FATF

Anti-money laundering and counter-terrorist financing measures

Sweden

Mutual Evaluation Report

April 2017

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 February 2017 Plenary meeting.

Citing reference:

FATF (2017), *Anti-money laundering and counter-terrorist financing measures - Sweden,* Fourth Round Mutual Evaluation Report, FATF, Paris
www.fatf-gafi.org/publications/mutualevaluations/documents/mer-sweden-2017.html

Photo credits cover photo: © Björn Olin/Folio/imagebank.sweden.se

CONTENTS

Executive Summary

1. This report provides a summary of the anti-money laundering and combating the financing of terrorism (AML/CFT) measures in place in Sweden at the date of the on-site visit (26 May 2016 to 10 June 2016). It analyses the level of compliance with the *FATF 40 Recommendations,* the level of effectiveness of Sweden's AML/CFT system, and makes recommendations on how the system could be strengthened.

A. Key Findings

- Sweden has a reasonable understanding of its ML/TF risks, but this is not consistent across authorities. Sweden does not have a national coordination body for AML/CFT at the policy level, which has a negative effect on Sweden's effectiveness in other areas, including the understanding of risk across agencies.
- Sweden's implementation of targeted financial sanctions (TFS) against terrorist financing is ineffective, mainly because of serious technical deficiencies that are inherent within the framework of applicable EU regulations, and because of Sweden's failure to propose or make designations itself. Sweden is not able to transpose TFS against proliferation financing without delay, but this is mitigated by other factors and has not had a practical effect on Sweden's ability to properly comply with UNSCRs on proliferation.
- Sweden prioritises international cooperation and has established highly effective mechanisms for providing it, including specific liaison mechanisms with Nordic and Baltic neighbours, EU cooperation instruments, and dedicated channels for operational cooperation with law enforcement authorities.
- Sweden systematically collects and uses financial intelligence; however, the FIU has inadequate IT tools and its strategic analysis function is still being established. These deficiencies limit its ability to identify complex cases of money laundering and to provide risk information for other authorities and the private sector.
- Authorities show a high degree of commitment and capacity to pursue ML and TF cases and to trace and confiscate the proceeds of crime. Prior to 2014 Sweden suffered problems with both its ML and TF offences. The new ML offence (introduced in 2014), and the new TF offence (introduced in 2016) have

addressed these problems and have greatly improved the potential for investigation and prosecution of ML and TF, although authorities still need to build experience and precedents for applying the new offences in practice.

- Sweden has a comprehensive supervisory system. Financial institutions and Designated Non-Financial Business and Professions (DNFBP) generally comply with their obligations, and have been subject to enforcement action when they do not. However, not all supervisors have a sufficient understanding of the risks to apply a risk-based approach effectively, and the FSA should increase its capacity, in order to conduct an appropriate number of AML/CFT-focused supervisory actions given the risk and size of Sweden's financial sector.
- Legal ownership and control is highly transparent in Sweden, and some beneficial ownership information is available. However, this is not sufficient to ensure that beneficial ownership information is available in all cases as such information is not collected systematically and not subject to adequate verification or sanctions.

B. Risks and General Situation

2. Sweden is an open economy that is located in the northern periphery of Europe. The economic system is characterised by a large proportion of card transactions, and consequently a small proportion of cash handling. Sweden is ranked by the IMF as one of 29 systemically important financial centres in the world, and has a large banking sector with assets amounting to about four times GDP. Sweden is also an important financial centre for the Nordic and Baltic regions.

3. Sweden is generally perceived as a safe country with low crime. Sweden ranks near the top of international indices for low corruption and strong rule of law. Tax crimes are the most significant predicate offence for money laundering identified in Sweden's national risk assessment. Fraud is also identified as a major and growing concern. Both offences contribute a large part to the proceeds of organised crime in Sweden. The most significant criminal typology is tax fraud related to unregistered labour where, in order to bypass tax regulations, businesses pay undeclared cash wages. Some such schemes use corporate structures in Sweden and other countries, and false invoicing, to conceal the nature of the activity. Organised crime is also associated with smuggling, mainly of narcotics, performance enhancing drugs, cigarettes and arms.

4. Terrorism, and as a consequence terrorist financing, in Sweden is dominated by actors motivated by violent Islamic extremism, whose purpose is to promote or commit acts of violence in conflict areas such as Syria, Iraq, Afghanistan, Somalia and Yemen, or against Sweden or Swedish interests. The emergence of ISIL in Syria and Iraq transformed the terrorist threat in Sweden: between 2012 and 2015, approximately 300 Swedish residents had travelled to Syria to join ISIL, of which 40 have been confirmed deceased and 140 had returned to Sweden, where they constitute a new risk.

C. Overall Level of Effectiveness and Technical Compliance

5. Following the last FATF evaluation in 2006, Sweden's AML/CFT regime has undergone significant reforms. The introduction of a revised money laundering offence and other measures in 2014 and a revised terrorist financing offence in 2016, together with organisational changes to a number of authorities, has led to significant changes and improvements in Sweden's AML/CFT system. Nevertheless, improvements are still needed in national AML/CFT policy coordination, the assessment of risk, and the implementation of targeted financial sanctions.

6. While these changes have been implemented quickly in some cases, there has been limited time for them to be reflected in the results being achieved and assessed for Effectiveness. The quality and use of statistics relevant for money laundering is uneven, especially regarding the proceeds of crime. Sweden is highly effective in the area of international cooperation, and achieves a substantial level of effectiveness in the investigation and prosecution of both money laundering and terrorist financing as well as in confiscation of the proceeds of crime, and in the application of measures to counter the financing of proliferation of weapons of mass destruction. Sweden achieves only a moderate level of effectiveness in other areas, and significant improvements are needed in understanding ML/TF threats, domestic coordination, using financial intelligence and other information, the supervision of financial institutions and non-financial businesses and professions, the application of targeted financial sanctions for TF, and measures to prevent the misuse of legal persons and arrangements.

C.1 Assessment of risk, coordination and policy setting (Chapter 2; IO.1, R.1, 2 & 33)

7. Sweden's authorities perceive their highest ML risks to be tax crimes, fraud, organised crime, and cash movements. The identified risks are largely reasonable, but some significant risks identified by law enforcement are not sufficiently developed in the national risk assessments (NRAs), for example the misuse of companies and new technologies. Key agencies in Sweden have gone beyond their limited NRAs in terms of identification and understanding of the risks that Sweden faces. But gaps remain and not all authorities have done so, which limits how Sweden is able to address its risks, in particular some areas that have been identified as higher risk. The strengths of the process and results of the development of the NRAs are the broad agency involvement and the frank identification and description of the vulnerabilities and knowledge gaps. Swedish authorities have commissioned a number of follow-up reports to the NRAs in different formats.

8. Sweden has a national strategy to address key deficiencies identified by the 2013–14 NRAs. It outlines high-level priorities and describes a number of measures to be taken, such as legislative amendments to improve LEAs' tools for pursuing ML, TF, confiscation and cross-border cash movements, actions to fill knowledge gaps in several areas, and necessary improvements in co-ordination and analysis. The strategy is a significant step for Sweden's development of AML/CFT policies, but contains a number of gaps, in part because of the knowledge gaps identified by Sweden's NRA. With a few exceptions it does not contain national priorities to address Sweden's specific ML/TF risks identified (e.g. tax crimes, fraud, organised crime and cash movements). There

is no formal mechanism of coordination to assess risks and develop policy in Sweden. Nor is there any formal mechanism in place to review and update the strategy.

9. Sweden's largest challenge is the coordination of a complex structure of agencies in the field of AML/CFT. Currently, there is no national coordination body for AML/CFT and responsibilities are dispersed between many autonomous agencies. While operational cooperation and coordination is good in some areas (e.g. on organised crime or tax), there are some disconnects in Sweden's system, as individual agencies form and pursue their own priorities. There is also a concern that relevant risk information gathered by one agency may not be shared in an effective manner with other agencies. Swedish authorities are aware of these deficiencies, which are identified both in the 2013 NRA on ML and the Strategy of 2014.

C.2 Financial intelligence, and ML investigations, prosecutions and confiscation (Chapter 3; IO.6, 7, 8; R.3, 4, 29–32)

10. Sweden systematically collects and uses financial intelligence and other relevant information in investigations of money laundering and in tracing criminal proceeds. The ability of Sweden to use financial intelligence has improved since the new money laundering offence entered into force July 2014. The new offence provided the authorities with better tools to freeze assets and prosecute money-launderers. As a consequence, the work of the financial intelligence unit and law enforcement authorities has since focused more on the money laundering offence itself, while previously their focus was on the predicate offences. Several major money laundering investigations and prosecutions have been undertaken on the basis of financial intelligence, and the FIU also supports other law enforcement investigations.

11. However, the Swedish FIU (the Financial Police – "Fipo") has not yet achieved its potential because its operational analysis is not able to identify complex cases of money laundering. This is mainly due to the inadequate IT tools that do not allow for transaction pattern recognition. Fipo's strategic analysis function is still being established and it does not yet produce strategic intelligence products. Sweden's access to financial intelligence in some financial sector entities and DNFBPs has been hindered by the fact that Fipo has not provided supervisory authorities and the private sector with information on typologies, trends, and financial profiles. Improved strategic analysis of ML (beyond the misuse of cash), and increased access to financial intelligence, would contribute to better understanding of ML scenarios by law enforcement. This should enhance the investigation and prosecution of third-party ML, particularly large scale cases.

12. The new ML offence (in force since July 2014) has greatly improved Sweden's ability to investigate and prosecute ML. The requirements of the pre-2014 ML offence severely limited LEAs' ability to investigate and prosecute ML activity. Since 2014, the new ML offence requires prosecutors to show that laundered property "derives from criminal activity". The new legislation has been used proactively and has contributed to good results in a short time period. Different types of ML have been investigated, prosecuted and convicted, particularly targeting stand-alone ML. The authorities show a high degree of commitment to the new ML offence, particularly embedding the ML offence within their structure and practices. Due to the legislation being relatively new, it is not yet clear whether the sanctions imposed are effective and dissuasive. Lack of comprehensive statistics (due in

part to Sweden's sentencing practices) also limits the ability of the authorities to monitor convictions and fully understand the impact of the new legislation.

13. The authorities consider depriving criminals of their assets to be a highly dissuasive penalty and therefore prioritise tracing and confiscating assets. Confiscation is pursued as a policy objective. Asset tracing investigations are generally effective: Swedish LEAs efficiently trace assets, take measures to secure them, and are increasingly able to ensure that judges award the confiscation of criminal assets. Nonetheless, the lack of clear statistics on the assets recovered from criminals make it challenging to quantitatively assess the degree to which Sweden achieves the objectives of its confiscation policies. The identification and seizure of cash by Customs could be improved, and the efforts to uncover ML through transportation of cash do not reflect the risks identified.

C.3 Terrorist and proliferation financing (Chapter 4; IO.9, 10, 11; R.5–8)

14. Swedish authorities prioritise combating terrorist financing and have developed methods and capacity to pursue it. Financial investigations are conducted alongside all counter-terrorism cases, and authorities disrupt terrorist financing activity in cases when it is impossible to obtain a conviction for TF. There is active and well-coordinated inter-agency and international cooperation, including through dedicated liaison staff, and CFT is reflected in Sweden's measures to prevent terrorism and violent extremism.

15. Sweden has only prosecuted a small number of TF cases reflecting the difficulty of successfully conducting prosecutions under the old TF offence, and the very recent introduction - in April 2016 - of a new TF offence. In addition, TF threats to Sweden relating to foreign terrorist fighters have escalated sharply since 2014. The new TF offence, addresses past problems, but it is too early for its practical impact on effectiveness to be widely felt, and authorities still need to build experience and precedents for applying the new offence in practice. The combination of new threats and new laws mean Sweden cannot demonstrate a long track record of cases in this area, but nevertheless seems to have a substantial level of effectiveness.

16. Sweden's implementation of targeted financial sanctions (TFS) against terrorist financing is ineffective, mainly because of serious technical deficiencies that are inherent within the framework of applicable EU regulations, and Sweden's failure to use either mechanism to propose or make designations. Sweden has no mechanism to use targeted financial sanctions at a national level in response to terrorist threats affecting Sweden, has never on its own proposed a designation to the UN or to the EU, and has no mechanism to make its own designations. Sweden also suffers excessive delays in the transposition of UN sanctions, and gaps in the ability to sanction EU internal terrorists. This appears to weaken authorities' ability to prevent terrorist financing flows.

17. Sweden has a solid and effective framework of measures to prevent the misuse of NPOs. While there is limited formal oversight or supervision, there are strong self-regulatory initiatives and voluntary engagement with government agencies. Rigorous self-regulatory measures apply to NPOs which account for a significant portion of the financial resources under control of the sector, and additional oversight by the Swedish International Development Agency (SIDA) applies to those which represent a substantial share of the sector's international activities.

18. Sweden implements targeted financial sanctions (TFS) regarding the financing of proliferation of weapons of mass destruction, through EU measures. TFS relating to proliferation are in a technical sense not implemented without delay, owing to the time taken to transpose UN designations into EU regulations. However, in the case of Iran, sanctions were implemented without delay as a result of the more extensive EU sanctions regime, and in the case of the DPRK, the risk posed by delays is largely mitigated by the negligible trade and financial links between Sweden and the DPRK. Overall, persons and entities designated by the United Nations Security Council Resolutions (UNSCRs) on proliferation of weapons of mass destruction (WMDs) are identified, deprived of resources, and prevented from raising, moving, and using funds or other assets for the financing of proliferation.

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

19. Financial institutions' and DNFBPs' compliance with their obligations is generally adequate. Large banks, especially those that have been subject to enforcement actions by the FSA, have made significant efforts in enhancing AML/CFT compliance and in strengthening their compliance resources. The larger banks and large MVTS providers are generally aware of their obligations and are also in frequent contact with the authorities. As a result, their level of risk understanding is stronger, and consequently they have applied additional risk-mitigating measures where necessary. Smaller FIs and DNFBPs are aware of their obligations and apply those in accordance with the law. But their knowledge of their ML/TF risks is limited to only what is in the NRAs and other reports, and they receive little additional guidance on risk from the authorities. The application of additional measures to address specific risks by these sectors is very limited.

