).

a) *Undercover operations* are allowable under Federal Law 144-FZ, Article 6 (denoted as "operational implanting").

b) *Intercepting communications* – Authorised interception includes the "bugging of telephone conversations" and gleaning information from communications channels (144-FZ, Art. 6, para. 10). CPC Article 186 states that wiretaps should be based on sufficient grounds to believe that the telephone or other conversations of the suspect, accused, or another person may contain information important to a criminal case. A court's permission to monitor and record discussions is required. (CPC Arts. 186(3), 165).

c) *Accessing computer systems* – The receipt of computer information is a permitted criminal intelligence activity per Article 6 of Federal Law 144-FZ.

d) *Controlled delivery* is authorised under Article 6 of Federal Law 144-FZ.

Criterion 31.3 **–** Russia has mechanisms in place to identify, in a timely manner, whether natural or legal persons hold or control accounts (Federal Law 395-1, Art. 26). LEAs may use Rosfinmonitoring resources to identify where a suspect banks, as Rosfinmonitoring provides indirect access to the FTS' registry of bank accounts. Seizures of bank records are considered by a judge in a closed court session, without prior notice (see c.31.1(a)). Banks and other entities may be prohibited from disclosing the information obtained or seized during an investigation (CPC Art. 161) and disclosure of the data of a preliminary investigation, in contravention of a lawful instruction not to disclose, is a criminal offence (CrC Art. 310).

Criterion 31.4 **–** Competent authorities conducting ML, predicate, and TF investigations are able to ask for all relevant information held by the FIU. The FIU must respond to the demands, orders, and inquiries of a prosecutor or investigator (CPC Art. 21(4)).

Weighting and Conclusion

All criteria are fully met.

Recommendation 31 is rated compliant.

Recommendation 32 – Cash couriers

In its last MER, Russia was rated non-compliant for former SR.IX (para.275-302). Deficiencies related to a lack of a clear power to stop or restrain declared cash or BNIs in case of suspicion of ML, customs declaration forms were not in line with the legal requirements, customs authorities did not keep all required data relating to ML/TF, there was inadequate co-ordination among relevant competent authorities, administrative fines for false or non-declarations were not dissuasive or effective, corruption affected the effectiveness, and failures under the SR.III had a negative impact.

Criterion 32.1 - Russia implements a written declaration system as required by the EAEU, which is comprised of Russia, Belarus, Armenia, Kazakhstan and Kyrgyzstan. Russia implements the EAEU CC when "goods" are physically transported across the custom borders of the EAEU. Goods are defined as "any movable property, including currency of the Member States, securities and/or currency assets, travellers cheques, electric power and other items in transportation equated to immovable property" (art.2(45) EAEU CC). This broad definition covers any moveable property, which is broadly in line with the definitions of currency and BNIs contained in the FATF Glossary.

The EAEU CC outlines when a declaration is required. Specifically, incoming/outgoing goods through the EAEU border, that are intended for personal use, listed in paragraph 1 of Article 260 of the EAEU CC (incl. cash and BNIs when equivalent value exceeds 10 000 USD in accordance with the exchange rate on the day of the submission of the declaration) are to be declared in a written form (art.256 and 260 EAEU).

As indicated above, this declaration system applies only to movements (both inward and outward) of cash and BNIs from and to the EAEU, meaning that only movements that cross the external borders of the EAEU are subject to the declaration requirements.

This deficiency is partly mitigated by border control measures by the Border Control Service of the FSB, which is in place at all Russian borders, including borders with EAEU member states. This includes surveillance, electronic scanning, and the use of service animals (para 11 GR50). Customs authorities also have the power to stop and search motor vehicles along the borders with EAEU members (art.261 L289).

Criterion 32.2 - Cash and traveller's checks are subject to a mandatory written declaration upon entry and exit from the customs union when the amount exceeds USD 10 000, or its equivalent value (art.260 (1.7-8) EAEU CC). Other monetary instruments must be declared regardless of the amount. Declaration is optional for the movement of cash and traveller's checks below USD 10 000 USD or equivalent. All travellers are required to complete a passenger custom declaration form when crossing the border of the customs union (art.260(14.17) EAEU CC).

As noted in c.32.1, there are no declaration requirements within the EAEU.

Criterion 32.3 - Russia does not implement a disclosure system.

Criterion 32.4 - Upon discovery of an incomplete, or false declaration, or non-compliance with the customs declaration obligations, customs authorities have the

right to request commercial, accounting documents, the certificate of origin of the goods (which includes currency and monetary instruments) and/or other documents and/or data, including the written explanations, necessary to establish the reliability and completeness of the information contained in the customs declaration (art.325(4) EAEU CC).

Criterion 32.5 - The EAEU CC states that the declarant is liable for failure to fulfil its custom declaration obligations (art.84(3) EAEU CC). Failure to declare or falsely declaring amounts of money in cash or monetary instruments by natural persons is as an administrative offence, resulting in a penalty of the amount under declaration or from one-half to two-fold of the amount of cash non-declared, and/or the confiscation of the cash or monetary instruments (CAO art.16.4). These administrative penalties are assessed as proportionate and dissuasive.

The illegal movement of cash or monetary instruments on a large scale[139] across the customs border of EAEU is punishable with: (1) a fine ranging from three-fold to ten-fold the amount of illegally moved money in cash; (2) and/or the value of illegally moved monetary instruments in the amount of the convict's wage/salary or another income for a period of up to two years; (3) or restriction of freedom for a term of up to two years; (4) or forced work for a term of up to two years (art. 200.1 CrC).

A provision also exists for aggravated circumstances when the illegal movement of cash or monetary instruments is committed by a group of persons and exceeds the equivalent to USD 50 000. In these cases the punishment ranges from a fine from 10-fold to 15-fold the sum of illegally moved money in cash and/or value of illegally moved monetary instruments; or in the amount of the convict's wage/salary or another income for a period of up to three years; or restriction of freedom for a term of up to four years; or forced work for a term of up to four years (art. 200.1(2) CrC). These criminal penalties are assessed as proportionate and dissuasive.

Criterion 32.6 - Customs authorities of EAEU Member States are required to "transfer the information received by them, including preliminary information, to state authorities of their state, if the specified authorities need such information to perform the tasks and to exercise the functions imposed on them under the legislation of that Member State, in the manner and in compliance with the requirements of the legislation of that Member State on protection of state, commercial, tax, bank and other secrets protected by the legislation of that Member State, or any other confidential information" (art.356(3) EAEU CC).

In the framework of the Agreement for Information Co-operation between the FCS and Rosfinmonitoring, customs authorities must provide information on transportation of cash and other monetary instruments by individuals through the customs border of the EAEU to Rosfinmonitoring (art. 2 Agreement between Custom

[139] According to Article 200.1 of RF Criminal Code, an illegal movement of money in cash or monetary instruments is committed on a large scale when the sum of illegally moved money in cash and/or the value of illegally moved monetary instruments exceeds the two-fold sum of money in cash and/or value of traveler's cheques permitted by the customs legislation of the Customs Union, and it is committed on an especially large scale when that sum exceeds the five-fold sum of money in cash and/or value of traveler's cheques permitted by the customs legislation.

Service and RFM). Moreover, customs authorities must provide information on residents included in "the list of persons (residents) performing dubious currency transactions".[140] This information must be provided through the databases of Rosfinmonitoring and FCS (art.3 Agreement between Custom Service and RFM).

Criterion 32.7- Interaction between Rosfinmonitoring and the FCS is based on the "Agreement on Information Co-operation", signed in September 2013. This agreement outlines and types of information and channels for exchange between these authorities. Additional co-operation exists between the FCS and MoI (Protocol 2013). Moreover, co-ordination amongst customs and other authorities is also achieved through the Interagency AML/CFT/CPF Commission, which is chaired by Rosfinmonitoring and includes representation from FCS.

Criterion 32.8- Article 3 of the Customs Union Treaty on AML/CFT requires the FCS to seize currency/BNIs on the basis of information provided to it by LEAs and/or other authorised parties, and shall promptly notify the authority that provided the relevant information. This article broadly covers the ability to restrain currency and BNIs based on false declarations, as the inaccurate information could be identified by LEAs, including the FCS. Article 2 of this Treaty states that when there is missing information in a customs declaration, the customs authority shall not allow the movement of currency or monetary instruments. Templates related to seized currency/BNIs have been established by the Eurasian Economic Commission Board (Resolution 37).

Criterion 32.9-

a) Documents needed for the conduction of customs control (which include custom declarations) must be kept for five years (art.320 EAEU CC).

b) In cases of false declarations, which would constitute an administrative or criminal offence, these declarations would be retained as part of the criminal record-keeping in Russia. The criminal/administrative offence records are held electronically, and are permanent.

c) Declarations that cause a suspicion of ML/TF are required to be disseminated to Rosfinmonitoring (Protocol 2013).

Criterion 32.10 - The information collected pursuant to the EAEU customs declaration obligation is subject to confidentiality (art.356 EAEU CC). Federal Law Nº 152-FZ of 27 July 2006 on Personal Data provides measures for ensuring the security of personal data when being processed (art.19). This law also obliges operators and other persons who have been granted with access to personal data to not disclose or distribute personal data to third parties without the consent of the personal data subject, unless otherwise provided by federal law (art.7). L289, on customs regulation in Russia and on amendments to certain legislative acts of Russia, establishes that information obtained and used by customs authorities must be used solely for the

[140] The Federal Customs Service is required to provide to Rosfinmonitoring information on participants of foreign trade activity, conducting suspicious transactions in a view of the currency legislation, related to inflow of goods that are not subject to customs or tax payments (Protocol no.2 of 2018 between Customs and RFM).

tasks and functions assigned to them, and is not subject to transfer to other persons and use for other purposes (art.311).

Criterion 32.11 - The illegal movement of cash or monetary instruments on a large scale[141] across the customs border of EAEU is punishable with: (1) a fine ranging from three-fold to ten-fold the amount of illegally moved money in cash; (2) and/or the value of illegally moved monetary instruments in the amount of the convict's wage/salary or another income for a period of up to two years; (3) or restriction of freedom for a term of up to two years; (4) or forced work for a term of up to two years (art. 200.1 CrC).

If the illegal movement of cash or monetary instruments was not committed on a large scale, it is considered an administrative offence (art.16.4 CAO). The administrative penalty may be in the amount "from one-half to two-fold amount of cash non-declared and/or the value of monetary instruments or confiscation of the subject of the administrative offence".

Penalties for ML and TF may be applied to persons who are carrying out a physical cross-border transportation of currency or BNIs only if their conduct otherwise qualifies as ML or TF. Equally, the penalties available for predicate offences may be applied should the transportation relate to a predicate offence.

The maximum penalties available for the most severe violation of the ML offences are a term of imprisonment of seven years and a fine of RUB 1 million (approximately EUR 13 680) or up to five years' salary or income (see also c.3.9).

Natural persons convicted of a TF offence are punishable by proportionate and dissuasive criminal sanctions of deprivation of freedom (imprisonment) for a term of 8 to 15 years with the possibility of a fine up to RUB 700 000 (approximately EUR 9 640) or 2-4 years' salary. A maximum sentence of life in prison is also possible for TF and there are certain enhancements in the range of potential terms of imprisonment for organising TF, financing an act of international terrorism, and financing an illegal armed group (art. 205.1(1.1) and (4), 208(1), 361(2) CrC).

The Criminal Code permits confiscation of money, valuables, or other property which are the subject of illegal movement across the customs border of EAEU or Russia with member states of the EAEU punishable under Articles 200.1, 200.2, 226.1 and 229.1 of this Code (art. 104.1(1a) and 200.1 CrC).Confiscation of cash or monetary instruments is permitted for an administrative offence (Art. 3.7 CAO).

[141] According to Article 200.1 of RF Criminal Code, an illegal movement of money in cash or monetary instruments is committed on a large scale when the sum of illegally moved money in cash and/or the value of illegally moved monetary instruments exceeds the two-fold sum of money in cash and/or value of traveler's cheques permitted by the customs legislation of the Customs Union, and it is committed on an especially large scale when that sum exceeds the five-fold sum of money in cash and/or value of traveler's cheques permitted by the customs legislation.

Weighting and conclusion

Russia has made significant improvements to R.32 since its last MER. However, Russia's declaration system applies only to movements (both inward and outward) of cash and BNIs from and to the EAEU, meaning that only movements that cross the external borders of the EAEU are subject to the declaration requirements.

Recommendation 32 is rated largely compliant.

Recommendation 33 – Statistics

In the last MER, Russia was rated largely compliant with former R.32, as not all authorities kept quality statistics on matters relevant to the effectiveness of the AML/CFT system.

Criterion 33.1 - Current regulatory arrangements provide for maintaining of comprehensive AML/CFT-related statistics, as follows:

a) *STRs, received and disseminated*

Rosfinmonitoring maintains detailed statistic on STRs received from reporting entities and disseminations to competent authorities (PD, N.808, Art.5, Para.4).

b) *ML/TF investigations, prosecutions and convictions*

MoI collects and maintains statistics on, *inter alia,* criminal offences, crime rate and outcomes of investigations (GO No. 671, Section III). The GPO does the same for investigations and inquiries, crime reports and corruption-related offences by the (Subsection 62), while data on convictions (valid court judgments) for all crimes achieved at all courts is collected by the Judicial Department under the Supreme Court (Subsection 64). Relevant decrees and orders define the (template) forms, as well as the procedures for and the periodicity of generation and submission of statistical information. All statistical reports on prosecutions (including on number of convictions for ML and TF-related criminal offences), as well as statistical reports from the federal database are publicly accessible on the Internet.[142]

c) *Property frozen, seized and confiscated*

Statistics on frozen and seized property (assets) is maintained by the MoI, the FSB and the IC in accordance with their area of competence. The aggregate data provided by these agencies is used to produce a report on voluntary compensation of inflicted losses (damage), on property, funds and valuables that are frozen, and on the value of seized assets. Since 2017, this report also provides data on ML-related criminal offences, amounts of laundered proceeds of crime, as well as on frozen and seized property, funds and valuables. The Federal Bailiffs Service collects its own data on recovery of criminal and administrative fines, recovery of losses (damage) and confiscation of property and funds. The Federal Agency for State Property Management registers and keeps records of confiscated property. The FCS

[142] E.g., www.cdep.ru for information on convictions; www.FSBprus.ru for information on enforcement of judicial acts, etc.

maintains data on the disposal of property forfeited to the state due to customs-related crimes.

d) *Mutual legal assistance or other international requests for co-operation made and received*

Relevant MLA and international co-operation statistics, including ML and TF, are maintained by the: Supreme Court, MoJ, IC, the MoI and the FSB, and the GPO (CPC, Art. 453, Para 3). Rosfinmonitoring maintains statistics on information exchanges with the foreign counterparts and non-counterparts, in accordance with the relevant orders of the Director of Rosfinmonitoring.

Weighting and Conclusion

All criteria are fully met.

Recommendation 33 is compliant.

Recommendation 34 – Guidance and feedback

In its last MER, Russia was rated partially compliant with former R.25. Most deficiencies were later addressed, as noted in follow-up reports.

Criterion 34.1 **-** Rosfinmonitoring issued informational letters and methodological recommendations with guidance on the implementation of related Federal Laws, and on monitoring and reporting transactions to FIs and DNFBPs. Rosfinmonitoring has published about 40 informational letters for the private sector since 2013. Meetings and other outreach events are held to improve compliance of FIs and DNFBPs.

Methodological Recommendations (with detailed description of the characteristics of suspicious customers or transactions) and guidelines (such as approaches to risk assessment management in the AML/CFT sphere) are issued by the BOR to both CIs and non-CIs. In addition, meetings, informational and educational events are held by BOR to raise awareness of risks and to discuss on monitoring suspicious transaction.

For the DNFBPs sectors, Assay Chamber of Russia jointly with Rosfinmonitoring issued an Information Letter for DPMS explaining the procedure for identifying certain categories of transactions and filing the relevant STRs Rosfinmonitoring has also issued an Information Letter on application of provisions of L115 for legal or accounting services (RFM 54). Methodological Recommendations on the fulfilment of the AML/CFT Law by lawyers (e.g. RFM 60), auditors (e.g. RFM 56) and notaries (approved by the FTS on24 August 2009) were issued by Rosfinmonitoring and/or jointly with supervisory authorities to improve AML/CFT performance of entities.

Regulators supplement their guidance with training, conferences, bilateral engagements and other outreach activities. For example, specialists from entities had been provided training through the International Training and Methodology Centre for Financial Monitoring and the International Network AML/CFT Institute. Meetings and other outreach activities are also held by regional offices of Rosfinmonitoring in order to clarify requirements and to assist entities in applying AML/CFT measures. The Advisory Board and Compliance Council, and the Personal account on the Rosfinmonitoring website, are used as mechanisms of communications with the

private sectors. The BOR regularly participate in various meetings, conferences and seminars organized by industry associations.

Feedback on the quality of STRs is given in a general way: i) Supervisory authorities issue information letters on the shortcomings of the STR sand how to improve them, ii) "Thank-you letters" were given to entities when the STRs were used during financial investigations, and iii) related talks during Compliance Councils meetings. However, no specific feedback on the quality of individual STRs is given to reporting entities.

Weighting and conclusion

Overall, the guidance provided by competent authorities, supervisors, and SRBs is adequate. However, no specific feedback on the quality of individual STRs is given to reporting entities.

Recommendation 34 is rated largely compliant.

Recommendation 35 – Sanctions

In the last MER, Russia was rated partially compliant with former R.17. Deficiencies included: low maximum fines; and lack of powers for supervisors to withdraw a licence when the owners are convicted of a relevant criminal or economic offence, or to replace directors and senior management.

Criterion 35.1 **-** Under article 13 of the AML/CFT law, licenced entities (for credit institutions, Law on BoR, article 74) in breach with the provisions of Articles 6, 7, 7.2, 7.3 and 7.5 (except for article 7 para 3) of the AML/CFT law may cause revocation (annulment) of the licence in the manner envisaged by Russian law. Natural persons guilty of breaching AML/CFT law shall be liable under the administrative, civil and criminal law of Russia. Legal persons bear no criminal responsibility. There are administrative sanctions available for supervisory authorities under Code of Administrative Offences and specific federal laws, as explained below.

Financial sector **–** Sanctions depend on different types of violations in article 15.27 of the Code of Administrative Offenses, administrative fine from RUB 50 000 to 1 000 000 on legal entities and a fine from RUB 10 000 to 50 000 or disqualification for a term of one to three years on officers can be imposed by BOR on natural or legal persons, except for credit organisations which have limited administrative liability pursuant to the Notes of article 15.27. Warning and suspension of activities for a period up to 60/90 days can also be imposed. Supervisors have the right to order the elimination of the offense, and failure to do so carries administrative liability (art. 19.6). Sanctions imposed on AML/CFT offenses are proportionate compared to other similar offenses, but the maximum fines that can be imposed on entities and officials are low, limiting their dissuasiveness. The suspension of activities, revocation of licence, and disqualification of officers increase the dissuasiveness.

A credit institution which fails to execute orders of the BOR to correct deficiencies within the prescribed time period may face a penalty of up to 1 percent of the size of the paid-up share capital, or the BR may order re-organisation, replacement of persons, or issue a ban on individual types of banking operation for a period of up to one year (according to article 74 of L86).

For non-credit institutions, in case of deficiencies or non-fulfillment of BoR orders, BoR can impose sanctions in the form of restrictions and prohibitions such as ban from raising funds, issuing loans, or accepting new members on consumer credit cooperatives, and comparable restrictions on other types of NCIs.

In the case of repeated violations of TFS, licences of FIs can be cancelled or suspended.

BoR can impose an administrative fine on legal entities of RUB 10 million to 60 million if they violate the provisions on financial support to terrorism (article 15.27.1).