20. Financial institutions and DNFBPs generally conduct adequate CDD and monitoring of their customers. However, the measures taken with regard to beneficial ownership are not commensurate with the risks. Financial institutions and DNFBPs also seem over-reliant on information in held in company registers when identifying and verifying the identity of beneficial owners.

21. The authorities report that the quality of the Suspicious Transaction Reports (STRs) has improved over the past two years, particularly for those filed by larger institutions. However, most DNFBP sectors (such as Trust and Company Services Providers (TCSPs), lawyers, and real estate agents) are filing very few STRs, despite the risks identified in those areas. Supervisory authorities have been trying to improve the ability to recognise suspicious activity and the number and quality of STRs by focusing on suspicious activities and reporting requirements in their inspections. However, this will be difficult as there is very limited guidance on typologies, red flags and indicators, insufficient information shared by the FIU and LEAs, and as most DNFBPs have little or no interaction with the relevant supervisor.

C.5 Supervision (Chapter 6; IO.3; R.26–28, 34, 35)

22. The supervisory AML/CFT system in Sweden covers all obliged entities. All fundamental elements of an AML/CFT supervisory system are in place, but there are weaknesses in applying risk-based supervision. Supervisors' understanding of ML/TF risks is based on the 2013-2014 NRAs, which do not provide a comprehensive picture and analysis of Sweden's risks. The FSA has made

efforts to understand the TF risks by commissioning additional research and is updating its knowledge from external sources as the media and international fora. Most of the other supervisors have not assessed any additional ML/TF risks that may occur in their sectors. The current methods of assessing the ML/TF risks of most types of supervised entities are basic and do not allow for effective risk-based supervision.

23. Sweden is a significant financial centre. More supervisory resources need to be allocated in order for the Swedish FSA to undertake appropriate onsite and offsite supervisory actions commensurate with the risk and the size of Sweden's financial and DNFBP sectors.

24. Most supervisory authorities have in their activities identified deficiencies in the implementation of AML/CFT control measures by reporting entities and have taken actions to improve their compliance, including enforcement actions which have been published. The FSA has revoked the licence of a large credit market company in one case, and in another case used the highest monetary fine available to it – however at that time, the maximum available fine was low relative to the size of the bank. Sweden has since changed its laws in August 2014 to increase the maximum fine from an absolute figure to a percentage of turnover. The FSA has applied lower levels of sanctions in other cases. All supervisors have issued AML/CFT regulations and some authorities (the FSA, the CABs, the SBA, the FMI) have issued additional guidance. However, the level of understanding by the private sector is uneven, which may be due to some of the guidance provided not giving sufficient detail in terms of AML/CFT obligations.

C.6 Transparency and beneficial ownership (Chapter 7; IO.5; R.24, 25)

25. Legal ownership and control is highly transparent in Sweden, due to a strong tradition in the transparency of information, including the public availability of information held in the company registers, as well as corporate and personal information (e.g. tax returns of individual companies and natural persons). Hence, complex legal structures established in Sweden and their legal owners can easily be traced, with the exception of some legal entities such as non-profit associations and some types of foundations that are not obliged to register, and foundations that have yet to comply with their requirement to register. However, the misuse of legal persons is a vulnerability identified by Sweden. Sweden has yet to perform a full assessment of the ML/TF risks associated with all types of legal entities. The use of false identities, corporate structures, and straw persons (i.e. where legal owners or directors are not the actual beneficial owners/controllers) are identified by the authorities as regularly used in criminal schemes which can affect the reliability of the information collected. Some beneficial ownership information is available from company registers (for simple ownership structures) or from financial institutions and DNFBPs (from CDD measures). Although this does not make beneficial ownership information available in all cases, beneficial owners may be identified by competent authorities through investigative measures using other sources of information.

26. Swedish law does not provide for the creation of trusts or other legal arrangements, and Sweden is not a party to the Hague Trust Convention. But there is no prohibition on trust activities being conducted, and banks do have trustees as clients (although this is not common), and some trust service providers operate in Sweden. Information on trust-relevant parties is therefore only

available from CDD information collected by the FIs and DNFBPs, and through investigative measures by competent authorities.

C.7 International cooperation (Chapter 8; IO.2; R.36–40)

27. Sweden prioritises international cooperation and has established highly effective mechanisms for providing it. Sweden exchanges and seeks appropriate information, financial intelligence, and evidence, and facilitates action against criminals and their assets. Cooperation is very close with the Nordic and Baltic regions, but extensive cooperation also takes place with EU members and other countries worldwide. Sweden provides timely mutual legal assistance and extradition/surrender to countries using direct European mechanisms (e.g. European arrest warrants, Eurojust), and through dedicated international chambers of public prosecutors and a central authority at the Ministry of Justice.

28. Law enforcement cooperation is a particular strength, particularly thanks to the well-resourced Single Point of Operative Contact (SPOC) which receives, actions, and follows-up on requests for cooperation. Sweden also uses a network of liaison officers to facilitate cooperation, including both Swedish liaisons and shared Nordic liaison officers. Investigators and prosecutors make effective use of joint investigative teams to investigate ML and recover the proceeds of crime. FIU to FIU cooperation takes place through shared platforms and appears to currently be prioritised effectively by the FIU. Sweden's FSA collaborates closely with foreign supervisors when supervising Swedish financial institutions which operate in other countries, through supervisory colleges and joint on-site inspections, as well as coordination on investigations and sanctions cases.

29. Sweden actively seeks international cooperation when intelligence or evidence is needed from foreign partners, including tracing money abroad and authorities have successfully prosecuted some cases involving international criminal networks through cooperation with foreign counterparts. Sweden is able to provide available beneficial ownership information on legal persons to requesting states though there are certain limitations concerning the identification of beneficial owners particularly when foreign legal persons are involved.

D. Priority Actions

30. The prioritised recommended actions for Sweden, based on these findings, are:

- Sweden should urgently introduce legal powers which will enable authorities to apply targeted financial sanctions relating to terrorism or proliferation, as a bridging measure; to EU internal terrorists; or on a national basis, together with a body or mechanism responsible for developing proposals for designation.
- Sweden should establish a national mechanism to ensure adequate cooperation and coordination at policy level between ministries and operational agencies. Clear policies/instructions on division of labour; procedures for cross-agency case handling; and forums for sharing of risk information should be established, particularly between the FIU and LEAs and the supervisors.

- Sweden should increase the access to and use of financial intelligence to identify complex cases of money laundering as well as professional money laundering, based on improved IT systems at the FIU and by developing its strategic analysis capacity.
- Supervisors should improve their understanding of risks in their specific sector(s), supported by better tools and inter-agency communication, and use this understanding to implement a risk-based approach towards supervising the reporting entities. Sweden should increase the capacity of the FSA's AML unit in order for it to undertake appropriate AML/CFT on-site and off-site supervisory actions, commensurate with the risk and size of Sweden's financial sector.
- Sweden should take forward its plans to establish a central register of beneficial ownership (as required by the EU Fourth Anti-Money Laundering Directive). Sweden should also conduct a full risk assessment of the misuse of all the legal persons for ML/TF, and develop measures to mitigate the use of straw-men and corporate structures.
- Authorities should build experience and establish precedents for prosecution and sentencing under the recently revised ML and TF offences.

Effectiveness & Technical Compliance Ratings

Effectiveness Ratings (High, Substantial, Moderate, Low)

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
Moderate	**High**	**Moderate**	**Moderate**	**Moderate**	**Moderate**
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	
Substantial	**Substantial**	**Substantial**	**Moderate**	**Substantial**	

Technical Compliance Ratings (C - compliant, LC – largely compliant, PC – partially compliant, NC – non compliant)

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	**PC**	**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**	**LC**	**LC**	**C**	**LC**
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	**C**	**C**	**PC**	**PC**	**PC**
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**	**C**	**LC**	**LC**	**PC**
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	**PC**	**LC**	**LC**	**LC**	**C**
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
LC	**PC**	**LC**	**LC**	**LC**	**C**
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**	**C**	**C**		

MUTUAL EVALUATION REPORT

Preface

This report summarises the AML/CFT measures in place in Sweden 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 Sweden's 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 Sweden, and information obtained by the evaluation team during its on-site visit to Sweden from 26 May to 10 June 2016.

The evaluation was conducted by an assessment team consisting of:

- Mr. Anders Schiøtz Worren, Ministry of Justice and Public Security, Norway (Legal expert)
- Ms. Alison Kelly, Metropolitan Police Service, UK (Law enforcement expert)
- Mr. Kwiwoong Lee, Korea Financial Intelligence Unit, Korea (Law enforcement expert)
- Ms. Maud Bökkerink, Dutch Central Bank, Netherlands (Financial expert)
- Mr. Bernardo Mendoza Ruenes, National Banking and Securities Commission, Mexico (Financial expert)
- Mr. Tom Neylan, Mr. Francesco Positano, and Mr. Song Biao Shiao, policy analysts, FATF Secretariat
- Ms. Olayinka Akinyede, GIABA Secretariat.

The report was reviewed by Jaakko Christensen, National Bureau of Investigation, Finland; Veronika Mets, MONEYVAL Secretariat; and Richard Lalonde, IMF.

Sweden previously underwent a FATF Mutual Evaluation in 2006, conducted according to the 2004 FATF Methodology. The 2006 evaluation and 2010 follow-up report have been published and are available at www.fatf-gafi.org/countries/s-t/sweden/.

Sweden's 2006 Mutual Evaluation concluded that the country was compliant with six Recommendations; largely compliant with 20; partially compliant with 16; and non-compliant with five. Two of the Recommendations were assessed to be not applicable to Sweden. Sweden was rated compliant or largely compliant with 12 of the 16 Core and Key Recommendations. Sweden was placed under the regular follow-up process immediately after the adoption of its 3rd round Mutual Evaluation Report, and was moved to biennial updates in October 2010.

CHAPTER 1. ML/TF RISKS AND CONTEXT

31. Sweden is a Nordic country on the Scandinavian Peninsula in northern Europe. Sweden has a land border to Norway in the west and Finland to the north-east, and is connected to Denmark across the sea via the Öresund Bridge to the south-west. With a land area of 449,964 km^2, Sweden is the fifth largest country in Europe by size. However, Sweden's population of 9.85 million inhabitants only constitutes approximately 1.3 percent of Europe's population. Sweden has a low population density with 21 inhabitants per km^2, with the southern part of the country significantly denser. A relatively large portion of Sweden's population is born abroad, amounting to 17 percent in 2015.

32. The capital of Sweden is Stockholm, the largest city in the country, with 1.4 million inhabitants in the city and 2.2 million inhabitants in the metropolis. The second largest city is Gothenburg, with 550,000 inhabitants in the city and 970,000 inhabitants in the metropolis. The third largest city is Malmö, with 280,000 inhabitants in the city and 690,000 in the metropolis.

33. Sweden is a constitutional monarchy, which means that the Head of State is the King or a reigning Queen. Today, however, the Head of State has mainly representative duties. There are four political levels in Sweden. The Riksdag is the parliamentary legislative organ on the national level. On the local and regional level, there are municipalities (290) and county councils (20). The European level is added to these three levels through Sweden's membership in the European Union (EU). Sweden consists of a single state entity with common legislation and is thus not a federation. Some power has been devolved to regional and municipal authorities, which enjoy certain levels of autonomy in devolved matters.

34. Sweden is a member of the UN and is one of the organisation's main contributors. It has been a member of the EU since 1995, but has not adopted the Euro as its currency.

ML/TF Risks and Scoping of Higher-Risk Issues

Overview of ML/TF Risks

35. Sweden is generally perceived as a safe country with low crime[1]. Sweden ranks near the top of the list on the international indexes on corruption[2] and rule of law[3]. However, economic crime in Sweden is an area of interest. In 2015, a total of 14,458 tax offences and 14,641 accounting offences were reported.[4] Reported drug offences have increased by 41 percent over the past decade[5]. Sweden also has relatively high levels of reported offences for some proceeds-generating crime, including the highest reported rate of theft in the EU, the second-highest for vehicle theft, and is in the top quintile for drug offences and burglary. These figures could however be reflective of high relative reporting,

1 4th in terms of Societal Safety & Security, Global Peace Index 2015, Institute for Economics and Peace

2 3rd in the Corruption perceptions index 2015, Transparency International

3 3rd in the Rule of law index 2015, World Justice Project

4 Swedish National Council for Crime Prevention (Brå), https://www.bra.se/bra/bra-in-english/home/crime-and-statistics/fraud-and-economic-crime.html

5 Swedish National Council for Crime Prevention (Brå), https://www.bra.se/bra/bra-in-english/home/crime-and-statistics/drug-offences.html

1

rather than actual crime, and could also be a result of changes in the way Sweden have been recording crimes. The basis for these statistics was examined by the assessment team.

36. Sweden is an open economy that is geographically located in the northern periphery of Europe with a large financial sector in relation to GDP. The economic system is characterised by a large proportion of card transactions, and consequently a small proportion of cash handling. Cash is strongly associated with high ML/TF risk by the Swedish authorities, and large cash transactions are almost automatically considered suspicious. Many bank branches in Sweden have ceased handling cash over the counter completely owing to low demand and high costs, and as a consequence, the authorities have observed organised crime taking an increased interest in cash-intensive businesses and currency exchangers, subjecting them to higher ML/TF risks in spite of the low overall cash use in Sweden.

37. Organised crime in Sweden has historically been characterised by smuggling, where the nature of the smuggled goods has changed over time. Today mainly narcotics, performance enhancing drugs, cigarettes and arms are smuggled. The incentive to make some money on the side has historically correlated strongly with tax legislation, various bans and criminal politics. Traditionally organised crime has been fuelled by existing or created markets (such as high excise duties on alcohol or tobacco). A large part of the profits of organised crime come from various types of tax offences or economic crime. The largest amounts appear to originate from tax fraud related to unregistered labour. Construction, cleaning, restaurants and bars are prone to hire unregistered labour. In order to bypass tax regulations when paying cash wages in large scale operations and to finance other expenses, funds in accounts must be convertible to cash. Some of the schemes also incorporate the use of the services of a financing or factoring company. In more advanced cases, there are complex arrangements where criminal organisations operate their own invoicing, financing and exchange offices.