Roscomnadzor can issue warnings, suspend the licence for failure eliminate the identified violation, and revoke the licence for failure to eliminate the circumstances that caused the suspension of the licence, within the established period (Art. 37, Art. 39 L126). It can also consider cases of administrative offences provided for in parts 1-3 of article 15.27 CAO, according to article 23.44 of the same Code.

DNFBPs – Notaries who fail to report suspicious transactions face are subject to the disciplinary procedures of the Board of the Notary Association. No other sanctions are available for notaries. Lawyers can face disciplinary sanctions (including remarks, warnings, and terminating their professional status) if they are found in breach of the norms of the code of professional ethics, (L63-2, article 17, article 33, para.7, article 4 of L64, article 18 of the Code of professional ethics of lawyers). Auditors who violate AML/CFT requirements can face sanctions ranging from warnings, orders to remedy the breach, fines, and suspension or cancellation of their professional status. Real estate agents, dealers in precious metals and stones and casinos are under the scope of AML/CFT obligations and sanctions can be imposed in accordance with article 15.27 CAO as equivalent to FIs.

NPOs – Possible sanctions on NPOs include: warnings, instructions to eliminate deficiencies, suspension of activity, imposition of administrative liability, and liquidation of NPO can be imposed depending on the violations(article 32(5.5) of L7, art.42 of L82, articles 19.7.5-2, 19.34, 20.28 CAO article 61(para. 3) CC).

TFS violations – FIs and DNFBPs which violate TFS obligations can be fined from RUB 300 000 to 500 000 (from EUR 4 000 to 7 000) or face administrative suspension of activity for up to sixty days and officials in the amount of RUB 30 000 to 40 000 (EUR 400 to 700). These sanctions are too low to be dissuasive. As noted under R.6, there is no penalty available for natural and legal persons.

Criterion 35.2 - Sanctions are applicable to officers (including directors and senior management) according to article 15.27 CAO.

Weighting and Conclusion

Financial supervisors have adequate powers to impose a broad range of sanctions for both natural and legal persons. Even if there is a broad range of sanctions applicable to credit institutions, the monetary sanctions are not fully dissuasive. The penalties related to TFS violations are not sufficient to be proportionate and dissuasive.

Recommendation 35 is rated largely compliant.

Recommendation 36 – International instruments

In its last MER, Russia was rated largely compliant with these requirements. The main deficiency was that the TF offence did not extend to the theft of nuclear material as required by the TF Convention.

Criterion 36.1 – Russia has become a party to the four required conventions.[143]

Table 36.1: Signature and Ratification

Convention	Signed by Russia	Ratified by Russia
U.N. Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention)	19 January 1989 (signed by predecessor State)	17 December 1990 (ratified by predecessor State)
U.N. Convention against Transnational Organized Crime (Palermo Convention)	12 December 2000	26 May 2004
U.N. Convention against Corruption (Merida Convention)	9 December 2003	9 May 2006
International Convention for the Suppression of the Financing of Terrorism (TF Convention)	3 April 2000	27 November 2002

Criterion 36.2 – Since its last MER, Russia criminalised the theft of nuclear material or radioactive substances (CrC Arts. 220-221) to comply with the Convention on the Physical Protection of Nuclear Material, and, in turn, the TF Convention. However, minor legal gaps preclude Russia from full implementation of the TF Convention (see analysis of c.5.1 and c.5.2). There are minor shortcomings in the criminalisation of ML (see analysis of c.3.1), which impact the full implementation of the Vienna and Palermo conventions. The crimes set out in the mandatory articles of each of the four conventions, as listed in footnote 71 of the FATF Methodology, are generally addressed in the Russian Criminal Code. Shortcomings analysed in R.12 pertaining to the requirements for FIs to identify PEPs and perform EDD impact the full implementation of the Merida Convention.

Weighting and Conclusion

Minor deficiencies in compliance with R.3 and 5 result in minor shortcomings in 36.2.

Recommendation 36 is rated largely compliant.

Recommendation 37 - Mutual legal assistance

In its last MER, Russia was rated largely compliant with these requirements due to issues of effectiveness.

Criterion 37.1 – Russia has a number of legal bases that allow it to rapidly provide a wide range of (MLA in relation to ML, associated predicate offences, and TF investigations, prosecutions, and related proceedings. CPC Chapter 53 is the principal domestic framework and the procedures of the requesting state or of the applicable treaty may be applied if they do not contradict domestic law. The courts, prosecutors, and investigators are charged with executing requests from foreign competent authorities (CPC Art. 457). The authorities of a requesting state may be present when

[143] Russia has made declarations and notifications to the Palermo and Merida conventions relating to jurisdiction and co-operation. Russia made a declaration upon signing the TF Convention related to co-operation. These declarations do not appear to impact implementation in any negative way.

the actions requested are carried out on its behalf. Assistance may be provided on the basis of the treaties of Russia or reciprocity. The AML/CFT law is an additional legal basis for Russia to provide MLA on either ground (Federal Law 115-FZ, Art. 10). This provision covers all stages of a case, from information gathering and preliminary investigation through litigation and execution of court judgments.

The range of available MLA is not enumerated under Russian law; therefore, the types of assistance available are determined by reference to the examples contained in international agreements or by reciprocity. Russia is a party to several multilateral conventions (and additional protocols) with non-exhaustive provisions on mutual legal assistance—such as the Palermo Convention—and instruments with specific provisions related to particular crimes. Russia has in place bilateral and regional agreements concerning MLA in criminal matters with more than seventy states.

Criterion 37.2 – Russia does not have one central authority for the transmission and execution of MLA requests and uses other established mechanisms. For outgoing MLA, the following entities transmit various types of requests pursuant to CPC Article 453:

Table 37.1: Authorities Involved in Outgoing MLA

Supreme Court	Requests involving the judicial activity of the Supreme Court
MoJ	Requests involving the judicial activity of all courts except the Supreme Court
IC; Interior Ministry; FSB	Requests involving criminal cases under the jurisdiction of each respective agency
GPO	All other requests

For incoming MLA, GPO is charged with maintaining direct relations with its counterparts abroad and cooperating with them (Federal Law 2202-1 (amended 2017), Art. 2). GPO Order No. 68/35 (2009) sets out procedures that should be followed by the Russian prosecution authorities for reviewing and executing MLA requests at the investigative (pre-judicial) stage. For MLA in criminal matters related to the Palermo Convention, the Merida Convention, the COE Convention on Criminal Responsibility for Corruption, and the OECD Anti-Bribery Convention, the GPO is the designated central body. For MLA in criminal matters relating to the Minsk Convention—an agreement among Russia and its CIS neighbours—incoming and outgoing requests for MLA go directly to and from competent authorities (PD 170 (2017)). For incoming MLA at the post-investigative (judicial) stage, the MOJ is competent to execute requests. Within GPO, the GDILC reviews requests for treaty compliance, refers them for execution, and tracks and provides updates.

On prioritisation and timely execution, according to GPO Order No. 68/35 (2009), Article 1.3.8, and GPO Order No. 67 (2009), Article 2.5, the GPO shall ensure and monitor the timely and proper execution of requests. As a matter of practice, Russian authorities state that MLA requests are executed on a first-come, first-served basis, that urgent requests can elicit immediate action, and that special attention is paid to requests related to terrorism, TF, economic crimes, drug trafficking, and requests which may prompt the opening of a domestic criminal case under CPC Articles 144-145. There is a minor deficiency in that this stated policy on MLA request prioritisation is not articulated in a handbook, process, plan, or guidance used by GPO or GDILC in conducting its day-to-day activities. Instead, guidance is provided at

higher level, through agency and national strategic documents.[144] The GDILC does have an internal order for the processing and timely execution of requests dealing with identification and seizing of assets (GDILC Order No. 2 (2016)). GPO Order Nos. 67 and 68/35 state that requests should be executed in a timely manner with prompt investigation, and that GPO should monitor the timeliness and completeness of execution. Under c.37.2, there is a clear process for timely execution, but less clarity on prioritisation.

GPO Order No. 450 (2011) sets the procedures for document management and record-keeping in the GPO. GPO implements a hardware and software infrastructure and a system called AIC Supervision, which contains information about all documents, correspondence, and movement of case documents, and is used to monitor progress on requests. GPO Order No. 105 (2012) requires generation of reports on the results of GPO's MLA interactions every six months. These reports enable a holistic view of requests processed by Russia, and the pace and productivity of co-operation efforts as a whole. GDILC Order No. 2 (2016), requires similar data to be separately recorded on requests related to confiscation. There is a small deficiency in that the case management system does not have capability to prompt action on particular cases, such as through electronic reminders.

Criterion 37.3 – Requests shall be returned unexecuted if providing the assistance sought would contradict the legislation of Russia or if it may inflict damage upon Russia's sovereignty or security (CPC Article 457(4)). Thus, the formal grounds to deny assistance are limited and Russia's reason for a refusal must be explained to the requesting state. This does not constitute an unreasonable or unduly restrictive condition on the provision of MLA.

Criterion 37.4 – The only grounds to refuse a request are detailed in c.37.3, so Russia will not refuse a request for MLA solely on the basis that the offence involves fiscal matters or on the grounds of secrecy or confidentiality requirements on FIs or DNFBPs. Certain confidential information and professional secrets are protected, but there are procedures by which such material can be accessed by LEAs. Banking secrecy is no obstacle (Federal Law 395-1 (1990), Art. 26).