38. The use of fake invoices issued by front companies and companies represented by straw men is considered to be a high risk area in Sweden. In the 2015 NRA by the Swedish National Council for Crime Prevention (Brå), the regular use of straw men was highlighted and additionally, the prosecutors have indicated problems with obtaining information on beneficial owners. Some institutions mention the use of "false" IDs or the use of an ID by someone else other than the rightful owner. The risks of the misuse of companies may be increased by the availability of an exemption from audit requirements, which some 28 percent of Swedish limited companies make use of, and where 74 percent of those exempted companies have as a result never been audited.

39. An area that is closely related to cash handling is wholesale cash transports, which often enable criminal organisations to handle and launder money, but conversely can play a significant role in preventing such operations. Money transfers are also considered an area or sector that is associated with high ML risks.

40. Sweden's large financial sector and advanced financial services that involve transactions via the international payment system also pose as higher ML/TF risks. The potential of new forms of payment solutions (such as pre-paid cards, mobile wallets and virtual currencies) could make criminal organisations less dependent on cash and thus create new difficulties.

Country's risk assessment

41. Sweden has a long history of threat assessments for various types of crimes, hereunder economic crime and organised crime. Various agencies have produced their own threat and risk information, with Brå developing several relevant reports.

42. In 2012, the Swedish Government ordered the development of the first national risk assessments concerning AML/CFT, which were completed in 2013 for the ML National Risk Assessment (NRA), and 2014 for the TF NRA. The NRAs were developed by 16 authorities and a self-regulatory body: Brå, the Swedish Estate Agents Inspectorate (FMI), the Financial Supervisory Authority (FSA), the Swedish Gambling Authority (LI), the three County Administrative Boards (CABs) for Stockholm, Västra Götaland and Skåne, the Swedish Tax Agency (STA), Swedish Customs (TV), the Swedish Economic Crime Authority (EBM), the Supervisory Board of Public Accountants (RN), the Swedish Security Service (Säpo), the Swedish Bar Association (SBA), the Swedish Prosecution Authority (SPA), Fipo (the Financial Intelligence Unit (FIU) also representing the Police Authority, the Swedish Enforcement Authority (KFM) and the Swedish Companies Registration Office (SCRO). The FSA was appointed as coordinating authority for the NRA. Relevant representatives from other authorities and the private sector were also invited to participate.

43. Follow-ups to both the ML and the TF NRA were published in December 2015. In contrast to the cross-authority production of the original NRAs, a single authority was given responsibility for each follow-up. The follow-up NRA on ML was developed by Brå, while the follow-up to the TF NRA was developed by the Centre for Asymmetric Threat Studies (CATS) at the Swedish Defence University.

Scoping of Higher Risk Issues

44. In deciding what issues to prioritise, the assessment team reviewed material provided by Sweden on national ML/TF risks, and information from reliable third-party sources (e.g., reports by other international organisations). The issues listed present not only the areas of higher ML/TF risks (including threats and vulnerabilities), but also contain issues that were of significant concern to the assessment team based on material provided before the on-site visit.

- Tax crimes are the most significant predicate offence for money laundering identified in Sweden's NRA. Fraud is also identified as a major and growing concern. Both offences frequently involve the misuse of corporate structures, in Sweden and other countries, including companies, trusts and foundations, false invoicing, and concealment of beneficial ownership. The assessment team focused on the investigation and prosecution of these offences, and on how effectively authorities were able to uncover the use of domestic and foreign legal persons in such cases. The assessment team further took note of the high risk posed by cash-intensive businesses including bureaux de change and money or value transfer service (MVTS) providers.
- Besides the role of analysing and disseminating STRs, the FIU plays a central role in Sweden's AML/CFT system. While the FIU is a member of several of the coordination arrangements of the Swedish authorities, its (indirect) participation in some large

1

working groups was analysed. The assessment team reviewed the FIU's powers, priorities, and responsibilities, and how financial intelligence is generated and used by Swedish authorities.

- Sweden has a higher number of Foreign Terrorist Fighters than most European countries on a per capita basis, and the support and facilitation of these present the highest current terrorist financing risks. Many FTFs have returned to Sweden after having taken part in training or conflicts in other countries. The assessment team focused on how Sweden manages these risks.
- In light of Sweden's role as a financial centre for Nordic and Baltic regions, the assessment team focused on how well cross-border ML and TF risks are understood and managed by financial institutions, and on how effectively supervisors are responding to these risks in the region.

Materiality

45. Sweden has a large public sector which is mainly collectively funded via the national tax system. The tax pressure, or tax quota (total tax revenue divided by GDP), is relatively high in comparison to other states, and is relevant to tax crimes being the most significant predicate offence identified. In 2015, it was 43.2 percent (the OECD average is approximately 34 percent). Direct and indirect taxes on labour constituted 60 percent of total tax revenue in 2014, while the remaining 40 percent was made up of capital taxes (including corporate tax), VAT, and excise and import duties.

46. Sweden's banking market is dominated by the four major banks, Svenska Handelsbanken, Nordea, SEB and Swedbank, with Nordea being one of the FSB's 30 identified global systemically important banks (G-SIBs). Sweden is also an important financial centre for the Nordic and Baltic regions. This exposes Swedish banks to ML risks originating outside Sweden, and makes Sweden's supervision of its financial institutions' compliance with AML/CFT obligations important to the region as a whole.

47. The Swedish payment system is technically well developed and highly efficient, which means that payments are made in a rapid, secure and cost-efficient manner. Consequently, the use of cash has been decreasing rapidly while the average value of individual card transactions in Sweden has fallen. Practically all Swedes have access to a bank account with a debit card. The value of cash in circulation has been declining over the last decade, to 2% of GDP in 2014. In 2012, 96 percent of Swedes below age 35 paid their invoices via internet banking. Checks are practically non-existent in Sweden.

Structural Elements

48. The key structural elements for effective AML/CFT control are present in Sweden, such as political and institutional stability, accountability, transparency and rule of law.

49. All persons resident in Sweden have social security numbers which are used for identification purposes. Information (such as name, domestic and/or overseas addresses, date of birth, citizenship,

family members, and taxable income) on registered persons can be easily accessed by the public. Companies in Sweden have organisation numbers and similar information about them is also public.

50. Sweden's principle of public access to official documents safeguards the right for all people to partake of official documents, i.e. documents that have been submitted to, created by or are kept by a public authority. The principle of public access to official documents is regulated in one of the Swedish fundamental laws, the Freedom of the Press Act (1949:105). The need to maintain confidentiality for some documents is regulated by the Public Access to Information and Secrecy Act (2009:400).

Background and other Contextual Factors

AML/CFT strategy

51. Sweden has a national AML/CFT Strategy, decided by the Government on 19 June 2014. The strategy is mainly based on the findings in the 2013 ML NRA and the 2014 TF NRA, and consists of three components – objectives, priorities and measures. The strategy sets out its objectives for an effective AML/CFT Regime and lists the following priorities:

- **Requirements of knowledge** – building and enhancing knowledge of ML/TF,
- **Special areas of focus** – a need to on an ad hoc basis or long term take special and targeted measures concerning specific areas, sectors or phenomena,
- **Cooperation** – establishing a new and effective structure,
- **Information management** – developing and enhancing the management of information and knowledge in the system,
- **Regulatory measures** – ensuring an effective and adequate legislation over time.

52. The strategy includes specific short and long term measures:

- **Cooperation** – a wider and enhanced mechanism of cooperation with a clearer mandate to produce national risk assessments and to develop policy and risk-based measures,
- **Knowledge-enhancing measures** – improving the understanding of ML/TF and addressing existing knowledge gaps,
- **Specific targeted measures**: (1) Alternative money transmitters, (2) Cross-border cash couriers, and (3) Fundraising for beneficiaries abroad,
- **Adapting the new police organisation** (which was reformed in 2015) to international standards – improving the information management in the system,
- **Regulatory measures** – (1) Revision of the AML/CFT Act, (2) A new ML offence.

53. The priorities, which are high level, aim to be the starting point of the work to achieve the objectives of the Swedish AML/CFT regime and highlight some of the necessary elements and structural components that need to be in place in order to build an effective AML/CFT system. It is

1

intended that the authorities pursue their own strategies and to develop policy in the area according to the direction set by this strategy (see Chapter 2).

Legal & institutional framework

54. AML/CFT efforts involve several ministries: the Ministries of Finance, Justice, Culture, Enterprise and Innovation, and Foreign Affairs. A large number of authorities answer to the ministries and have either been assigned tasks related to AML/CFT or are directly affected by AML/CFT measures.

55. The Swedish system for AML/CFT consists of five main groups of actors:

- the law enforcement and controlling authorities (mainly the Police and the two Prosecution Authorities, the Security Service, the Tax Agency and Customs),
- the supervisory authorities (the Financial Supervisory Authority, the Estate Agents Inspectorate, the Swedish Gambling Authority, the Supervisory Board of Public Accountants, the three County Administrative Boards of Skåne, Stockholm and Västra Götaland counties),
- a directory authority (the Companies Registration Office),
- a self-regulatory body (the Bar Association), and
- the obliged entities (financial, non-financial and other non-financial actors).

56. Supervisory authorities:

- The Swedish Financial Supervisory Authority (FSA) comes under the authority of the Ministry of Finance and is responsible for issuing regulations, the review of licences and oversight of financial markets and financial companies. The FSA's mandate includes contributing to a stable and well-functioning financial system. With regard to AML/CFT, the FSA is responsible for the supervision of the financial sector institutions.
- The Swedish Estate Agents Inspectorate (FMI) comes under the authority of the Ministry of Finance and is the government agency that reviews estate agent applications, and registers and supervises real estate agents, as well as determining disciplinary measures against them. For AML/CFT, the FMI is responsible for registered real estate agents.
- The Swedish Gambling Authority (LI) comes under the authority of the Ministry of Finance and is the government agency commissioned with ensuring the legality, security and trustworthiness of the Swedish gambling market. LI is responsible for oversight of casino gambling for AML/CFT.
- The Swedish Supervisory Board of Public Accountants (RN) comes under the authority of the Ministry of Justice. RN's AML/CFT oversight covers activities as an approved or authorised public accountant or registered accounting firm.
- The Swedish Bar Association (SBA) is a self-regulatory organisation that regulates and supervises the legal profession independently and without government or other

external involvement. The SBA is responsible for oversight of lawyers and associates at law firms for AML/CFT, i.e. when they undertake certain services designated under legislation.

- The County Administrative Boards of Skåne, Stockholm and Västra Götaland counties (CABs) come under the authority of the Ministry of Finance and are the state authorities that constitute a link between citizens and municipalities, and government, parliament and central authorities. For AML/CFT, the CABs share supervisory authority for professions that are not already covered by other supervisory agencies, such as accounting and tax advisers, independent legal professionals, TCSPs, and DPMS.

57. Criminal investigation agencies:

- The Swedish Police Authority is the national police authority, whose operations are organised over seven regions. The Swedish police previously consisted of 21 partially autonomous and geographically divided police authorities, with a central administrative authority. Investigations and preventative work against financial crime and money laundering is conducted over all seven regions and within the National Operations Department (NOA). NOA includes the Criminal Investigation Unit, which focuses on criminal investigations such as ML investigations and asset tracing and recovery. The Criminal Intelligence Unit focuses on intelligence work and detection of serious organised crime, including ML and TF. Fipo (the FIU) is a department within the Criminal Intelligence Unit. The Fraud Reporting Centre is a unit within the Police Authority.
- **The Swedish Security Service (Säpo)** is a security service with police powers conducting intelligence and security work to prevent, pre-empt, protect, detect and investigate crimes against Swedish national security including terrorism.
- **The Swedish Prosecution Authority (SPA)** comes under the authority of the Ministry of Justice and contributes to the reduction of crime and increasing the safety of people by ensuring that persons who carry out crimes are subject to criminal investigation and prosecution. Prosecutors at the authority have a responsibility to lead criminal investigations (carried out by Police or Customs personnel) in more complicated cases, take decisions on matters of prosecution and bring court proceedings in all cases that are referred to the authority. The Prosecution Authority has particular expertise in analysis and investigation of fields such as confiscation, proceeds of crime, international and organised crime and terrorism.
- **The Swedish Economic Crime Authority (EBM)** comes under the authority of the Ministry of Justice and is a specialist authority within the Swedish prosecution, with particular expertise in analysis and investigation of economic crime. The authority's remit is to create security and justice by preventing and combating economic crime, e.g. accounting offences, tax crimes, crimes on the financial market, and ML relating to predicate offences within their remit. The Economic Crime Authority also takes crime prevention measures and undertakes intelligence activity.

1

- **The Swedish Tax Agency (STA)** comes under the authority of the Ministry of Finance and is the agency that administrates taxation, property tax, the population register and estate inventory records. The Tax Agency includes tax crime investigation units. Their duties are to conduct criminal investigations on behalf of prosecutors, conduct intelligence activities and undertake crime prevention work.
- **Swedish Customs (TV)** comes under the authority of the Ministry of Finance and is one of Sweden's revenue collection agencies. Swedish Customs is tasked with collecting customs duties, taxes and fees and for reducing tax and revenue collection errors. Swedish Customs is tasked with combating cross-border crime, and is also the government agency that is notified of cash funds from travellers bringing in or taking out a minimum of EUR 10,000 to and from the EU.

58. Other agencies:

- **The Swedish Companies Registration Office (SCRO)** comes under the authority of the Swedish Ministry of Enterprise and Innovation and is the agency in charge of registering most forms of business such as limited companies, partnerships, economic associations and sole traders. The SCRO conducts reviews, administers registration and provides information to ensure a legally sound business sector, and also maintains records of prohibitions from engaging in commercial activities and can determine the compulsory liquidation of companies that do not comply with certain legislative rules. The SCRO's records are a central source of information about all types of business relationships and for criminal investigation agencies. The SCRO also maintains records of parties engaged in activities that are subject to supervision by the County Administrative Boards (CABs).
- **The Swedish National Council for Crime Prevention (Brå)** comes under the authority of the Ministry of Justice and is both a government agency and a research and development centre. The National Council for Crime Prevention has conducted a number of projects on areas related to money laundering as part of an ongoing research programme into asset-focussed crime prevention.
- **The Swedish Enforcement Authority (KFM)** comes under the authority of the Ministry of Finance and is commissioned with maintaining a healthy willingness to pay in society and with combating phenomena that could lead to over-indebtedness. This government agency has four principal aims. These are to recover unpaid receivables, handle payment injunctions, receive and decide on applications for debt restructuring and to manage supervision of the receivership process.