Criterion 37.5 – Competent authorities engaged in AML/CFT activities must ensure the confidentiality of information furnished in MLA requests and use it only for the purposes specified (Federal Law 115-FZ, Art. 10). Russia's multilateral conventions and most treaties have confidentiality articles that can be invoked by the requesting or requested state. Two GPO documents also require strict observance of treaty requirements and the CPC, unless a treaty stipulates otherwise (GPO Order No. 68/35, Art. 1.2.1, and GPO Order No. 67, Art. 1.2). Federal Law 149-FZ (2006) governs data

144 For example, MoI, in its annual directive for 2018, has made improving the efficiency of international co-operation related to provisional measures, confiscation, and compensation of damages a major priority (MoI Directive No. 1 (2018)). Similarly, in IC Order No. 6 (2018), management is instructed to ensure that subordinates provide timely and high-quality execution of foreign requests assigned to the IC. GPO Order No. 292/86r (2016) established a working group on the recovery of the proceeds of domestic corruption offences from abroad. This working group is tasked to, among other things, improve Russia's efficiency in seizing and confiscating assets located abroad. These documents underscore the importance of mutual confiscation assistance, but they message policy on prioritisation, not process.

protection and dissemination of information on or from IT systems. There are sufficient safeguards to maintain the confidentiality of requests in order to protect the integrity of ongoing investigations or inquiries. CPC Article 161 prohibiting disclosure of investigative information also applies to the execution of MLA requests.

Criterion 37.6 – Where MLA requests do not involve coercive actions, Russia does not make dual criminality a condition for rendering assistance.

Criterion 37.7 – Dual criminality is required for MLA involving coercive actions such as search and seizure of property. For extradition, there is an explicit dual criminality requirement in the CPC for outgoing requests: Russian law requires a description of the "actual circumstances and the legal qualification of the act" (CPC Art. 460(4.3)). Although there is not a corresponding instruction for the consideration of an incoming extradition or MLA request, the focus of the dual criminality analysis, by analogy, appears properly focused on the "acts" not the "offence" and its precise name or categorization (CPC Arts. 462(3.1), 464(1.6)). There is flexibility for Russian authorities to examine the actual circumstances, or the conduct, underlying a request, whether for extradition or MLA. Minor gaps in the criminalisation of ML and TF may affect the dual criminality determination by Russian authorities (see analysis of criteria 3.1, 3.4, 5.1 and 5.2), however, this is judged to be a minor shortcoming due to the low likelihood of a request that would implicate the exact deficiencies in the domestic ML/TF offences and the possibility that the conduct may qualify as another crime under Russian law such that dual criminality could be satisfied.

Criterion 37.8 – Competent authorities can utilise all powers specified under Recommendation 31 in response to an MLA request subject to the conditions under Russian law that would be in place in an equivalent domestic investigation.

Weighting and Conclusion

There are minor shortcomings in the clarity of processes for the prioritisation of requests and the sufficiency of the case management system to monitor progress on individual requests. The evaluation of dual criminality for coercive forms of assistance may, in rare cases, be impacted by minor deficiencies in the ML and TF offences, but the materiality of this gap is low.

Recommendation 37 is rated largely compliant.

Recommendation 38 – Mutual legal assistance: freezing and confiscation

In the last MER, Russia was largely compliant with these requirements, as minor deficiencies in the international co-operation framework affected freezing and confiscation.

Criterion 38.1 – Russia has the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize, and confiscate criminal assets to the extent permitted under domestic law. Dual criminality is required for MLA involving coercive actions such as search and seizure of property. As detailed in c.4.1(b), Russia has dual systems in place for confiscation of the proceeds of predicate offences: confiscation under the Criminal Code applies to the list of crimes specified in CrC Article 104.1(1)(a), including ML and TF, and confiscation under the Criminal Procedure Code applies the proceeds of a subset of predicate offences likely to result

in financial harm to victims, such as theft and fraud. There is only a minor limitation on Russia's legal ability to provide MLA in response to confiscation-related requests as a result of this split regime. The potential gap lies in confiscating corresponding value (c.38.1(e)) on behalf of another country if the dual criminality rests on an offence which, under Russian law, would only be forfeitable using the CPC, because the CPC does not have explicit provisions on substituting clean assets for traceable proceeds. Otherwise, property laundered (c.38.1(a)), proceeds (c.38.1(b)), and instrumentalities (c.38.1(c)-(d)) can be restrained, seized, or confiscated by Russia in response to foreign requests, including those based on multilateral conventions and Russia's international agreements specifically addressing confiscation-related co-operation.

The AML/CFT law further enables co-operation. Article 10 states that authorities engaged in combatting ML and TF shall meet requests to identify, freeze/seize and confiscate assets, including through the relevant investigative measures such as interrogations, searches, and seizures. In terms of identifying property connected with ML, predicate offences, or TF, Rosfinmonitoring is authorised to interact and exchange information with foreign competent authorities in conformity with the international treaties of Russia or on the basis of the principle of mutuality (PD No. 808 (2012), para. 5(15)). LEAs may carry out operational search measures (investigative activity), on the basis of requests from foreign law enforcement bodies (Federal Law 144-FZ, Art. 7(6)).

Confiscation of virtual assets (VA) is not yet possible under Russian law. Although Russia can investigate and trace VA, it can only seize or confiscate VA once converted into another type of property, both domestically and in the context of international co-operation.

Russia can enforce foreign confiscation judgments and sentences (Federal Law 115-FZ, Art. 11). Final decisions issued by foreign courts regarding persons having criminal proceeds shall be recognised, as well as final decisions concerning the confiscation of income derived through crime and property of equivalent value (CPC Arts. 473.1, 473.6(3)). CPC Chapter 55.1 details the procedures for the recognition of foreign judgments or sentences naming assets located in Russia. "[I]ncome derived through crime" is given the same meaning as in the CrC Article 104.1 (CPC Art. 473.1(3)). The importation of this definition impacts the scope of foreign judgments that could be enforced if the underlying offence is not listed in CrC Article 104.1(1)(a), as there some predicates missing from that provision, as noted in c.4.1. Notice to the person affected by the foreign decision and interested persons shall be provided and those parties may participate in the court's process of recognition, along with representatives of the foreign state (CPC Art. 473.4). Grounds for refusal to recognise a foreign confiscation judgment include a lack of dual criminality or finality (CPC Art. 473.5). Chapter 55.1 of the CPC does not permit enforcement of provisional measures; a conviction of guilt is necessary (CPC Art. 473.6(2)).

Criterion 38.2 – Russia has the authority to provide assistance to requests for co-operation made on the basis of non-conviction based (NCB) confiscation, at a minimum, where the perpetrator has died. Under SC Order No. 17 (2018), para. 13, it is possible to confiscate assets where a domestic criminal case is terminated on the basis of the death of the accused. When the death of the accused results in the closing of a domestic criminal prosecution, confiscation may go forward without a conviction.

Russia could provide similar assistance when a perpetrator is unavailable by reason of death and the foreign criminal prosecution has been terminated for this reason. It is not possible for a Russian court to issue a confiscation decision pursuant to SC Order No. 17, para. 13, where the foreign NCB proceeding is premised on an unknown perpetrator or a perpetrator who is unavailable by reason of flight or absence.

As detailed in c.4.1, Russia has some NCB confiscation powers in the areas of corruption and terrorism, but neither law mentions international co-operation. It is possible that Russia may be able to assist in MLA requests based on NCB proceedings involving corruption or terrorism that are coextensive with Russia's domestic legal authorities, but this is untested. While Russia can enforce a confiscation decision stemming from a criminal case, there is no similar authority for enforcement of a foreign NCB judgment (CPC Arts. 473.2(1.2), 473.6(2.3)).

Russian authorities contend that confiscation under the CPC Article 81 can be used for NCB assistance. The article requires the court to make a final determination, *regardless of conviction or acquittal*, about the fate of the material evidence kept in custody as part of the criminal case. On this basis, a court could confiscate or otherwise dispose of instrumentalities and proceeds, contraband, evidence, and items taken into custody during an investigation, even absent a conviction. Presumably, then, to provide MLA, Russia would have to open a domestic criminal case and then ask the court to confiscate assets as material evidence and not as a part of a punitive sentence. While this asserted legal authority has logical appeal, it is not enumerated in law, and the assessors could not credit this without examples of implementation. Therefore, a domestic proceeding pursuant to SC Order No. 17 would be Russia's main legal mechanism by which it could provide NCB assistance based on an MLA request, and this is definitive only as it relates to deceased defendants.

Criterion 38.3 – Russia has arrangements for coordinating seizures and confiscation actions with other countries. The CPC governs the execution of MLA requests, but the procedures of the requesting state or of Russia's treaties may be applied, and the authorities of a requesting state may be present in Russia when the actions requested are carried out on its behalf (CPC Art. 457(2)-(3)). Russia also applies the relevant provisions of relevant conventions (Merida, Art. 57 and Palermo, Art. 14). Russia applies its domestic mechanisms for managing, and when necessary, disposing of property frozen, seized, or confiscated pursuant to the request of a foreign state (see description in c.4.4). Federal Law 229-FZ (amended 2007), Article 104, also provides mechanisms for the Bailiff to take possession and dispose of property confiscated in execution of treaty obligations.

Criterion 38.4 – Russia is able to share confiscated property with other countries, in particular when confiscation is directly or indirectly the result of co-ordinated law enforcement action. Russia may transfer property in full or in part to a foreign state, including when it recognises and gives effect to a confiscation decision of a foreign court (Federal Law 115-FZ, Art. 11).

Weighting and Conclusion

Russia can provide MLA related to freezing and confiscation with minor shortcomings related to the confiscation of value corresponding to the proceeds of certain offences for which domestic confiscation relies on the CPC and related to the confiscation of virtual assets. There are also minor gaps in relation to the criminalisation of ML and

TF which may in rare circumstances preclude a finding of dual criminality. Russia can enforce conviction-based confiscation judgments from foreign courts, co-ordinate seizure and confiscation with other countries, and share confiscated assets. It can provide some assistance for NCB confiscation, i.e., in connection with deceased defendants. Overall, the weight of the shortcomings is minor.

Recommendation 38 is rated largely compliant.

Recommendation 39 – Extradition

In its last MER, Russia was rated largely compliant with these requirements. The main technical deficiency related to gaps in the criminalisation of ML and TF which could impede extradition in light of the dual criminality requirement. Those deficiencies were subsequently remedied by Russia's criminalisation of certain offences.