59. National Cooperation Arrangements:

- **The Coordination Supervisory Body**, which was established in 2009, consists of representatives from the supervisory authorities (FMI, FSA, LI, RN and the CABs), as well as the SBA, Fipo and the SCRO on a voluntary basis. Säpo has attended since 2016. The tasks of the body are regulated by the AML/CFT Ordinance pursuant to the AML/CFT Act.

- **FIU-STA-EBM Cooperation**. Since 2012, Fipo, the STA, and the EBM have had a separate cooperation model established, where the STA and the EBM have staff seconded to Fipo to lend their expertise to intelligence that is related to economic/tax predicate offences, and to serve as liaisons.
- **A joint Government venture against aggravated organised crime (GOB)** was instigated in 2009 to counter aggravated organised crime by coordinating competences from several authorities. This venture and closer co-operation allows information from several authorities to be collected, processed and analysed, with the purpose of mapping and fighting organised crime optimally. The former National Bureau of Investigation (now the Police Authority's National Operations Department (NOA)) was appointed to coordinate a venture, which comprised the EBM, the Swedish Prison and Probation Service, the KFM, the Swedish Coast Guard, the STA, Säpo, TV and SPA. Since 2009, the Swedish Social Insurance Agency, the Swedish Migration Agency and the Swedish Employment Agency have joined the venture.
- In June 2013, as part of the GOB venture, the Government instructed six authorities (the EBM, the SPA, the Police Authority, TV, the STA and the KFM) to develop and follow up the cooperation between authorities in the area of the proceeds of crime. Part of the task included developing a cross-authority strategy for working with the proceeds of crime in cooperation, to develop processes for more effective cooperation and to identify areas where further development is needed.
- **The National Centre for Terrorism Threat Assessment (NCT)** is an informal permanent working group where Säpo, FRA, and the Swedish Military Intelligence and Security Service (Must) participate. NCT produces reports that affect and are distributed among all the participating authorities as well as the Government Offices and the 14 agencies in the National Counter-Terrorism Cooperative Council.

60. Sweden also has informal cooperation arrangements between different authorities and between authorities and obliged entities (see Chapter 2).

Financial sector and DNFBPs

61. Sweden is ranked by the IMF as one of 29 systemically important financial centres in the world[6], and has a large banking sector with assets amounting to about four times GDP[7]. The latter's proportion of the total balance sheet of the financial market was 39 percent at the end of 2013. The banking market is dominated by the four major banks, Svenska Handelsbanken, Nordea, SEB and Swedbank, all of which are headquartered in Stockholm. Nordea is one of the 30 Global Systemically

6 IMF (2013), Mandatory Financial Stability Assessments Under the Financial Sector Assessment Program: Update, www.imf.org/external/np/pp/eng/2013/111513.pdf

7 OECD (2015), OECD Economic Survey Sweden www.oecd.org/eco/surveys/Sweden-2015-overview.pdf

1

Important Banks (G-SIBs)[8]. An overview of the numbers of registered financial institutions in Sweden can be found in Table 2 below.

62. The full range of DNFBP sectors exist within Sweden, and are all covered by the AML/CFT regime. There is a state monopoly on casinos in Sweden, with the four casinos in Stockholm, Gothenburg, Malmö and Sundsvall run as a state-owned company. There is however online gambling operated by licensed operators from other EU jurisdictions that illegally advertise in Sweden; the authorities are as a result not able to act significantly against these violations. Companies can easily be formed through the SCRO without the use of lawyers or company service providers, although there are businesses which provide such services, including the sale of off-the-shelf companies. Similarly, while Swedish law does not provide for the creation of trusts or other legal arrangements, such service providers do exist. Dealers in precious metal and stones are covered within the broader definition of professional traders in goods that allow for cash payments of at least EUR 15,000. The numbers of registered entities in each DNFBP sector is found in Table 3 below.

Preventive measures

63. Administrative regulations in Sweden are to a large extent based on the EU's Third Anti-Money Laundering Directive, which was implemented in Sweden through the AML/CFT Act (2009:62), which came into effect on 15 March 2009, the AML/CFT Ordinance (2009:92) and via regulatory directives. Following that, additional revisions have been made to the Act ahead of the full implementation of the Fourth Anti-Money Laundering Directive.

64. The objective of the AML/CFT Act is to prevent financial and other business operations being used for money laundering or terrorist financing.

65. Pursuant to Section 8 of the AML/CFT Act, the FSA, LI, FMI and the CABs have issued regulatory directives relating to this area. RN has issued directions pursuant to the Swedish Auditors Act (2001:883) and the Auditors Regulation (1995:665). RN's regulations refer to good auditing practice in this area. The content of such practice is expressed, for example, in the EtikU 11 Members' Application of the Act on Measures against Anti-Money Laundering and Terrorist Financing, which has been approved by RN. SBA has produced a memorandum entitled Guidance on the Act on Measures against Anti-Money Laundering and Terrorist Financing (version 2). This guidance is intended to provide both an introduction to money laundering legislation and support in certain issues of a practical and administrative nature.

Legal persons and arrangements

66. In November 2015, Sweden had slightly in excess of 1.272 million registered legal entities. Business enterprises typically take the form of limited companies, sole proprietors, trading partnerships, limited partnerships, and economic associations. Besides these, there are legal entities that are generally used for other purposes such as housing associations, religious associations, housing cooperatives, foundations, and non-profit associations (not all of which need registration, or

8 FSB (2015), 2015 update of list of global systemically important banks (G-SIBs), www.fsb.org/wp-content/uploads/2015-update-of-list-of-global-systemically-important-banks-G-SIBs.pdf

are registered, with the Swedish authorities). Foundations (a legal entity in Sweden) are often used to perform the functions that trusts perform in other countries, e.g. bequeathing assets to future generations.

67. Most businesses are small, with approximately 93 percent having less than five employees. Based on tax filings, around 100,000 businesses are dormant. Sweden ranks 8th among 189 economies in the World Bank's Ease of Doing Business rankings[9], and a new limited company can be registered in four working days[10]. The extent of foreign ownership of Swedish companies – 13 986 foreign-owned companies in 2015[11], is about 3 percent of all companies.

Table 1. **Overview of Company Types (30 November 2015)**

Legal person	Number
Limited companies	503 117
Sole proprietors	619 835
Trading partnerships	62 679
Limited partnerships	20 057
Economic associations	14 977
Housing associations	29 981
Registered foundations	16 240
Non-profit associations with commercial characteristics	1 228
Branches of foreign companies	3 086
Other	571

Source: SCRO's register, CABs' foundation register

68. Swedish law does not provide for the creation of trusts or other legal arrangements, and Sweden is not a party to the Hague Trust Convention. As such, trusts do not have any legal status or validity in Sweden. Foundations (a legal entity in Sweden) are often used to perform the functions that trusts perform in other countries, e.g. bequeathing assets to future generations. There is however no restriction on trust activities being conducted in Sweden using foreign trust law, and there is no information on the size and scale of such activities.

Supervisory arrangements

69. AML/CFT requirements for financial institutions and DNFBPs are contained in the AML/CFT Act (2009:62). These are supplemented by the respective FI/DNFBP-type legislation and/or

9 World Bank (nd), Doing Business – Sweden, www.doingbusiness.org/data/exploreeconomies/sweden/

10 www.bolagsverket.se/en

11 Growth Analysis (2016), Foreign controlled enterprises 2015, www.tillvaxtanalys.se/in-english/publications/statistics/statistics/2016-06-27-foreign-controlled-enterprises-2015.html

1

regulations. The FSA is the AML/CFT supervisor for all relevant financial institutions, while there are several supervisors for the different DNFBP types.

Table 2. **Financial institutions in Sweden (27 January 2016)**

FIs	Licencing/Registration	Number
Banks and credit market companies	Banking and Financing Business Act (2004:297)	
Banking companies		38
Members banks		2
Savings banks		47
Branches of foreign banks		28
Credit market companies		35
Branches of foreign credit market companies		2
Consumer credit companies	Certain Consumer Credit Related Operations Act (2014:275)	
Consumer credit institutions		45
Deposit companies	Deposit Taking Operations Act (2004:299)	
Deposit companies		20
Life and investment related insurance	Insurance Business Act (2010:2043)	
Life insurance companies		30
Unit-linked insurance companies		9
Small and medium local insurance companies		63
Foreign insurance companies and branches		7
Insurance intermediaries	Insurance Mediation Act (2005:405)	
Insurance brokers		1 031
Branches of foreign life insurance brokers		12
Securities firms	Securities Markets Act (2007:528)	
Securities firms		112
Branches of foreign securities firms		39
Agents of foreign securities firms		6
Investment fund managers	Investment Funds Act (2004:46)	
Investment fund managers		42
Branches of foreign investment firms		17
Alternative investment funds managers	Alternative Investment Fund Managers Act (2013:561)	
Alternative investment fund managers (authorised and registered)		110
Payment services companies	Payment Services Act (2010:751)	
Payment institutions		27

FIs	Licencing/Registration	Number
Registered payment service providers		64
Foreign payment institutions and branches		202
Electronic money issuers	Electronic Money Act (2011:755)	
E-money institutions		5
Financial institutions[1]	Obligation to Notify Certain Financial Operations Act (1996:1006)	
Financial institutions		307

Table Note
1. "Financial institution" is a specific class of licence in Sweden for the business of currency exchange, or other financial operations (such as the granting of loans, financial leases, guarantees or letters of credit, or providing financial advice, means of payment or currency trading services).

Table 3. **DNFBPs in Sweden (January 2016)**

DNFBP	Licencing/Registration	AML/CFT Supervisor	Number
Casinos	Casino Act (1999:355)	Gambling Authority (LI)	4
Real estate agents	Real Estate Agents Act (2011:666)	Estate Agents Inspectorate (FMI)	6 732
Authorised or approved auditor/registered audit firm	Public Accountants Act (2001:883)	Supervisory Board of Public Accountants (RN)	3 664
Advocates and associate lawyers at law firms	Code of Judicial Procedure (1942:740)	Bar Association (SBA)	6 935
Other accounting and auditing professionals	AML/CFT Act (2009:62)	County Administrative Boards (CABs)	20 060
Tax advisers			680
Other independent legal professionals			2 694
Trust service providers			17
Company service providers			787
Dealers in precious metals and dealers in precious stones[1]			8 492

Table Note:
1. DPMS are regulated under the same category as other high value dealers in Sweden. The number of actors reflected here is a compilation from multiple SNI codes such as trading with cars, gems, boats etc. Only a minority of these companies will accept cash payments in excess of 15,000 euro.

International Cooperation

70. There are various kinds of international cooperation initiatives in the area of AML/CFT. For example, both ministries and agencies participate in FATF work on an ongoing basis, although to

1

different extents. The FIU cooperates with numerous international intelligence units, and with inter-governmental organisations such as Europol and the OPC (Operative Committee of the Task Force on Organised Crime in the Baltic Sea Region, BSTF). In addition, both the Swedish Government Offices and government agencies participate in a large number of working groups at a global and European level that aim to directly or indirectly combat money laundering. For example, the FSA participates in the Europe-based Anti-Money Laundering Committee (AMLC), which is a committee of the European Supervisory Authorities (ESAs).

Terrorist Financing and Financing of Proliferation

71. Terrorism, and as a consequence TF, in Sweden is dominated by actors motivated by violent Islamic extremism, where the purpose is either to promote or commit acts of violence in conflict areas, such as Syria, Iraq, Afghanistan, Somalia and Yemen, or terrorist threats against Sweden or Swedish interests. Between 2012 and 2015, approximately 300 Swedish residents had travelled to Syria to join ISIL, of which 40 have been confirmed deceased and 140 had returned to Sweden. The authorities note that the foreign fighter returnees potentially constitute new challenges and risks. Since the autumn of 2010, Säpo has noticed a greater intent to attempt violent acts against Sweden. The authorities are also aware of activities in Sweden that support terrorism in other countries that are not limited to actors motivated by violent Islam.

72. Säpo has observed, among other factors, that individuals who travel to Syria to support ISIL or similar groups often accumulate capital by taking so-called text loans or blanco loans (with no intention to ever pay them back), or other forms of fraudulent behaviour. Another example is schemes where individuals have acted as retailers of large amounts of mobile telephones using shell companies and evading VAT when the profits are sent abroad. Given the problem of the actual individuals travelling to conflict areas themselves, self-financing is even more relevant.

73. Swedish industry generally operates on a high technological level, with important (often transnational) companies active in several fields which may be relevant for the development of weapons of mass destruction and their delivery systems. Sweden has a well-developed defence and aerospace industry. This high technological level presents an enhanced risk of being targeted for illegal procurement attempts, both directed at acquiring technologies and equipment. Before 2010, Iran for decades used to represent one of Sweden's most important export markets in the Middle East with yearly export figures up to 8 billion SEK (approximately EUR 840 million). Many big Swedish companies were (and some still are) represented in Iran and important financial flows used to go through Swedish banks.

74. While the availability of very advanced technologies in Sweden may in theory draw a similar interest from the DPRK, the lack of similar business and trade history compared to with Iran result in a significantly lower risk exposure to the DPRK.

CHAPTER 2. NATIONAL AML/CFT POLICIES AND COORDINATION

Key Findings and Recommended Actions

Key Findings

- Sweden has a national strategy to address key deficiencies identified by the 2013–14 NRAs. The strategy is a significant step for Sweden's development of AML/CFT policies, but contains a number of gaps, in part because of the knowledge gaps identified by Sweden's NRA. Key agencies in Sweden have gone beyond their limited NRAs in terms of identification and understanding of the risks that Sweden faces, but this is not consistent across authorities. The understanding of TF risks is overall better than that of ML risk
- Sweden's largest challenge is the coordination of a complex structure of agencies in the field of AML/CFT. Currently there is no national coordination body for AML/CFT and responsibilities are dispersed between many autonomous agencies. While operational cooperation and coordination is good in some areas (e.g. on organised crime or tax), there are some disconnects in Sweden's system, as individual agencies form and pursue their own priorities. The lack of national mechanisms for AML/CFT coordination and cooperation also hinders the effective sharing of relevant ML/TF risk information across agencies.
- The quality and use of statistics relevant for money laundering is uneven, especially regarding the proceeds of crime.
- Sweden has introduced a revised money laundering offence and other measures in 2014 through the Act on Penalties for Money Laundering Offences, and implemented organisational changes to a number of authorities. While these changes have been implemented quickly in some cases, there has been limited time for them to be reflected in the results being achieved.

Recommended Actions

- Sweden should establish a national mechanism to ensure adequate cooperation and coordination at policy level between ministries and operational agencies. Clear policies/instructions on division of labour; procedures for cross-agency case handling; and sharing of risk information should be established, particularly between the supervisors, LEAs and the FIU.
- Sweden should continue to develop its assessment of risks, involving all relevant agencies, and based on a broad use of methods, tools, and information.
- Identified knowledge gaps should be filled and further policies and activities should be developed based on risks. Risk information should be communicated to reporting entities promptly and proactively.
- Sweden should enhance the use of the results of the risk assessments in determining exemptions or enhanced measures.
- Sweden should enhance the use of available statistics to improve its own analysis and understanding of efforts to combat ML/TF, and manage its priorities.

75. 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, R.2 and R.33.

Immediate Outcome 1 (Risk, Policy and Coordination)

Country's understanding of its ML/TF risks

76. Swedish authorities draw upon a sound framework for assessing various risks and threats relating to economic crimes and proceeds, due to a large number of publications on various related subjects. A number of agencies publish annual reports and occasional typologies, and the Swedish National Council for Crime Prevention (Brå) has developed a number of studies on specific proceeds-generating predicates, organised crime, etc. Such documents represent a strength in the risk understanding relevant to ML and TF; they are also widely referenced and form to a certain extent the basis for the NRAs.

77. Based on the NRAs, and interviews and case studies/examples from key agencies, Sweden's highest ML risks are perceived by the authorities to be tax crimes, fraud, organised crime, and cash movements. The identified risks are largely reasonable, but some significant risks identified by law enforcement are not sufficiently developed in the NRAs, for example the misuse of companies and new technologies. As Sweden is near to being a cash-free society, with mitigation measures in place against the risks of cash-use, the authorities still consider that cash is a key tool for criminals in the threats identified (e.g. organised crime) and consequently focus much of their attention on the use of cash and cash-intensive and related businesses.

78. Generally, the risk understanding of key agencies is sounder and more developed than the risk understanding elaborated in the 2013–14 NRAs, which were either limited in scope and risk analysis, or, in the case of TF, outdated. The most important authorities on the financial and law enforcement side (e.g. the EBM, the STA, the FSA) are to a substantial degree aware of their risks at a national level. Other authorities base their understanding on the NRAs, and are therefore affected by the respective shortcomings. There is also a concern that relevant risk information gathered by one agency may not be shared in an effective manner with other agencies (see more under the section on coordination).

79. Sweden completed an ML NRA in 2013, developed as a broad cross-agency effort led by the FSA, with the involvement of 17 agencies, and with the Swedish Defence Research Agency (FOI) contributing analytical and methodological support. The 2013 NRA on ML was mostly a threat assessment, and quite short and general in its descriptions and findings. It identified a number of knowledge gaps (such as insufficient awareness of the forms and extent of money laundering, and how predicate offences and threats can be linked to various forms of money laundering), and was followed by a 2015 NRA on ML by Brå which gave a more detailed picture of ML in Sweden, drawing on earlier trend reports and research, and interviews and workshops with representatives from authorities and industry organisations.

80. Sweden has conducted one NRA on TF, in 2014. It was published shortly before the threat of ISIL and FTFs materialised fully, and is hence practically outdated. Following that, the FSA commissioned the Centre for Asymmetric Threat Studies (CATS) at the Swedish Defence University, to carry out an updated analysis on TF in Sweden. The report was published in December 2015. The assessment team found that Säpo has a clear understanding of their current TF risks. Their understanding is underpinned by integrated terrorism and TF threat assessments produced regularly by the National Centre for Terrorist Threat Assessment (NCT) as well as by their own analysis.

81. The strengths of the process and results of the development of the NRAs are the broad agency involvement, and the frank identification and description of the vulnerabilities and knowledge gaps in the 2013 NRA on ML. The latter finding is the basis for the follow up in the form of Brå's 2015 NRA on ML.

82. The main weaknesses of the NRAs on ML are the lack of quantitative data and research in trends and methods. Both NRAs rely heavily on impressions of authorities rather than current data, and the assessments are impeded by the lack of strategic analysis of financial intelligence. Furthermore, the quality and use of statistics relevant for money laundering is uneven and should be developed, especially regarding the proceeds of crime.

83. The two NRAs on ML have been good learning experiences for Sweden, and constitute a good basis for further work on new and current risks. Sweden is currently planning further work on risk assessments, with the goal of further developing timely and comprehensive reports.

National policies to address identified ML/TF risks

84. Sweden's national AML/CFT Strategy of 2014 is the main policy document for AML/CFT. It outlines the high-level priorities and describes a number of measures to be taken in response to the 2013 NRA on ML and 2014 NRA on TF. This includes, for example, various legislative amendments to improve LEAs' tools in pursuing ML, TF, confiscation and cross-border cash movements that have since been implemented. Among the priorities in the strategy is the need to fill knowledge gaps in several areas, and the strategy also points to necessary improvements in co-ordination and analysis, among other things. The strategy identifies high-level institutional and knowledge-building activities. With a few exceptions (such as the special focus areas), it does not contain national priorities to address Sweden's specific ML/TF risks identified (e.g. tax crimes, fraud, organised crime and cash movements). This can most likely be attributed to the fact that the strategy is mainly based on the 2013–2014 NRAs, and it consequently suffers from the knowledge gaps and weaknesses of the NRAs, such as the significant threat of FTFs, and ML risks not identified in the 2013 NRA on ML. There is no formal mechanism of coordination to assess risks and develop policy in Sweden. Nor is there any formal mechanism in place to review and update the strategy. Revisions to it (like the NRAs) are consequently dependent on an active decision from the Government.

85. While Sweden has implemented a number of large, significant and impressive reforms relating to AML/CFT following the Strategy, there is a question of whether these reforms were developed based on the ML/TF risks of Sweden. The majority of legislative measures were explained

2

as having been initiated in response to new (and sometimes not so new) international standards. However, it does not seem like ML/TF risks of particular relevance to Sweden (or the EU) identified in the NRA process or by individual agencies have led to the initiation of new legislation, although once the legislative process was stated, risks are considered. Development of policies and legal tools is included in some ordinances and/or as standing items on the agenda when operational agencies meet ministries, but there are few examples of AML/CFT-related measures or resource allocation enacted on such a basis. A risk-based development seems to be more systematic and well developed in the areas of tax and organised crime.

Exemptions, enhanced and simplified measures

86. As an enhanced measure, Sweden has recognised bitcoin exchangers as a financial institution in Sweden and required them to register with the FSA.[12] Registered bitcoin exchangers are required to apply AML/CFT preventive measures, including filing STRs.

87. Some types of legal entities (NPAs, a few types of foundations) are not required to register their existence with any authority, nor are required to file some basic information (tenant housing associations), but these exemptions from what is required by R.24 were not given on the basis of an assessment of risks.

88. There are also exemptions (some of which are based on EU requirements) from some preventive measures, e.g. certain wire transfer information as a result of the EU Regulation on Wire Transfers (R.16), and for simplified CDD measures by FIs based on EU/EEA vs non-EU/EEA countries, e.g. where third-parties may be based (R.17) and group policies (R.18), which are based on a presumption of low risk, rather than a risk assessment as such.

Objectives and activities of competent authorities

89. The relevant authorities generally base their activities on the established policies, with the national strategy of 2014 being the most significant basis for AML/CFT. As described above, the strategy is a plan of objectives, priorities and measures based on the findings of the 2013–2014 NRAs. While useful for this purpose, the strategy is not a set of national AML/CFT policies, and there is no mechanism for regularly reviewing it and keeping it up to date. Even though there are examples of authorities taking positive steps as a direct result of the strategy, it provides a limited basis for individual authorities to take reference from for their own objectives and activities. In some areas, this is mitigated by other national policies that led some agency priorities, for example the cross-agency commitment to the GOB for organised crime, approaches to confiscation, and the Swedish counter-terrorism strategy with associated implementation initiatives.

90. The consistency between identified risks, and authorities' objectives and activities, are varied. Important authorities on the financial supervision and law enforcement side are to a substantial degree aware of the AML/CFT risks in their areas, and have taken measures in response. The FSA has

12 The FSA considers bitcoin exchangers as providers of payment funds based on para 5 in Annex 1 to 2013/36/EU (the Fourth Capital Requirements Directive and subsequent transposition into Swedish law).

for example increased their focus on currency exchanges and money transmitters, as a result of their assessment in 2015 of the high ML/TF risks posed by the sectors and in line with the national strategy. The FSA has also, in cooperation with EBM, produced a typology on activities related to high-risk issues such as false invoices, currency exchange and cash handling. On the other hand, DNFBP supervisors seem to have targeted ML/TF but it is not risk-based, although there are steps in that direction, e.g. the three CABs have carried out a risk classification exercise of the entities under their charge. The Police Authority's high-level guidance is set by the government in the annual budgetary appropriations process, an example of which is tasking it to increase the level of confiscations, while at the operational level the authority has broad discretion to determine how the guidance is followed.

91. Weaknesses in coordination have also led to inadequate sharing of risk information and agencies' pursuing their own priorities rather than on the basis of national AML/CFT risk. Improvements are most prominent in the cooperation between LEAs (hereunder the FIU) and supervisors (see more under the section on coordination).

National coordination and cooperation

92. Sweden does not have a national coordination mechanism for AML/CFT policies and activities, and operational cooperation and coordination is varied. There are formal and informal mechanisms and cooperation in areas relevant for AML/CFT, and in some instances there have been direct instructions from the Government to cooperate on certain issues. There doesn't seem to be any formal obstacle to effective cooperation and coordination. Some formal mechanisms exist, most notably the Coordinating Supervisory Body, which is tasked to enhance AML/CFT supervisory efforts, and where LEAs also provide inputs. While it is a formal structure, its scope is limited to supervisory cooperation and lacks a mandate to play a larger role in coordinating AML/CFT policy and activities.

93. Sweden's largest challenge is the cooperation and coordination of a fairly complex structure of key agencies in the field of AML/CFT. Swedish authorities are aware of the deficiencies, which are identified both in the 2013 NRA on ML and the Strategy of 2014, but at the time of the onsite, the deficiencies had not been addressed. The mentioned documents and interviews with key agencies show that the system is not working together in a wholly adequate manner, as agencies pursue different priorities and do not ensure a comprehensive approach to, for example, the identification and sharing of risk information, feedback to the private sector, and coordinated action against reporting entity non-compliance or criminal breaches of the AML/CFT requirements.

94. The weaknesses in cooperation and coordination seem to start at the policy level. The key ministries and agencies have not shown that they coordinate priorities, resource allocation or instructions between themselves in an effective manner. In addition, without a national coordination mechanism, there is also a lack of a platform where the Government and operational agencies can systematically coordinate AML/CFT priorities, resource allocation, and activities to ensure the development of policies based on operational experience and evolving risks.

95. Furthermore, while there are examples of good operational cooperation between agencies, this is mostly ad hoc and informal, and varies greatly. Good results have been achieved in the efforts

to counter organised crime, through the formalised GOB framework, where a number of agencies contribute resources and expertise to target criminal individuals and environments. However, key deficiencies exist in the missing cooperation, weak communication between law enforcement and supervisory agencies, lack of procedures, and lack of clear division of labour between LEAs and Fipo on one side, and supervisors/economic agencies on the other. The most important concerns are as follows:

- Fipo has to a very limited degree developed typologies and strategic analytical products, which both impedes its own work, but also that of other LEAs and supervisors. This leads to for example the FSA and other supervisors not being able to set priorities based on risks informed by financial intelligence.
- The risk information being detected by police and prosecutors in the course of investigations and prosecution, most significantly in NOA and EBM, is not shared with the supervisors, again an obstacle to forming effective risk-based priorities.
- There is a lack of coordination mechanisms, e.g. instructions or guidelines, on how the authorities should handle reporting entities' AML/CFT compliance failures. While this is an area that is being explored in the context of specific cases investigated and prosecuted by LEAs, it is unclear how LEAs and the supervisors would coordinate and decide whether a case should be handled through supervisory sanctions or criminal enforcement action (or a combination).
- Feedback to reporting entities on STR filing is inadequate. This is elaborated on under the sections covering IO.3 and IO.6 below.

Private sector's awareness of national AML/CFT risk assessments

96. The authorities mainly communicate risks to the private sector by making the mentioned NRAs available publicly. Private sector entities that participated in the development of the NRAs would be more familiar with the reports. In the context of Brå's 2015 NRA on ML, the results were actively communicated and shared with the private sector through seminars. Similarly, the TF follow-up report produced by CATS was followed by a workshop arranged by the FSA where results and conclusions were communicated to the private sector. Although significant, this does not, however, allow for a current and continuous communication to the private sector of the authorities' risk understanding that is not contained in the NRAs or in other reports. While the authorities do conduct a good amount of outreach on new risks and trends on specific topics, e.g. on TF, the communication on national ML/TF risks as a whole is inadequate, not least as a result of the concerns identified above.

Conclusions

97. Through the development of the NRAs, Sweden has enhanced its risk understanding on ML. Work remains on filling knowledge gaps and developing further risk assessments based on a broader use of methods, tools, and information. Key agencies in Sweden have gone beyond their limited NRAs in terms of identification and understanding of the risks that Sweden faces, but this is not consistent across authorities, which limits how Sweden is able to address its risks, in particular areas that have been identified as higher risk. Nonetheless, the authorities have expressed commitment to improve their national understanding of ML/TF risks. The understanding of TF risks is overall better than that of ML risk.

98. Sweden's national strategy address key deficiencies identified by the 2013–14 NRAs, and there are some mechanisms for cooperation between authorities. Sweden uses their understanding of risk to inform policy development, and actions to mitigate risks, only to some degree. Sweden does not have a national coordination mechanism for AML/CFT strategies, policies and activities. Operational cooperation and coordination is varied. Deficiencies relating to cooperation, coordination and feedback have a knock-on effect on Sweden's effectiveness in other areas, such as in providing guidance on typologies to the private sector and in setting supervisory priorities based on risks informed by financial intelligence.