Criterion 39.1 – Russia is able to execute extradition requests in relation to ML and TF. Russia will extradite on the basis of an international treaty[145] or reciprocity (CPC Art. 462(1)). Decisions on extradition are made by the Prosecutor General (PG) or his or her deputy, and such decisions are appealable to a court (CPC Arts. 462(4)-(5), 463). The PG has discretion over which request to grant when multiple states seek extradition of the same person (CPC Art. 462(7)), and whether to postpone extradition if the person sought is being prosecuted or is serving a sentence in Russia (CPC Art. 465(1)). A restriction measure, such as custodial arrest, may be imposed even if it is not sought by the requesting state (CPC Art. 466).

a) ML and TF are extraditable offences (CPC Art. 462(3.1)). Minor deficiencies in criminalisation may preclude extradition if dual criminality is not met (see c.3.1, 3.4, 5.1, and 5.2), but this shortcoming is not weighed heavily due to the low likelihood that the facts of a request would implicate the exact deficiencies in the ML or TF offences and the possibility that the conduct may qualify as another crime under Russian law to satisfy dual criminality.

b) Russia prioritises extradition requests solely on the basis of the length of time for which a person can be detained pending extradition and the limitation periods under domestic law and procedure. This means that minor and ordinary offences are accorded first priority because the period of detention cannot exceed six months. Incoming requests are considered in order of arrival and outgoing requests preference terrorism cases (GPO Instruction No. 116/35 (2018)). The procedures outlined in CPC Ch. 54 and Instruction No. 116/35 provide timelines for the GDILC and deadlines for prosecutors. The extradition process is clear in terms of interaction between authorities, required paperwork and deadlines, the timing of notice to the wanted person and allowance for court appeals, the decision period for the court, the entry into force of the judicial decisions, and the timing of the handover of a person to the foreign country (CPC Arts. 462-463). However, the PG makes the ultimate decision on extradition and there are no constraints on the length of this process. This could potentially cause undue delay. Also, the case

[145] Russia has several treaties pursuant to which it may conduct extradition, including ten multilateral conventions, a number of European conventions, and 39 bilateral agreements, not counting two additional agreements not yet in force.

management system maintained to monitor progress on individual extradition matters is not fully adequate (see c.37.2).

c) Russia shall or may refuse extradition on a number of grounds, none of which appear to place unreasonable or unduly restrictive conditions on the execution of requests. Article 63 of the Constitution requires dual criminality and prohibits the extradition of a person persecuted for political convictions. The CPC forbids extradition of a person who has been granted asylum in Russia (Art. 464(1.3)). Russia also applies the rule of specialty such that it only will extradite if the requesting state guarantees that it will prosecute the individual only for the crime named in the request (CPC Art. 462(3.3)). Russia will refuse extradition if the person has already been sentenced for the same act in Russia, has had his or her Russian criminal case terminated (CPC Art. 464(1.3)), or if the criminal case cannot be instituted, or sentence executed, because the statute of limitations has expired "or on another legal ground" (CPC Art. 464(1.4)). Russia may refuse extradition if the crime was committed on in Russia, or against its interests, or if the person is being prosecuted in Russia (CPC Art. 464(2.3)).

Criterion 39.2 **–** Under Article 61 of the Constitution, a citizen of Russia cannot be extradited (see also CPC Art. 464(1.1) and CrC Art. 13). The Criminal Code directs that "citizens of Russia Federation and stateless persons permanently residing in Russia who have committed outside Russia a crime against the interests guarded by the [Russian Criminal] Code shall be subject to criminal liability in accordance with the [Criminal Code]" (CrC Art. 12(1)). In line with CPC Article 459, the PG shall consider initiating an investigation of a Russian citizen who has perpetrated a crime abroad on the basis of a foreign request and material provided by the foreign state. Communications about a crime from "other sources" can be grounds for the institution of a criminal case (CPC Art. 140). Prosecution without undue delay is not mentioned as a requirement.

Criterion 39.3 **–** Dual criminality is required for extradition (CPC Art. 462(3.1)), but the requirement can be met regardless of whether both countries place the offence within the same category of offence, or use the same terminology, provided that both countries criminalise the underlying conduct. In the context of outgoing extradition requests, Russian law requires a description of the "actual circumstances and the legal qualification of the act" (CPC Art. 460(4.3)). By analogy, there is flexibility for Russian authorities to examine the actual circumstances, or the conduct, underlying an incoming extradition request (CPC Arts. 462(3.1), 464(1.6)).

Criterion 39.4 **–** Russia does not have mechanisms for simplified extradition. Fundamental principles of domestic law are cited to justify this, as Russia must conduct a citizenship check on all wanted persons to comply with its Constitutional bar on extraditing Russian citizens.[146] However, it is unclear why the required citizenship check could not also be carried out in the context of simplified extradition.

[146] See IO.2 for additional context on extradition complications arising with regard to persons wanted by states that were part of the U.S.S.R. prior to 1991. Many of Russia's incoming extradition requests concern citizens of CIS countries and neighboring countries and there is a high probability that such persons also have Russian citizenship, by operation of law, and they may not be aware of this fact.

Even so, extradition in Russia is administrative (not judicial), and since detention periods cannot exceed six months for minor and ordinary offences, these extraditions proceed swiftly by necessity. In practice, the average time it takes to process extradition from start to finish does not normally exceed 2-3 months. Assuming the PG renders a prompt decision, there are no court challenges, and that legal constraints on the length of detention dictate the timing of the extradition process, Russian procedures are comparable to processing times for EU or Nordic arrest warrants or other simplified procedures.

Weighting and Conclusion

There are minor shortcomings in relation to the criminalisation of ML and TF which may preclude a finding of dual criminality for extradition in rare circumstances. The case management system is not fully adequate to monitor individual extradition matters. While the PG has an unlimited amount of time in which to make a final determination on extradition, this potential delay appears not to be a problem in practice. Russia addresses extradition requests in order of receipt and on the basis of how long it may detain an individual. While this may serve as a constraint on the PG's discretionary time, it may not allow authorities to prioritise urgent cases concerning serious offences such as terrorism. There is no simplified extradition due to asserted fundamental principles, but the administrative character of extradition in Russia means that processing times are comparable to simplified mechanisms available in other jurisdictions. There is no explicit requirement that prosecution of nationals that cannot be extradited proceeds without undue delay.

Recommendation 39 is rated largely compliant.

Recommendation 40 – Other forms of international co-operation

In the last MER, Russia was rated compliant with these requirements, which were strengthened since the 3rd round assessments.

Criterion 40.1 **–** Russia ensures that all competent authorities can provide a wide range of international co-operation in the areas of ML, TF and predicate offences. Competent authorities can cooperate with their foreign counterparts in compliance with international treaties, or on the basis of reciprocity (L115, Art. 10, Para. 1 and 2; Law on International Treaties, Art. 3, Para. 2). The agreements between Russian authorities and their counterparts are concluded in accordance with the model forms endorsed by the Government.

Criterion 40.2

a) Competent authorities have legal basis for providing co-operation (Art.10 of the L115, see also c.40.9 to c.40.20).

b) Competent authorities can co-operate directly with their counterparts.

c) Competent authorities have clear and secure gateways, mechanisms or channels to facilitate, transmit and execute requests for assistance. For example, Rosfinmonitoring uses the Egmont Secure Web as well as alternative channels for communication with non-Egmont member FIUs. MOI, FSS, IC and GPO use the Interpol communication channels as well as protected e-mail correspondence and video-conferences. Other authorities

use the relevant multilateral networks, postal or courier services, e-mail correspondence and diplomatic channels.

d) Competent authorities have processes in place to assess and prioritise requests and ensure timely assistance is provided. For example, request prioritization and execution within Rosfinmonitoring is regulated by internal orders[147], and a dedicated unit prepares a selection of incoming priority requests. In the NCB Interpol office, it is required to respond to "Urgent" requests within 24 hours and to "Non-urgent" requests within 30 days. All other competent authorities have similar prioritisation procedures.

e) Competent authorities have processes for safeguarding any information received. There is a general requirement applying to all competent authorities for non-disclosure of exchanged information (Art. 10, Para. 6 L115). National standards[148] for the protection of restricted access information (including personal data) also apply to information exchanged internationally. Additionally, all competent authorities have implemented internal regulations and systems for safeguarding information possessed by them, including that received from international counterparts.

Criterion 40.3 – Competent authorities have a range of bilateral and multilateral agreements and MOUs to facilitate co-operation with foreign counterparts. Such agreements are not required for Russian authorities to provide assistance, but can be established promptly if required by foreign authorities (Law on International Treaties, Art.3; L115 Art. 10, Para. 2). Whereas the legislation does not specify deadlines for negotiating and signing such agreements, the respective processes are streamlined by the model forms endorsed by the Government.[149] The key competent authorities have concluded numerous agreements.[150]

147 Such as Order No. 32 of 1 February 2016 "On modification of the order of the Federal Service for Financial Monitoring of June 5, 2012 No. 191 "On Temporary regulations of execution of function of Federal Service for Financial Monitoring on consideration and formation of requests, answers, information messages at interaction with divisions of financial intelligence of foreign States and territories"".

148 Such as the Federal Law No. 149-FZ of 27 July 2006 on information, informational technologies and the protection of information; GR No. 676 of 6 July 2015 on the requirements for the order of creation, development, commissioning, operation and decommissioning of state information systems and further storage of information contained in their databases; the FSTEC Order No. 17 of February 11, 2013 on the requirements for protection of data contained in state information systems that do not constitute state secrets, etc.

149 E.g. GO No. 653 of June 29, 1995 (as amended on 21 February 2017) for MOI; GO No. 1922-r of 30 October 2010 for RFM; GO No. 870-r of 5 May 2017 for FCS.