99. Sweden has achieved a moderate level of effectiveness for IO.1.

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Key Findings and Recommended Actions

Key Findings

Use of financial intelligence (Immediate Outcome 6)

- Sweden systematically accesses and uses financial intelligence and other relevant information in investigations of ML cases and in tracing criminal proceeds. Financial information is routinely used by law enforcement agencies to develop evidence and trace criminal proceeds in relation to ML, TF, and other crimes, and for intelligence purposes. The ability of Sweden to access and use financial intelligence has improved since July 2014, when the new ML offence entered into force and the FIU started putting focus on the ML offence and not just on predicate offences. Several major investigations have been undertaken on the basis of STRs, and the FIU plays a key role in supporting investigations with financial intelligence in response to law enforcement requests.
- However, the FIU (Financial Police – "Fipo") has not yet achieved its potential because its operational analysis is not able to identify complex cases of money laundering. This is mainly due to the inadequate IT tools that do not allow for transaction pattern recognition. Fipo's strategic analysis function is still being established and it does not yet produce strategic intelligence products that could support operational analysis and provide guidance and feedback to supervisors and reporting entities.
- Competent authorities cooperate well on financial intelligence; however there is no formal feedback from law enforcement agencies to Fipo. There are also weaknesses in Fipo's guidance and feedback to the FSA, supervisory authorities and reporting entities. These factors hamper the ability of Sweden to access and use financial intelligence and other information, and also limit potential for Fipo to assess its own ability to conduct analysis.

ML Investigation and prosecution (Immediate Outcome 7)

- The new ML offence in force since July 2014 has greatly improved Sweden's ability to investigate and prosecute ML, particularly because of the need to simply prove that laundered property "derives from criminal activity". Before July 2014, the predicate offence had to be confirmed in court before someone could be convicte d of ML ("handling stolen money"), which severely limited LEAs' ability to investigate and prosecute ML activity, which basically focused on proving the predicate offence.
- Since July 2014, the new legislation has been used proactively and has contributed to good results in a short time period. A relatively large number of different types of ML have been investigated, prosecuted and convicted, particularly targeting stand-alone ML. The authorities showed high degree of commitment to the new ML offence, particularly embedding the ML offence within their structure and practices. Improvements are still needed in relation to the understanding of the ML scenarios. This should lead to investigation and prosecution of third-party ML, particularly large scale cases.

3

- Due to the legislation being relatively new, it is not yet clear whether the sanctions imposed are fully effective and dissuasive.
- Lack of comprehensive statistics on all convictions of ML (due in part to the application of the principle of concurrent offences and sentencing practices in Sweden), limits the ability of the authorities to monitor convictions and fully understand the impact of the new legislation.

Confiscation (Immediate Outcome 8)

- The authorities consider depriving criminals of their assets to be a highly dissuasive penalty at their disposal, equivalent to a criminal punishment – and therefore prioritise tracing and confiscating assets as an important part of the penalty for crimes. The new ML offence in force since July 2014 significantly improved the ability of the authorities to secure assets at an early stage (through Prohibitions on Disposal of Property, i.e. freezing), and to confiscate criminal money. Asset tracing investigations are effective.
- The Government's policy to make crime unprofitable is pursued through a number of legal means, and the statistics suggest that, when criminal activity is detected, Swedish LEAs do efficiently trace assets, take measures to secure them, and are increasingly able to ensure that judges award the confiscation of criminal assets. While confiscation is generally pursued as a policy objective, some of the authorities lack the tools and indicators to measure whether the objectives are being met.
- The lack of clear statistics on the assets recovered from criminals make it challenging to quantitatively assess the degree to which Sweden achieves the objectives of its confiscation policies. Even though complete information on the sums recovered from criminals are not available, the evidence presented and the case examples provided indicate that these represent significant sums which are broadly consistent with the crime environment. In particular for tax crimes, which are the most significant proceeds-generating crimes in Sweden, significant assets are recovered using tax recovery procedures.
- The identification and seizure of cash by Customs could be improved, and the efforts to uncover ML through transportation of cash do not reflect the risks identified.

Recommended Actions

Immediate Outcome 6

- Sweden should significantly increase the use of financial intelligence to identify complex cases of ML as well as professional ML. To do this, Fipo should improve operational analysis by urgently developing a sophisticated IT system that allows patterns detection; and by developing strategic analysis to be used in patterns recognition. Then, Fipo should adapt its analytical techniques to better integrate and exploit STRs and other available information. Fipo should also start conducting appropriate strategic analysis to identify patterns, trends, and profile of ML activities and actors.
- Sweden should ensure that Fipo makes better use of crime reports made to the Police, particularly by improving communication between the Fraud Reporting Centre and Fipo.
- Sweden should improve cooperation between Fipo and other authorities in order to measure

the effectiveness of the information disseminated by Fipo. Sweden should develop a more organised forum for formal feedback between competent authorities.[13] LEAs should give Fipo better feedback. Fipo should provide better information on typologies, trends, and financial profiles to the supervisors and private sector. Given the risk posed by straw persons, Fipo should particularly develop knowledge and red flag indicators on this issue, and raise awareness with reporting entities.

Immediate Outcome 7

- Sweden should monitor sanctions imposed for ML, and consider whether they are effective and dissuasive, especially for repeat offenders. Appropriate cases should be prosecuted and appealed to the Supreme Court to establish further precedent on the level of sanctions for the new ML offence.
- Sweden should further develop statistics and other forms of evidence and analysis to enable identification of all different types of money laundering offences investigated.
- Sweden should place a larger priority on identifying, investigating and prosecuting professional enablers and facilitators of ML.

Immediate Outcome 8

- Sweden should improve its ability to provide comprehensive statistical support on confiscation and related measures to deprive criminals of proceeds, and develop a consistent and uniform approach across agencies. The new statistical tool should provide comprehensive data on the value of assets deprived from criminals (both money and other property), whether from confiscation, victim restitution or tax surcharges, and should show the link from seizure, to confiscation requests, confiscation decisions and recovered confiscations.
- Sweden should further develop its policies and internal guidelines on confiscation, for example by developing more concrete criteria for success. Tools should be developed to assess the performance of all relevant levels of LEAs in the field of confiscation.
- Sweden should consider undertaking a study to better understand the size of the illegal economy and/or sums thought to be laundered, and use this use this understanding in setting strategy for confiscation.
- Sweden should target falsely / not declared or disclosed cross-border movements of currency, and develop the geographical scope of these efforts.[14]
- Sweden should consider taking a more active approach to the confiscation of companies, where appropriate.

13 Sweden is setting-up a centre for financial intelligence where different competent authorities will be able to make better use of financial intelligence and exchange feedback.

14 In 2016, the Police, in collaboration with Customs, has already established a cash team to focus on seizing cash at targeted ports.

100. 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.3, R.4 & R.29-32.

3

Immediate Outcome 6 (Financial intelligence ML/TF)

101. Sweden systematically accesses and uses financial intelligence and other relevant information in investigations of ML cases and to trace criminal proceeds. However, financial intelligence is used to a lesser extent with regard to complex ML cases. This is due to fact that the FIU (Fipo) prioritises the pursuit of links between the predicate and the money, but is not sufficiently able to recognise transaction patterns (following the trail of particular activities or transactions without a specific target).

102. It should be noted that the work of Fipo has improved since July 2014, with Fipo putting more focus on the ML offence, while previously Fipo only focused on establishing any possible predicate offence and a group of dedicated financial investigators assisted other Police units in asset recovery investigations. Now Fipo can also issue orders to temporarily freeze assets related to suspicious transactions (Prohibition on Disposal of Property – PDPs).

103. Fipo's analysis is categorised in: (i) case reports (when the analysis of data indicates that a crime may have been committed), (ii) "intelligence documents" (cases when the information managed by Fipo could be of interest for future criminal investigations but is not sufficiently tangible to constitute grounds to suspect a crime), or (iii) "ad acta" (when the analysis does not lead to any dissemination, the STR is filed for five years.

Use of financial intelligence and other information

104. The main authority dealing with financial intelligence is Fipo, although a number of other authorities produce and use financial intelligence for the purpose of developing ML investigations. Financial intelligence related to TF is mainly dealt with by Säpo.

105. Fipo uses financial intelligence mainly to investigate possible criminal activity and develop evidence in criminal cases where there is a direct or close link between the transaction and an offence (generally a predicate offence such as simple fraud, tax evasion, abuse of social security). Financial intelligence is also used to trace criminal proceeds. When an STR is received, case officers cross-check it against the database maintained by Fipo, as well as the databases maintained by the Police and other government agencies. Fipo also obtains additional information from reporting entities and other agencies. With the information available, Fipo is able to follow the trail of transactions and activities when these are linked to a specific target.

106. However, financial intelligence rarely identifies complex money laundering schemes or cases of professional money laundering. The ability to identify such cases mainly rests on LEAs' investigative techniques (see IO.7). Between July 2014 and December 2015, Fipo reported only one case of a commercial ML offence, and the cases presented to the assessment team show that the majority of investigations based on case reports are simple ML or asset tracing cases, and only rarely

include more sophisticated ML cases. This seems to reflect the fact Fipo does not have the capacity to link seemingly unrelated STRs and does not follow the trail of particular activities or transactions without a specific target. It may also reflect that Fipo's capacity to identify and analyse the ML offence itself (as opposed to the predicate crime) is at initial stages. As a consequence, Fipo does not identify targets based on suspicious patterns of activity.

107. The main reason why Fipo is not capable to identify targets based on suspicious patterns of activity is the inadequate IT tools available, which do not allow establishing transaction links between different STRs. This type of operational analysis is also hindered as a result of the fact that Fipo does not conduct strategic analysis, and therefore has not been able to develop profiles or tools that might be used to identify patterns of ML behaviour (see below).

108. Fipo does not fully exploit the intelligence value of the information available to it, particularly the STRs received. As can be seen from the table below, a small number of STRs received are disseminated; the rest is filed "ad acta" (i.e. STRs that are archived). Each case report or intelligence document normally includes more than one STR (on average, 5 STRs per case report). Fipo indicated that around 70-80% of the STRs are not further processed after initial scrutiny due to resource shortages. The percentage of STRs disseminated is considered relatively low, given that the total number of STRs received is also generally low and the quality of the STRs is generally good for a large part of them. The small amount of dissemination is mainly the result of the way Fipo conducts operational analysis, as described above, but is also the consequence of inadequate IT tools. A number of STRs which were previously filed in paper form have not yet been fully digitalised (only information on the individuals and/or companies involved has been). As a consequence, peripheral information in many STRs may never be made readily available for use in analysis or investigations.

Table 4. **Fipo's STR analysis and share of STRs**

	2014	2015
Received STRs	9 183	10 170
Case Reports	45	54
Intelligence Documents	1 218	796
Ad Acta	7 920	9 320

109. The "case reports" which are disseminated are used by LEAs to launch criminal investigations (see also below). With regard to the "intelligence documents", it is unclear the extent to which they are used. Fipo indicated that they are used in ongoing investigations, or in assisting with new investigations, however, Fipo does not monitor their use (see below). Fipo only receives regular feedback from the tax office (STA) and from the SPA and EBM on an informal basis. The STA and EBM indicated that "intelligence documents" are often used for their investigations.

110. Besides Fipo, other authorities produce and use financial intelligence for AML purposes. This is particularly the case for the National Operations Department (NOA), the tax authorities, SPA, and EBM, who have the resources and expertise to identify and develop ML cases on the basis of financial

intelligence (see beginning of IO.7 for more details). Financial intelligence is also used in the context of the Coordination against Organised Crime (GOB) initiative. Fipo actively participates in investigations and collaborates with other LEAs by directly providing information and replying to specific requests. Customs receives border transaction reports and files them to Fipo every week, however it does not add much value to the information received, though the Border Police does (see below).

111. The table below shows that most ML cases originate from authorities other than Fipo. These figures indicate that only a limited number of ML offences are reported by Fipo, compared to the ML reporting by the authorities. The majority of ML investigations originated from investigations of fraud offences, or when the Police finds cash or property clearly linked to criminal activities (such as drug-dealing). Financial intelligence is sometimes used in these investigations, with the support of Fipo.

Table 5. **Offences reported by Fipo compared with total reported offences**

	2014			2015		
	FIU	**other**	**FIU share (%)**	**FIU**	**other**	**FIU share (%)**
ML offence	53	305	17	100	980	10
ML offence – gross	27	43	63	34	252	13
ML offence – petty	0	3	0	0	17	0
Commercial ML	0	5	0	0	128	0
Commercial ML – gross	0	1	0	1	457	0.01
Commercial ML – petty	0	0	0	0	0	0
All ML offences	82	357	23	135	1 834	7

112. Fipo and LEAs appear to use financial intelligence for asset-tracing to a good extent, which reflects a long-standing expertise by Fipo on this issue. Fipo has dedicated staff and is able to assist LEAs with complicated cases of asset tracing. Since July 2014, as soon as an STR is received, Fipo tries to identify whether a transaction may be temporarily frozen for two days, and sends a case report to the relevant prosecutor, who must decide on whether to uphold the measure. This measure (called Prohibition on Disposal of Property – PDP) has proven quite effective in identifying and securing assets from the very beginning of an investigation. In 2014 (July-December) Fipo imposed PDPs in 25 cases for a value of SEK 3.5 million (approximately EUR 370 000); in 2015, Fipo imposed 72 PDPs for SEK 7.2 million (approximately EUR 750 000). All cases were upheld by the prosecutor, leading to seizure. The main reason for the PDP measures were cases of fraud.

Table 6. **PDP Cases and Related Offences**

	PDP Cases	Predicate Offences	Frozen
Jul – Dec 2014	25	15: frauds (9 abroad, 6 domestic) 9 tax offences 1 trade-related offence	SEK 3.5 million (approx. EUR 370 000)
Jan – Dec 2015	72	72 frauds (36 abroad, 36 domestic)	SEK 7.2 million (approx. EUR 750 000)
Jan – May 2016	32	32 frauds (15 abroad, 17 domestic)	SEK 12 million (approx. EUR 1.3 million) [1]

Table Note
1. From June to November 2016, there have been 22 more PDP for a total value of SEK 21.3 million (approximately EUR 2.2 million).

Box 1. **Case study: The use of intelligence in ML cases**

In autumn 2015 Fipo received intelligence information indicating that specific accounts in a Chinese bank would be used for money laundering and that a person of strategic interest controlled the accounts. A request was made to the largest four banks in Sweden in order to identify outgoing transactions to these accounts since January 2015. Almost at the same time as the request, a bank notified Fipo of payments with a fraudulent source to mentioned accounts. Fipo sized approximately SEK 300 000 (approximately EUR 31 000) in PDPs, but approximately SEK 200 000 (approximately EUR 22 000) were executed. During 2015 at least SEK 4.2 million (approximately EUR 420 000) were or were supposed to be transferred to the mentioned accounts. Some transactions, before the request was made to the banks, were executed, however after the request, several were stopped by the banks. The intelligence case concerning the mastermind of the accounts is ongoing and several investigations are concluded or ongoing. Furthermore some other intelligence sub cases have initiated due to this primary case.

113. Financial intelligence related to TF is mainly analysed by Säpo, which is in charge of TF investigations, including financial investigations (see IO.9 below). Fipo immediately disseminates to Säpo the information in all STRs which are marked by the reporting entities as related to TF. In addition, two case officers in Fipo analyse these STRs and seek to identify other STRs that might be linked to TF. Fipo disseminates the analysis to Säpo and responds to related queries from Säpo. In 2014 and 2015, Fipo disseminated to Säpo around 140 intelligence documents. Säpo indicated that it used the information provided by Fipo. Both Fipo and Säpo can impose PDPs in case of suspected TF.

STRs received and requested by competent authorities

114. Fipo received between 8 000 and 12 000 STRs a year between 2010 and 2015, mainly from the four largest banks (detailed figures of STR reporting are in Table 18). These STRs are useful for the purpose of operational analysis conducted by Fipo. By receiving information from Fipo or requesting information from Fipo, Swedish competent authorities are using information derived

from STRs and other reports to perform their duties. Feedback from the LEAs such as the Police Authority, EBM, the STA, Säpo, etc. has been positive, recognizing the value and usefulness of Fipo's financial intelligence reports for initiating and supporting their investigations. This feedback is supported by numerous cases and statistics on a relatively high number of investigations, and positive outcomes achieved in these cases (see below).

115. The quality of the STRs has improved over time, and is generally good for a large part of them. As noted under IO.4, several large financial institutions used to file a number of poor quality reports that were unusable by Fipo; however Fipo indicated that the quality of the STRs from banks has improved over the past two years, particularly since the introduction of a compulsory electronic form. The quality of STR reporting from the rest of the reporting entities is not yet fully satisfactory, and up until recently some STRs were filed in paper form.

116. Some reporting entities (the four large banks, MVTs, and casinos) submit a reasonable amount of STRs; however, there are concerns that other institutions and sectors file a relatively low level of STRs. As highlighted under IO.4, 179 entities filed STRs in 2015, representing around 0.35% of the total number of reporting entities. The reason underlying the low level of STR reporting from securities and insurance could be that these sectors are largely dominated by banks, which handle STRs in an integrated manner. Since the NRA inadequately addressed the risk of ML through the financial sector (see IO.1), there is uncertainty as to the amount of ML carried out within the financial sector and whether the appropriate level of STR filing from this sector is currently adequate.

117. With regard to non-financial operators, including sectors that are considered vulnerable, such as real estate, the low level of reporting could be attributed to an uneven understanding of the reporting obligations by these entities, which is partly due to the lack of adequate AML/CFT supervision of some sectors (see IO.3) and partly to the little feedback, instructions and guidelines provided by Fipo (see IO.4). Overall, with the very limited guidance on typologies, red flags and indicators, insufficient information shared by Fipo and LEAs, and limited or no interaction with the relevant supervisor, it will be difficult for reporting entities to effectively recognise suspicious transactions and enhance the number and quality of the STRs. Sweden indicated having a project within the Coordinating Supervisory Body to increase the low level of STR filing.

118. Besides STRs, there is information on potential cases of ML which is not immediately available for use by Fipo. There is no automatic mechanism for Fipo to use Police's money laundering offences data collected by the regional police. Cases of fraud identified by financial operators are also not directly available to Fipo, as transactions that clearly indicate patterns of fraud are reported directly to the "Fraud Reporting Centre" of the Police,[15] and although Fipo can access these data, there is no automatic mechanism to pass this information on to Fipo.

119. The table below shows the reasons for suspicion of the STRs filed. After foreign transactions, large amount transactions and repeated cash deposit/transactions are the largest grounds for suspicious transaction reporting. Fipo indicated that these STRs are mostly related to tax evasion

15 A reason for this is that major banks have a "fraud unit", which works independently from the AML/CFT compliance unit.

and fraud, which seem to properly reflect the NRAs. The emphasis on cash as a suspicion for ML activity is also consistent with the risk assessment; however, it does not necessarily reflect the risk of ML through more sophisticated means. Straw persons are not often identified by reporting entities, while the ML investigations conducted by Sweden suggest that straw persons are often misused (see also IO.7, IO.4, and IO.5).

Table 7. **Reasons for Suspicion of STR filings (%, Jan 2013 - Jun 2016)**[1]

Reason for suspicion	2013	2014	2015	2016 (June)
Repeated foreign transactions/large foreign transaction	27.2	33.2	30.6	18.8
Irregular transaction	11.4	14.8	22.2	23.1
Repeated transactions/large transactions to an account	8.8	14.4	12.9	27.7
Repeated cash withdrawals/large cash withdrawal	17.1	9.9	6.5	5.0
Repeated cash deposits/large cash deposit	11.7	9.1	10.1	6.5
Presumably the customer submitted false information	4.1	4.5	4.1	5.8
Repeated currency exchange/large exchange	9.4	3.8	2.6	1.8
The customer is likely to be an agent (straw person)	1.3	1.7	1.1	1.7
Repeated cash purchases/large cash purchase	1.7	1.2	0.8	0.6
Coloured notes	0.2	0.1	0	0.1
Terrorism financing	0.1	0.3	0.7	1.7
Other	7.1	7.0	8.4	7.3

Table Note
1. Fipo developed the framework and reporting entities must tick only one box when submitting the STR.

120. TF reporting is increasing, which may be due to the continuing awareness-raising activity carried out jointly by Fipo and Säpo, e.g. with a seminar on TF in November 2015. The 2015 follow-up report to the TF NRA produced by the Swedish Defence University, and the succeeding seminar arranged by the FSA which was directed towards obliged entities, may also have had a positive effect on the knowledge and consequently the reporting of TF.

121. Fipo also receives cash declaration reports of movements of over EUR 10 000 across the EU border reported initially to Customs (since 2016, once a week; previously, once a month). The number of declarations steadily increased (from 213 in 2010, to 851 in 2014), possibly thanks to an information campaign made by Customs on the obligation to declare. Fipo uses these cash reports, but it is unclear the extent to which cash reports are useful to Fipo or other authorities in ML and TF investigations (see also IO.8).

Operational needs supported by FIU analysis and dissemination

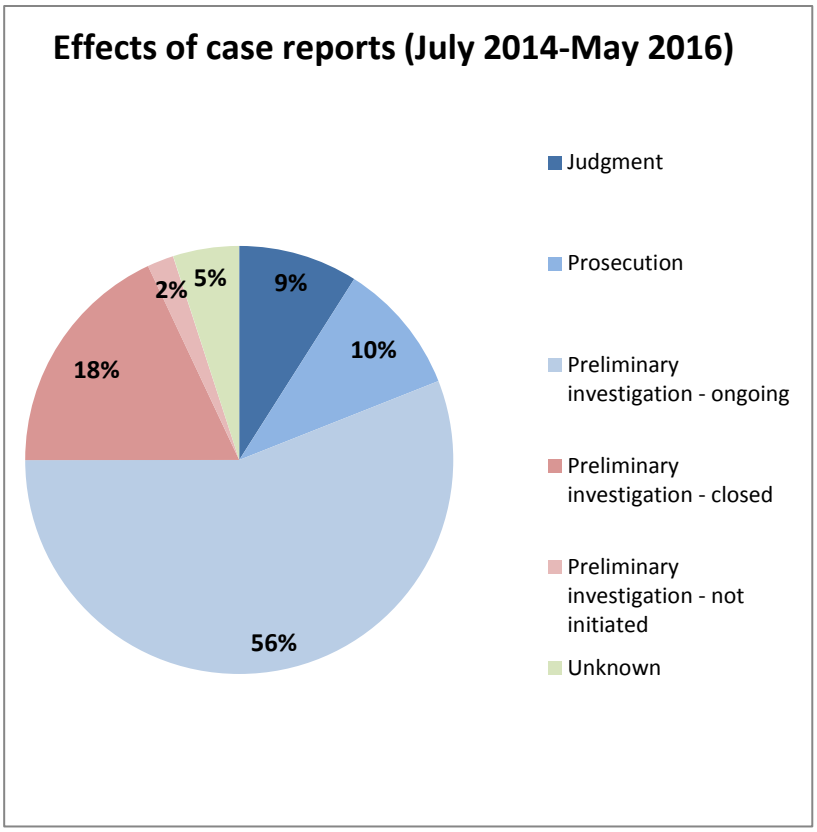
122. Fipo starts its operational analysis upon receipt of an STR with the purpose to establish if there are sufficient grounds to proceed to other measures, such as a criminal investigation. This means that Fipo analyses whether the transaction(s)/assets may be linked to criminal activity, including stand-alone ML since July 2014. Fipo also proactively initiates analysis without a specific STR. In such cases, Fipo collects information from sources of information and reporting entities, for example to chart a person's or a company's economic situation, connections to other persons or companies, and connections to their own or others' criminal activity. Fipo started "initiative cases" 11 times in 2013, 19 times in 2014 and 17 times in 2015. In 2016 (up to the end of November) Fipo had opened 25 initiative cases, including 17 relating to TF, and one in response to a foreign request. Initiative cases normally relate to TF, on input from Säpo (in at least 45 cases), but also to tax offences and fraud.

123. Fipo accesses additional information from the money laundering register, databases maintained by other authorities,[16] and reporting entities. Additional information from reporting entities can be collected when there is "cause to believe" that a crime has been committed and an investigation can be opened. The Swedish authorities have indicated that the threshold is very low. Fipo has indicated that an STR is per se sufficient to reach that level and request additional information from any reporting entity, including bank details. In order to facilitate access to additional information from reporting entities, Fipo uses a template form for banks and all other reporting entities. In practice, Fipo has not experienced any problem obtaining additional information from reporting entities.

124. Once the analysis is complete, Fipo disseminates information in the form of case reports and intelligence documents. A case report is disseminated by Fipo when analysis indicates that a crime may have been committed. Case reports contain intelligence information which is adapted to be part of a criminal investigation. Fipo started disseminating financial intelligence in the form of case reports in July 2014; previously it disseminated information in another form. For the period 1 of July 2014 – May 2016, Fipo disseminated 128 Case reports, 11 (8.6%) to EBM and 117 (91.4%) to the pre-investigation teams in the police. The figure below shows the use of case reports in preliminary investigations and prosecutions.

16 Fipo has access to information in the Police Authority's databases including the criminal records register (criminal convictions), suspicion register (actively suspected crime), the general surveillance register (intelligence information) and the central investigation register (operative register for modus operandi). Fipo also has direct access to information held by other authorities, such as census information, tax data, registries of property ownership, vehicle ownership, family relations and company information. Fipo can also obtain on request information from Säpo; the Police Authority regularly receives national and regional intelligence pictures on suspicious actors. On request, Fipo can also obtain information from Swedish Social Insurance Agency, the Swedish Prison and Probation Service, the Swedish Enforcement Authority, the SPA, the Swedish Migration Agency, the Swedish Employment Agency and the Swedish Coast Guard.

Figure 1. **Effects of 128 Case Reports– July 2014-May 2016**



125. The figure shows that 19% of 128 operative reports have led to either prosecution or judgment, while 20% resulted in the pre-investigation not starting at all or being closed down. The authorities interviewed during the on-site visit confirmed that the operative reports were generally thorough and useful to the investigations. Fipo indicated that in a number of cases, the preliminary investigation was closed because the investigators decided to focus on the predicate crime as opposed to the ML offence. The relatively high level of investigations opened following dissemination of a case report (at least 93% of the case reports resulted in a criminal preliminary investigation) is an indication of good quality analysis. However, this should not be overestimated given that the law obliges the police and prosecutors to open an investigation when there is "cause to believe" that a crime has been committed and an operative report should already indicate that a crime may have been committed.

126. The usefulness of the other form of dissemination –"intelligence documents" – is less clear. Fipo disseminates around 1 000 intelligence documents each year to LEAs and other authorities — about 19% of which related to TF, 81% related to ML or predicate offence. Intelligence documents are disseminated when Fipo's analysis does not lead to sufficiently tangible grounds to suspect a crime, yet the information may be of interest to an investigative authority. The recipient is then able to combine the information with other intelligence material for criminal investigations or preventive measures.

127. Fipo does not have a formal mechanism to track if and how intelligence is used. Intelligence documents disseminated to the police are uploaded to the police databases, and any police officer

(with access rights) can access it directly. EBM receives these documents directly, and indicated that they are useful, although they could be more developed (from January to May 2016, EBM received 200 intelligence documents, 24 of which led to opening a criminal investigation). Fipo and the Tax Agency (STA) have a close relationship, and Fipo indicated that around 75% of the information provided to the STA is used (even though this figure includes specific requests for information, and does not just relate to the use of intelligence documents). On the basis of informal cooperation and feedback, LEAs seem to make use of intelligence documents; however, it is difficult to establish their actual usefulness as there is no formal mechanism to track their use.