150 Rosfinmonitoring: Interagency agreements with 102 FIUs, as well as 1 intergovernmental agreement (with the Kingdom of Denmark). BR: 39 agreements (memoranda of understanding) in the field of banking supervision, most of which contain provisions on AML/CFT co-operation and information exchange; as well as 23 bilateral agreements (memoranda of understanding) with foreign financial market regulators, which mainly include a public list of co-operation areas allowing, where necessary, exchanges of information for AML/CFT purposes. MOI: Bilateral agreements, signed protocols and memoranda of co-operation in the fight against crime with competent authorities of 64 countries; FSS: around 100 agreements establishing official contacts with 209 security agencies, special services and law enforcement agencies from 104 foreign states; IC: 84

Criterion 40.4 – There is no explicit requirement or prohibition for competent authorities to provide feedback. Rosfinmonitoring uses a feedback form since 2017 which is sent quarterly to all FIUs that have exchanged information during the quarter. MoI has developed a standard form for responding to inquiries received from abroad. Other authorities, such as IC, GPO, FCS and BR provide feedback to their foreign counterparts upon request.

Criterion 40.5 – Russia does not prohibit or place unreasonable or unduly restrictive conditions on the exchange of information, which can occur "in the event it does not harm the interests of national security of the Russia and if it can allow the competent bodies of that state to commence an investigation or formulate a request" (L115 Art. 10, Para. 3). The notion of "harm the interests of national security" is construed to encompass the situations where Russia considers that execution of the request is likely to prejudice its sovereignty, security, public order or other essential interests (as set out in Art. 18, Para. 21 of the Palermo Convention). The decision on whether an information exchange would allow commencement of investigation or formulation of request by the foreign state is based on the general principles of the CPC.

a) Tax offences are criminalized (Art. 198, 199, 199.1 and 199.2 of the CrC), and applicable legislation does not stipulate that a request for assistance would be refused on the grounds that it is also considered to involve fiscal matters.

b) Bank or other professional secrecy provision does not hinder the provision of information to foreign partners in criminal cases (for example, Law 395-1, Art. 26) and between supervisors (Law on the BoR, Art. 51 and Art. 51.1; IAIS and IOSCO membership; Law on Auditing Activity, Art. 9, Para. 4; see also R.9).

c) State bodies involved in combating ML and TF to cooperate with foreign competent authorities of foreign states (L115, Art. 10) do not make such co-operation contingent upon the absence of an inquiry, investigation or proceeding underway in Russia. The model form endorsed by GO No. 1922[151] for agreements of Rosfinmonitoring (Art. 4, Para. 1) sets out that execution of a request for assistance may be refused in whole or in part if, *inter alia*, trial proceedings are underway in the requested country on the facts specified in request. This is not technically compliant, even though the authorities advise that this provision is normally negotiated and agreed upon separately by the parties on case-by-case basis, and that over the last five years there have been no refusals to execute the incoming requests on the "ongoing proceedings" grounds.

d) Co-operation is not contingent upon the nature or status (civil, administrative, law enforcement etc.) of the requesting counterpart authority vis-à-vis that of the respective Russian authority (L115, Art.10).

Criterion 40.6 – State bodies, which send requests on AML/CFT matters shall use provided information only for the purposes specified in the request (Art. 10, Para. 6).

intergovernmental and interagency agreements with relevant counterparts of foreign countries; GPO: 82 bilateral treaties and interagency agreements with foreign competent authorities. FCS: Intergovernmental agreements on co-operation and mutual administrative assistance in customs matters with 60 countries.

151 GO No. 1922-r of 30 October 2010 (as amended by GO No. 397-r of 21 March 2012)

While this provision does not explicitly require that information received from foreign counterparts can be used only by the authorities, for which information was sought or provided, this seems to be covered by applicable provisions of the co-operation agreements concluded by individual authorities with their foreign counterparts (which are considered as international treaties under Russian law). The AML/CFT Law applies the same condition to information provided by Russia (Art. 10, Para. 4). Model agreements establishing these procedures have been developed by, and are standard practices of, key competent authorities (Rosfinmonitoring, MoI, FSS, IC and GPO, FCS, BR, see also c.40.16).

Criterion 40.7 **–** The governmental bodies which send requests on AML/CFT matters shall ensure the confidentiality of provided information (L115, Art. 10, Para. 6). The law does not explicitly establish an authorization to refuse such exchanges where the requesting competent foreign authority cannot protect information effectively; nevertheless, this seems to be covered by applicable provisions of the co-operation agreements concluded by individual authorities with their foreign counterparts (which are considered as international treaties under Russian law). The key competent authorities have specific provisions establishing the protection of the confidentiality of information (for example, GO No. 1922-r, Art.4, Para. 1 and Art. 5, Para. 2 for Rosfinmonitoring; GO No. 870-r, Art. 4, Para. 5 and Art.5 Para. 5 for FCS; Law on the BoR, Art. 51, Part 5 and Art. 51.1, Part 7 for BoR).

Criterion 40.8 **–** The powers to conduct inquiries applicable for domestic purposes can be equally applied for international purposes (see R.27 to R.32). No obstacles exist in relation to conducting an inquiry on behalf of a foreign counterpart, and from exchanging information that the authorities can obtain domestically.

Criterion 40.9 **–** Rosfinmonitoring has an adequate legal basis to provide international co-operation (see also c.40.1 and c.40.5). In addition to the relevant provisions of the AML/CFT Law, the legal basis for co-operation is established by GO №1922-r[152] regarding international exchanges of information on transactions suspected for connection to ML, TF and predicate crimes, as well as by GO №630[153] and GO №209[154] regarding collection of information from domestic competent authorities and obliged entities to enable such exchanges of information.

Criterion 40.10 **–** There are no legal provisions to prevent Rosfinmonitoring from the provision of feedback, upon request or whenever possible, to its counterparts on the use of the information provided by them, as well as on the outcome of the analysis conducted on the basis of such information.[155]

Criterion 40.11 **–** The AML/CFT Law (Art. 10, Para. 1, 2 and 5) does not establish conditions that would make the exchange of information by Rosfinmonitoring with

152 Establishing the model form for agreements of RFM with international counterparts.

153 Establishing the rules for the provision of information to Rosfinmonitoring by other state bodies with the purpose of international co-operation.

154 Establishing the procedure for the submission of information to Rosfinmonitoring by obliged entities with the purpose of information exchange with the competent authorities of foreign states

155 Moreover, as a member of the Egmont Group, Rosfinmonitoring has to provide such feedback, upon request and whenever possible, to foreign counterparts (Clause 19 of the Egmont Principles for Information Exchange).

foreign counterparts contingent upon the method (i.e. access or obtainment) or the mode (i.e. direct or indirect) of acquiring information, as well as on the categories (i.e. STRs and additional information) and the types (i.e. financial, administrative, law enforcement) of acquired information (see also c.29.2 and c.29.3).

Criterion 40.12 – BoR[156] and FSSC[157] are the supervisors with a mandate to control compliance of financial institutions and have the appropriate legal basis to provide international co-operation (see also c.40.1 and c.40.5). In addition to the relevant provisions of the AML/CFT Law, the legal basis specifically defining the terms for BoR to exchange information with foreign counterparts is established by the Law on the BoR (Art. 51 and Art. 51.1) and by the Banking Law (Article 26) regarding exchanges of information and/or documents with foreign banking supervisors or financial market regulators. The definition of the nature or status of potential foreign counterparts appears to be reasonable having regard to the legally defined functions of BoR. Law on the BoR (Art. 73) contains a potential obstacle to effective home host practices, as a foreign supervisory authority would need written consent of the subsidiary established in Russia for accessing its premises. Also, BoR lacks the power to initiate sharing of information on an unsolicited basis, and confidentiality provisions in the Investment Fund Law conflict with the disclosure provisions in the Law on the BoR (for the securities market supervision).

Criterion 40.13 – Financial supervisors have the powers to exchange internationally the information available to them domestically, including information held by FIs. Relevant provisions of the Law on the BoR (Art. 51 and Art. 51.1) and the Banking Law (Article 26) entitle BoR to exchange with foreign banking supervisors or financial market regulators information and/or documents received in the course of performance of its supervisory function, including confidential ones, subject to bank secrecy, except for information that is deemed a state secret. IAIS and IOSCO membership of the BoR provides the necessary mechanisms for the timely exchange of information constituting insurance or other financial secrecy.

Criterion 40.14 – The provisions of the Law on the BoR (Art. 51 and Art. 51.1) and the Banking Law (Article 26) entitling BR to exchange with foreign counterparts refer to information and/or documents, which such counterparts might need for supervision purposes, thus establishing a scope of exchangeable information that is broad enough to encompass regulatory, prudential and AML/CFT information. The types of information, which may be exchanged between the BoR and a foreign counterpart, are specified in the respective bilateral agreement (memorandum of understanding)[158].

156 As the supervisor for credit and non-credit financial institutions.

157 As the supervisor for the Post of Russia; FSSC advises to be using the potential of Rosfinmonitoring for the exchange of AML/CFT-related information with foreign counterparts, where necessary. This has been considered sufficient for meeting the requirements under c.40.12-c.40.16 given the insignificant role of FSSC as a financial supervisor and, subsequently, the low materiality of such exchanges, if any.

158 For example, the Memorandum of Understanding between the BR and the Latvian regulator of the financial and capital markets (FCMC) provides for the exchange of information in areas such as licensing and regulation, control over the ownership structure, supervision of ongoing activities, financial rehabilitation and AML/CFT (including suspicious transactions and identified ML/TF schemes). Most of the agreements between the BR and its foreign partners

Criterion 40.15 **–** Financial supervisors can conduct inquiries on behalf of foreign counterparts (see also c.40.8). BoR can conduct inspections when requested by foreign counterparts (BRR No. 149, Art. 4.1). However, in relation to authorizing and facilitating the ability of foreign counterparts to conduct inquiries themselves in the country so as to facilitate effective group supervision, the Law on the BoR (Art. 73) contains a potential obstacle to effective home host practices, as a foreign supervisory authority would need written consent of the subsidiary established in Russia for accessing its premises. .

Criterion 40.16 **–** Financial supervisors must obtain prior authorisation from the foreign counterpart for any dissemination received (see c.40.6). In relation to cases when the requesting financial supervisor is under a legal obligation to disclose or report information received from the requested financial supervisor, the exceptions from the non-disclosure rule set out in the Law on the BoR (Art. 51, Part 2 and Art. 51.1, Part 3) in cases when the information is provided to a domestic court under the court's decision issued in criminal proceedings does not stipulate for promptly informing the requested financial supervisor on this circumstance. Nevertheless, the obligation to provide information received from foreign counterparts to a domestic court is duly disclosed in the requests to the foreign regulators pursuant to internal regulations of the BoR, as well as to the respective provisions in the memoranda of understanding concluded with them, thus meeting the condition stipulating that "prior authorization includes any deemed prior authorization under a Memorandum of Understanding" (INR40, Para. 13).

Criterion 40.17 **–** LEAs can exchange information available to them domestically (see c.40.1 c.40.5). Article 10 of the AML/CFT Law is an additional legal basis for Russian LEAs to exchange information related to ML and TF offences. Competent authorities may exchange information, including at the stages of intelligence gathering and preliminary investigation. LEAs may also provide information to counterparts related to the identification and tracing of proceeds to enable foreign authorities to open an investigation or draft a future MLA request. Russia is also an observer to CARIN. Through this informal network, Russia can search for the proceeds of crime located in foreign countries and provide reciprocal assistance.

Criterion 40.18 **–** LEAs can use their domestic powers to obtain information to respond to an international request. In response to requests, LEAs may perform tasks such as searching for, seizing, and confiscating the proceeds of crime, as well as performing expert examinations, interrogating suspects, defendants, witnesses, victims and other persons, executing searches and document seizures, transferring evidence, and serving documents (AML/CFT Law, Art.10; CPC, Chapter 53). The only restrictions are those related to confidentiality of the information sought or provided, and, as to requests for information about assets, that the information will only be used for the specific purpose specified in the request (Art.10 L115).

Criterion 40.19 **–**Russia may form joint investigative teams (JITs) with foreign authorities that are also parties to agreements or treaties acceded to by Russia. Currently, Russia has ratified one specific agreement on JITs with CIS Member States.

are available on the BR website (where such agreements provide for the possibility of their placement in the public domain): www.cbr.ru/today/ms/bn/mem/memorandum/

MoI also has MOUs in place with counterpart authorities which could allow for the formation of JITs.

Criterion 40.20 **–** There are no legal provisions inhibiting indirect exchange of information with non-counterparts. Overall, the general framework set out above appears to create an environment that would not inhibit indirect information exchanges between non-counterparts, where necessary, for AML/CFT purposes.

Weighting and Conclusion

All authorities have the powers and abilities to provide a wide range of international co-operation. There are minor shortcomings particularly relating to co-operation granted by financial supervisors.

Recommendation 40 is rated largely compliant.

Summary of Technical Compliance – Key Deficiencies

Compliance with FATF Recommendations

Recommendations	Rating	Factor(s) underlying the rating
1. Assessing risks and applying a risk-based approach	LC	• There is no explicit requirement for obliged entities to take enhanced measures for the management and mitigation of risks identified by national or sectoral risk assessments. • There is no explicit requirement for simplified CDD to be allowed only in case of identified lower risk. • There are no defined mechanisms to ensure that relevant obliged entities provide risk assessment information to SRBs. • There are no explicit provisions to require that internal control rules also enable management and mitigation of the risks identified by the country or, alternatively, that the risks identified by the country are taken into consideration by the obliged entities when developing and implementing risk management and mitigation programmes.
2. National co-operation and co-ordination	C	• All criteria are met
3. Money laundering offence	LC	• There are minor deficiencies related to the criminalisation of ML on the basis of the Vienna and Palermo conventions. • There is uncertainty regarding whether financial transactions involving only VAs can constitute ML. • There is limited administrative liability for legal persons with sanctions that are not fully dissuasive.
4. Confiscation and provisional measures	LC	• The proceeds of important predicate offences are not included in the main confiscation provision of the Criminal Code. Instead, reliance is placed on the Criminal Procedural Code to confiscate the proceeds of certain ML predicates, after restitution is decided. • There is a small gap regarding confiscation of corresponding value for certain offences. • There is no requirement to notify third parties if property they may have an interest in, and that was not previously seized, is to be confiscated. • Confiscation does not reach VAs.
5. Terrorist financing offence	LC	• While all offences listed in the Annex to the TF Convention are covered, some of these offences require proof of a specific terrorist purpose when they should not. • The TF offence inquiries into the perpetrator's knowledge of the recipient's intent. • The law does not unequivocally permit the mental element of the TF offence to be proven with evidence of the mere "intention" that funds should be used to carry out a terrorist act.
6. Targeted financial sanctions related to terrorism & TF	PC	• It can take up to two days for FIs and DNFBPs to implement TFS, which is not considered as occurring "without delay". • There are no legally enforceable requirements that apply to all natural and legal persons (beyond FIs and DNFBPs) to freeze or prohibit the provision of funds/assets/services to designated persons or entities.
7. Targeted financial sanctions related to proliferation	PC	• It can take up to two days for FIs and DNFBPs to implement TFS, which is not considered as occurring "without delay". • There are no legally enforceable requirements that apply to all natural and legal persons (beyond FIs and DNFBPs) to freeze or prohibit the provision of funds/assets/services to designated persons or entities.
8. Non-profit organisations	LC	• There are minor deficiencies relating to the lack of granularity of risk classification • Neither the TF NRA nor the NPO SRA include a reference to periodically reassess the risks faced by the NPO sector.
9. Financial institution secrecy laws	C	• All criteria are met

10. Customer due diligence	LC	• FIs are not obliged to identify BO at all times, notably if the identification or verification of identity proves to be a challenging enough effort for an FI to deem their application to be unreasonable or unavailable. • There are some deficiencies to establish the powers that regulate and bind the legal person/arrangements and to identify the management and the address of the legal person/arrangements. • The legislation does not clarify that FIs need to identify as BO the natural person holding the position of senior managing official. • No specific requirements exists to verify the identity of the beneficiary at the time of the payout. • There is no specific reference to include beneficiaries of life insurance contracts as a relevant risk factor when determining whether EDD is required at the time of payout. • The legislation does not specifically require the performance of EDD in all cases. • Where an FI is unable to comply with CDD measures, there is not an explicit obligation to terminate the business relationship in all cases. • There is no provision allowing the FI to elect not to pursue CDD and requiring it instead to file an STR.
11. Record keeping	LC	• There is no requirement to maintain records on all transactions, despite the extensive list of legally defined transactions subject to record-keeping obligation. • Non-CIs are not obliged to disclose CDD information and transaction records to a wide array of domestic competent authorities.
12. Politically exposed persons	PC	• When considering whether a customer falls within the category of foreign PEP, the determination should be made in accordance with the FATF Recommendations. This cannot be considered as a substantial national implementing measure and doubts arise whether this technique introduces clarity and certainty in the Russian legal system. • For foreign PEPs, senior management approval does not apply to continuing a business relationship (for existing customers). • Requirements to foreign PEPs are not applicable to certain transactions below a certain, reduced, threshold. • Eligibility of persons to be considered as PEPs mostly rely on being appointed rather than on the prominence of functions, which provides little flexibility for reporting entities to make their own appraisals. • EDD measures do not apply to close associates of any kind of PEP. • There is no provision requiring FIs to assess whether the beneficial owner of the beneficiary of life insurance policies is a PEP. • There are also no specific requirements for FIs to inform senior management before the payout of the insurance policy proceeds.
13. Correspondent banking	LC	• FIs are neither required to understand the quality of supervision of the respondent, to assess the respondent institution's AML/CFT controls or understand the AML/CFT responsibilities of each institution. • Legal requirements related to correspondent banking do not apply to FIs other than credit institutions.
14. Money or value transfer services	LC	• There is no obligation for MVTS providers to provide a list of its agents other than to Russian competent authorities. • There is also no requirements for MVTS providers to include their agents in the AML/CFT programme.
15. New technologies	C	• All criteria are met
16. Wire transfers	PC	• There are no requirements on ordering and intermediary FIs to ensure that information on the beneficiary accompanies cross-border wire transfers, which ultimately affects beneficiary FIs. • For cross-border wire transfers under a certain threshold, the information required is not available. • Intermediary and beneficiary FIs are not required to have a specific AML/CFT risk-based policy and procedure for determining when to execute, reject or suspend a wire transfer that lacks the required information on the originator and the beneficiary. • Intermediary FIs a not required to properly check the existence of the required originator and beneficiary information to accompany the wire transfer. • Beneficiary FIs are not required to detect whether beneficiary information is missing. • For a MVTS provider controlling both the ordering and beneficiary side of a wire transfer, only for funds transfers without opening of a bank account is there an implicit obligation to take into account the information from both sides in order to assess whether to file an STR

		or not. The application of this obligation to their branches, representative offices and subsidiaries is also an issue.
17. Reliance on third parties	LC	• There is no measure for the reliant FI to satisfy itself that third parties have measures in place in order to be able to adequately comply with CDD and record-keeping obligations.
18. Internal controls and foreign branches and subsidiaries	LC	• There is no screening procedure to ensure high standards for other employees. • There are several legal restrictions that may impede sharing within financial groups information related or unrelated to CDD as well as account and transaction information for AML/CFT purposes. • FIs are not specifically required to apply enhanced measures to manage ML/TF risks in case a state or territory where their branches and subsidiaries are located hinders implementation of the AML/CFT Law.
19. Higher risk countries	LC	• FIs are not explicitly required to apply enhanced due diligence proportionate to the risks from countries to which is called for by the FATF. • There is a right (not the obligation) to refuse to establish or terminate a business relationship in the cases relevant for R.19. • Communication of specific concerns about other countries' AML/CFT systems weaknesses can be improved.
20. Reporting of suspicious transactions	C	• All criteria are met
21. Tipping-off and confidentiality	LC	• Tipping-off provisions create some limitations to the sharing of information as established under R.18.
22. DNFBPs: Customer due diligence	LC	• Lawyers, notaries and accountants are not subject to AML/CFT requirements when they prepare for or carry out transactions on behalf or at the instruction of their clients concerning creation, operation or management of legal arrangements under foreign law • Persons (other than the DNFBPs specified by the AML/CFT Law) providing trust and company services are not covered by the AML/CFT Law. • Lawyers, notaries and accountants are exempt from the obligation to obtain senior management approval (in case they act not as sole entrepreneurs but as firms) before establishing a business relationship with foreign PEPs, as well as to update on a regular basis the information available on their foreign PEP clients • Deficiencies identified under the analysis for Recommendations 10, 11 and 12 bear an impact on the rating for Recommendation 22
23. DNFBPs: Other measures	LC	• Lawyers, notaries and accountants are not subject to AML/CFT requirements when they prepare for or carry out transactions on behalf or at the instruction of their clients concerning creation, operation or management of legal arrangements under foreign law • Persons (other than the DNFBPs specified by the AML/CFT Law) providing trust and company services are not covered by the AML/CFT Law. • Deficiencies identified under the analysis for Recommendations 18, 19 and 21 bear an impact on the rating for Recommendation 23.
24. Transparency and beneficial ownership of legal persons	LC	• The risk assessment should take additional data-sets into account to determine in more granularity the risk associated with legal persons. • There is no explicit obligation on a Russian legal entity to maintain the information on shareholder/members and of directors in Russia in all cases (e.g. where the legal person is not tax resident in Russia). • BO information be updated, but not necessarily to the extent that it is as up-to-date as possible. • Sanctions, particularly administrative sanctions, are not fully proportionate and dissuasive. • There is no legal reference requiring competent authorities to act rapidly when providing international co-operation in relation to basic and BO information.
25. Transparency and beneficial ownership of legal arrangements	PC	• The law does not require persons acting as professional trustees of a foreign trust to maintain and update basic or BO information of the trust. • There are no specific obligations for trustees to disclose their status to FIs or DNFBPs. • There is no liability or sanction for trustees who fail to maintain basic and BO information on the trust.
26. Regulation and supervision of FIs	LC	• The criminal record checks do not clearly cover criminal associates and the wider array of criminal offences. • There are minor shortcomings for supervision of Core Principles institutions. • Off-site supervision and unscheduled inspections can only be carried out on the ground of potential violation of the AML/CFT legislation by law, and not on the basis of other risk considerations.

		• There is no explicit requirement on reviewing the assessment of the ML/TF risk profile of a financial institution or group where major events or developments in the management and operations happen. • It is unclear whether Roscomnadzor is required to review the ML/TF risk profile of the institution supervised by it.
27. Powers of supervisors	LC	• Sanctions are not fully in line with the standards set out in R.35.
28. Regulation and supervision of DNFBPs	LC	• There is no designated supervisor for legal professionals. • There are no mechanisms to accredit legal professionals and to prevent criminal infiltration. • absence of measures to prevent criminal associates from being professionally accredited or from holding a significant or controlling interest in all DNFBPs. • There are no provisions or measures establishing the risk-based approach in supervision especially for lawyers and notaries
29. Financial intelligence unit	C	• All criteria are met
30. Responsibilities of law enforcement and investigative authorities	LC	• The responsibility to conduct financial investigations is widespread and may leave opportunities to properly investigate ML on the table.
31. Powers of law enforcement and investigative authorities	C	• All criteria are met
32. Cash couriers	LC	• The declaration system applies only to movements (both inward and outward) of cash and BNIs from and to the EAEU, meaning that only movements that cross the external borders of the EAEU are subject to the declaration requirements.
33. Statistics	C	• All criteria are met
34. Guidance and feedback	LC	• No specific feedback on the quality of individual STRs is given to reporting entities.
35. Sanctions	LC	• Monetary sanctions are not fully dissuasive. • The penalties related to TFS violations are not sufficient to be proportionate and dissuasive
36. International instruments	LC	• Minor deficiencies in compliance with R.3 and 5 result in minor shortcomings in R.36.
37. Mutual legal assistance	LC	• There are minor shortcomings in the clarity of processes for the prioritisation of requests and the sufficiency of the case management system to monitor progress on individual requests. • The evaluation of dual criminality for coercive forms of assistance may, in rare cases, be impacted by minor deficiencies in the ML and TF offences.
38. Mutual legal assistance: freezing and confiscation	LC	• There are minor shortcomings regarding the confiscation of value corresponding to the proceeds of certain offences and related to the confiscation of virtual assets. • The evaluation of dual criminality for confiscation-related assistance could be impacted by minor deficiencies in the ML and TF offences. • Assistance for non-conviction-based confiscation is partly limited.
39. Extradition	LC	• The evaluation of dual criminality for confiscation-related assistance could be impacted by minor deficiencies in the ML and TF offences. • The case management system has minor shortcomings. • Authorities may not be able to prioritise urgent cases concerning serious offences in all cases. • There is no explicit requirement that prosecution of nationals that cannot be extradited proceeds without undue delay.
40. Other forms of international co-operation	LC	• The execution of a request for assistance may be refused in whole or in part if, inter alia, trial proceedings are underway in Russia on the facts specified in the request. There is a potential obstacle to effective home host practices, as a foreign supervisory authority would need written consent of the subsidiary established in Russia for accessing its premises. • BoR lacks powers to initiate sharing of information on an unsolicited basis, and confidentiality provisions in the Investment Fund Law conflict with the disclosure provisions in the Law on the BoR (for the securities market supervision). • In cases when the information requested by the BoR from its foreign counterparts is provided to a domestic court under the court's decision issued in criminal proceedings, the BoR has no explicit obligation for promptly informing the requested financial supervisor on this circumstance.

Glossary of Acronyms[159]

AML/CFT Law or L115	Federal Law No. 115-FZ (2001) "On Combating Legalization (Laundering) of Proceeds of Crime and Terrorism Financing"[160]
BoR / BR	Bank of Russia
BRR	Regulation issued by the Bank of Russia (BoR)
CAO	Code of Administrative Offences
CI	Credit institutions
CvC	Civil Code of Russia
CCC	Credit consumer cooperatives
COE	Council of Europe
CrC	Criminal Code of Russia
CPC	Criminal Procedures Code of Russia
CPF	Countering the financing of proliferation of weapons of mass destruction
EAEU	Eurasian Economic Union
EUR	Euros
FCS	Federal Customs Service of Russia
FTFs	Foreign Terrorist Fighters
FTR	Federal Treasury of Russia (under the Ministry of Finance of Russia)
FTS	Federal Tax Service of Russia
FSB	Federal Security Service of Russia
ISIL	Islamic State in Iraq and the Levant
FTS	Federal Tax Service of Russia
GDILC	General Department of International Legal Co-operation
GR	Regulation adopted by the Government of Russia
GPO	General Prosecutor's Office of Russia
IAC AML/CFT/CPF	Interagency Commission for Combating ML, Terrorism Financing and Proliferation Financing, established by RFMO No. 304 (2016) (formerly, Interagency Commission for Combating ML and Terrorism Financing, established by RFMO No. 336 (2009))
IAC FATF Evaluation	Interagency Commission for Preparation of the FATF Fourth Round Mutual Evaluation, established by PO No. 31 (2016)
ITMCFM	The International Training and Methodology Centre for Financial Monitoring
IC	Investigative Committee
IWG Financial Crime	Interagency Working Group for Countering Illegal Financial Transactions, established by PO №344 of July 28, 2012
LEAs	Law enforcement authority(ies)
Law on Gambling Activities	Federal Law No. 244-FZ (2006) "On the State Regulation of Activities Associated with the Organization of and Carrying out Gambling and on Amending Individual Legislative Acts of Russia"
Law on International Treaties	Federal Law No. 101-FZ (1995) "On the International Treaties of Russia"
Law on Protection of Information	Federal Law No. 149-FZ (2006) "On Information, Informational Technologies and the Protection of Information"
Law on Notariate	Fundamentals of the Legislation of Russia on the Notariate No. 4462-1 (1993)

[159] Acronyms already defined in the FATF 40 Recommendations are not included into this Glossary.

[160] Many federal laws have been amended since the date of initial enactment noted herein. L115 was most recently amended in April 2018.

Law on State Statistics	Federal Law No. 282-FZ (2007) "On the Official Statistical Accounting and the System of State Statistics in Russia"
Law on the BoR	Federal Law No. 86-FZ (2002) "On the BoR"
Law on the Bar	Federal Law No. 63-FZ (2002) "On Advocates' Activities and the Bar in Russia"
LEAs	Law enforcement authorities
MCRs	Mandatory control reports
MFA	Ministry of Foreign Affairs of Russia
MLA	Mutual legal assistance
MoD	Ministry of Defence
MoF	Ministry of Finance of Russia
MoI	Ministry of Internal Affairs of Russia
MoJ	Ministry of Justice of Russia
NRA	National risk assessment
OCG	Organised criminal group
PD	Decree issued by the President of Russia
PO	Order issued by the President of Russia
Rosfinmonitoring	Federal Financial Monitoring Service of Russia
RFMO	Order issued by the Federal Financial Monitoring Service of Russia (Rosfinmonitoring)
RFMR	Regulations of the Federal Financial Monitoring Service of Russia (Rosfinmonitoring), endorsed by PD No. 808 (2012) and amended by PD No. 103 (2016)
Roscomnadzor	Federal Service for Supervision of Communications, Information Technologies and Mass Media
RUB	Russian roubles
SAC	State Assay Chamber of Russia (under the Ministry of Finance of Russia)
SRA	Sectoral Risk Assessment
USRLE	Uniform State Register of Legal Entities
USD	United States dollar
UNSCR	United Nations Security Council Resolution
VA	Virtual asset(s)
3PML	Third-party money laundering

www.fatf-gafi.org | www.eurasiangroup.org | www.coe.int/en/web/moneyval

April 2019

Anti-money laundering and counter-terrorist financing measures - Russia Federation

Fourth Round Mutual Evaluation Report

In this report: a summary of the anti-money laundering (AML) / counter-terrorist financing (CTF) measures in place in the Russian Federation (Russia) as at the time of the on-site visit from 11 to 29 March 2019.

The report analyses the level of effectiveness of Russia's AML/CTF system, the level of compliance with the FATF 40 Recommendations and provides recommendations on how its AML/CFT system could be strengthened.