Table 8. **Fipo's Dissemination of Intelligence Documents**

Receiving Authorities	2014		2015	
Economic Crime Authority (EBM)	557	51.3%	204	26.6%
Police Authority	147	13.5%	177	23.1%
Tax Agency (STA)	146	13.5%	162	21.1%
Security Service (Säpo)	135	12.4%	147	19.2%
Regional Intelligence Centres (RUCs)	56	5.2%	49	6.4%
Customs (TV)	16	1.5%	6	0.8%
Foreign FIUs	4	0.4%	7	0.9%
Others	24	2.2%	14	1.8%
Total	**1 085**	**100.0%**	**766**	**100.0%**

128. The figures presented above indicate that Fipo disseminates reports to a range of agencies. Fipo's dissemination is useful to some extent. The quality of the case reports is quite good, which is demonstrated by the use made by LEAs. It is not clear if and how intelligence documents are used. In any case, the level of dissemination is relatively low compared to the number of STRs received, and the broad access to additional information available to Fipo.

129. As mentioned above, Fipo's analysis and dissemination is useful to investigate relatively simple ML cases where there is a direct or close link to the predicate offence (e.g. simple fraud, tax evasion, abuse of social security) and to trace criminal proceeds. Many cases were provided to the assessment team concerning the identification of links between a predicate offence, the transaction and the person involved. However, only very few related to cases where Fipo was able to identify complex money laundering schemes or cases of professional money laundering. This seems to reflect, among other reasons, the weak capacity of Fipo to analyse information from a pool of STRs as a whole when they are available.

130. The main reason why operational analysis is not fully developed yet is that Fipo does not have adequate IT tools. Fipo's analysis is normally conducted through standardised working method for operational intelligence analysis (the ANACAPA method) supported by IT tools developed, customised and managed by the Police Authority (iBase, Analyst Notebook, Surfa and Excel). These

tools allow for cross-matching of information available in the databases and are useful to identify whether a person is linked to criminal activity and whether a transaction is linked to a person who is suspected of a crime. As such, the IT tools are good to identify cases of predicate offence, ML or TF where there is a close link (direct or immediate) to criminal activity.

131. However, the IT tools are not sophisticated enough to identify profiles or patterns indicating suspicious activity, involving seemingly unrelated transactions. With the present IT tools, Fipo cannot easily exploit its archive of STRs to identify complex ML cases or cases of professional money laundering and only focuses on identifying relatively simple cases – although its investigative role does include complex cases, once these have been identified. As a consequence, many STRs remain under-utilised for identifying criminal activity and the systematic feedback to reporting entities is limited.

132. Fipo acknowledged the need for modern IT tools that would improve the efficiency of its analytical work. Fipo indicated that a new IT system for receiving and analysing STRs has been under construction for several years, but has been delayed due to technical challenges. Fipo intends to buy "goAML" to help with data extraction, development of statistics, and collect information in a separate database. Fipo is also recruiting one or more IT experts to implement goAML and enhance data analysis (at the time of the onsite visit, there was no dedicated IT expert in Fipo, as Fipo relied only on the IT system and personnel provided by the Police Authority). Better software would allow Fipo to improve the quantity and quality of analysis and dissemination.

133. Fipo does not have in place clear procedural measures to support operational analysis, such as an internal regulation or manual on information analysis, established internal procedures for analysis, comprehensive statistics on each analysis step, and relevant feedback as a result of operational analysis.

134. Fipo's operative analysis is also limited because Fipo does not conduct strategic analysis that might identify patterns of ML behaviour. Strategic analysis is heavily hindered by the lack of modern tools (as mentioned above), but also by its own understanding of what strategic analysis should achieve. The focus of strategic analyses seems to be on making use of aggregate data and statistical analysis. Fipo recently realised the importance of this analysis, and hired analysts to focus on strategic analysis. At the time of the on-site visit, Fipo did not have the capacity to do strategic analysis of risks, trends, methods of ML behaviour that would allow it to develop profiles, provide feedback, or develop tools for operational analysis, although plans were underway to enhance its capacity in this area.[17]

135. Furthermore, LEAs do not regularly provide Fipo with feedback after using the financial intelligence disseminated by Fipo, which would give it additional opportunity to develop its analytical skills in operational and strategic analyses. Importantly, strategic analysis is not used as a basis to develop behavioural patterns that could be used for operative analysis.

136. Fipo's dissemination supports the operational needs of competent authorities only to a limited extent. Swedish LEAs access and use to a good extent financial intelligence in their investigations mainly for developing evidence of cases of ML where there is a direct or close link to

[17] After the on-site visit, Fipo had already hired three analysts to work on strategic analysis.

the predicate offence (e.g. fraud, tax evasion, abuse of social security) and to trace criminal proceeds. However, mainly because of the limitations in operational analysis and the lack of strategic analysis, financial intelligence is used to a less extent with regard to complex money laundering schemes or cases of professional money laundering.

Cooperation and exchange of information/financial intelligence

137. Cooperation and exchange of information and financial intelligence occur on a regular basis and through special projects. Only Fipo has direct access to the money laundering register, but relevant ML/TF-related information is provided to other intelligence and investigative agencies on request, under the provisions of the Public Access to Information and Secrecy Act. Fipo often conducts further analysis on request of other authorities. With regard to organised crime, financial intelligence is used in the context of the GOB initiative, where Fipo staff members participate in the National Intelligence Centre, and at four of the eight Regional Intelligence Centres (Stockholm, Västra Götaland, Syd, and Bergslagen). The head of Fipo is in the executive group at these RUCs, which decides on the cases that the RUCs should focus on and prioritise.

138. The STA and the EBM have seconded case handlers to Fipo since 2012. Intelligence is processed by the case handlers and shared with each respective authority, which shortens the process time and provides an efficient and secure flow of information between Fipo and these authorities. The structure of this cooperation increases the ability to detect and investigate cases, even when they do not clearly relate to ML, but where there are reasons to believe that economic crime or tax crime has occurred. Fipo's case handlers contact the STA in cases of tax offences that may be predicate crimes for ML and where they need access to information only accessible to the STA.

139. While it is clear that competent authorities easily share and cooperate on financial intelligence, there are some weaknesses in the feedback from law enforcement agencies to Fipo, in particular the lack of formal feedback on how the information disseminated by Fipo is used. This limits Fipo's ability to monitor its own effectiveness.

140. There are also weaknesses in Fipo's cooperation with the FSA and other supervisors.[18] The relationship between Fipo and the FSA is not fully exploited, because Fipo has not developed strategic analysis enough, and cannot provide guidance to the FSA, other supervisory authorities and reporting entities on ongoing trends in ML/TF. The little engagement with the private sector means the quality and quantity of STR filing could be improved. Fipo should develop risk information on the different sectors, financial profiles which could be used to identify suspicious patterns of activity for review, and should forward that information in the form of feedback to the supervisors on reporting entities.

141. Fipo and LEAs use secure channels for exchanging information, and protect the confidentiality of information exchanged or used. The information in the Fipo's databases is subject to the same legislation as any other registration or storage of personal data in the context of police operations.

[18] Since the onsite visit, Sweden has communicated that Fipo and FSA have started cooperating in a number of areas.

This ensures that the information is handled in a manner that protects the rights of individuals and data security. Fipo, as well as any other police unit, is regularly assessed by the Swedish Data Protection Authority for compliance with such regulations. The storage and processing of data is facilitated by the universal application of the same regulations across the Police Authority.

142. LEAs generally consider Fipo useful to collect financial intelligence needed in their investigations, and request Fipo to provide information on request in a number of cases, as indicated in the table below.

Table 9. **Fipo's Dissemination on LEAs' Requests**

	2013	2014	2015	2016
Police Investigating Units	12	12	47	24
Swedish Security Service (Säpo)	9	46	65	23
Police Intelligence Units	57	44	41	15
Economic Crime Authority (EBM)	17	37	25	14
Inter-Agency Intelligence Center (RUC & NUC)	36	42	35	5
Swedish Customs	3	9	5	3
Swedish Prosecution Authority (SPA)	1	0	0	1
Swedish Tax Agency (Tax Fraud Investigation)	32	19	6	1
Swedish Financial Supervisory Authority (FSA)	7	3	4	0
Swedish Enforcement Agency	0	0	1	0
Swedish Tax Agency (Fiscal Dept.)	0	0	1	0
Swedish Prison and Probation Service	0	0	0	0
Total	**174**	**212**	**230**	**86**

143. Fipo is actively exchanging information and collaborating with foreign partner FIUs, primarily through FIU.net and the Egmont channel since 2013.

144. To use and develop its analysis, Fipo needs to receive and use information from Swedish police about ML offences that have been identified by the police – the most common source of ML offences. As a way to improve the use of financial intelligence and raise Fipo's profile, Sweden may consider clarifying and simplifying the legal structure of Fipo's establishment and function (although it is clear that Fipo has operational independence and is not subject to any undue influence), and in particular institutionalising its relationship with relevant authorities outside the Police, including Säpo and the FSA, among others. This could be done, for example, through cooperation agreements.

Conclusion

145. Sweden has a systematic mechanism to access and use financial intelligence and other relevant information in investigations of ML cases and to trace criminal proceeds. In these areas,

competent authorities have the resources and skills to use the information to conduct their analysis and financial investigations, to identify and trace the assets, and to develop operational analysis. Assets are secured at an early stage thanks to the use by Fipo of PDPs.

146. However, Fipo is weak in exploiting financial intelligence in the Swedish AML/CFT system, and its potential is not yet fully realised. It is target-focused and prioritises its operational analysis on cases where the link between predicate offence and assets is clearly established. This orientation means less attention is paid to identifying activity or cases where the link to a predicate offence is not immediately evident.

147. Sweden's economy is such that most of transactions occur within the financial system. Fipo has also direct access to a large number of databases with useful information on natural and legal persons. Sweden needs to increase the capacity of Fipo to identify activity associated with money laundering as part of its operational analysis, through more advanced and integrated IT systems and databases. It should also enhance its capacity to conduct strategic analysis and develop profiles, by expanding its staff. It should encourage increased STR filing from certain reporting entities (particularly those involved in vulnerable sectors), and enhancing feedback and supervision on reporting entities. To realise its potential, Fipo needs to enhance its analytic function including strategic analysis and its presence.

148. Sweden has achieved a moderate level of effectiveness for IO.6.

Immediate Outcome 7 (ML Investigation and Prosecution)

149. There are a number of authorities in charge of investigation of money laundering activity: the police for most crimes, prosecutors at the Swedish Prosecution Authority (SPA) and at the specialised Economic Crime Authority (EBM), the tax office for ML related to tax crimes, and in a limited number of cases Customs for ML related to crimes detected across the border. Sweden established a coordination platform called the "GOB initiative" in 2009 to fight against organised crime.

150. A new comprehensive ML offence was introduced in July 2014 replacing the old "handling of stolen money" offence. The new legislation no longer require prosecutors to prove to the criminal standard of evidence the link between the money and the criminal activity; rather, it simply requires that money "derives from criminal activity". Self-laundering has also been criminalised. The new legislation has been used proactively and has contributed to good results in a short time period.

ML identification and investigation

151. Law enforcement agencies and prosecutors have the ability to investigate and prosecute a wide range of ML offences, including standalone ML offences, third-party laundering, foreign predicates and self-laundering. LEAs can also prosecute commercial ML, which refers to culpable risk-taking in the context of business operations or as part of activities that are conducted habitually or extensively. Swedish investigators and prosecutors have a "follow-the-money" attitude that is embedded in their investigative strategies. Therefore there is normally an integrated money

laundering investigation along the investigation of predicate offences as opposed to parallel money laundering investigations.

152. There are examples of stand-alone money laundering investigations, ML linked to various predicate offences (tax crimes and fraud particularly), third-party ML in the form of "commercial" ML; however there have been fewer examples of large scale third-party ML and self-laundering. Investigation of self-laundering is affected by the principle of concurrent offences and the sentencing practice in Sweden (see below). The investigation and prosecution patterns are also influenced by the principle and the practice (see below). The most likely reason why large scale third-party ML cases are not investigated to a sufficient extent is that professional enablers are rarely identified in the first place (see also IO.6 above).

153. Many of the more significant ML investigations (in terms of size and complexity) originate from investigations of tax crimes. A large number of simpler ML cases also originate from police investigations of other predicate offences, which identify money or assets linked to crime (usually cash). Investigators in many cases use financial intelligence as a key input into money laundering and predicate crime investigations and to trace assets (either on dissemination from the FIU, or by requesting specific intelligence from the FIU). When the Tax Agency or EBM receive an operative report from FIU the prosecutor will review and initiate a money laundering investigation. Cash reports from Customs are rarely, or never, used to identify ML activity, but Customs sometimes identifies property that is linked to criminal activity, starts an investigation into the predicate crime and informs the Police about starting a parallel ML investigation if necessary. There were 200 intelligence documents from Fipo to EBM during January-May 2016, and 24 of those cases led to the opening of a criminal investigation.

154. Swedish investigators have developed appropriate skills and experience in investigating and prosecuting ML. Police have conducted in-house training on the new ML legislation, training 600 officers nationwide. The NOA has a financial investigation department consisting of 10 people, a mix of police officers and civilian financial investigators. Around 60 or 70 officers and financial investigators work on asset recovery. In the prosecution chambers, there are prosecutors with specialised ML expertise (at one of the Stockholm chambers for example, 8 prosecutors out of 28 are dedicated to fraud and ML investigations; a major training effort in which all SPA and EBM prosecutors were trained about the new ML legislation took place during 2014, and since then ML is an element in the mandatory training for prosecutors). All prosecution chambers have, or have the possibility to use, forensic accountants to assist in investigations, particularly tracing the proceeds of crime. EBM, as a specialised investigation and prosecution agency focused on economic crimes, represents the gold standard of expertise and investigation in economic crimes, using innovative techniques. Law enforcement structures are flexible enough to enable them to address thematic risks, for example as shown in the coordination against organised crime (GOB) and also for bespoke risks, e.g. the ability of the NOA to put together a task force with specific skill sets as required including the cybercrime unit.

Box 2. **A coordinated approach against organised crime – the GOB initiative**

The GOB was established in 2009 to work together against organised crime from a common platform. This was a political initiative as a result of concerns at the rising influence of organised crime in Södertälje (see below). The GOB is organised as an inter-agency task force of 12 agencies with police in a co-ordinating role. 200 police officers have been allocated to the GOB, and GOB activities are conducted by the participating authorities. All the authorities involved prioritise GOB activity within their operations.

GOB's objective is to bring the Police and other authorities together to ensure an effective and sustainable fight against organised crime, particularly in the areas of companies engaged in criminal activity, unlawful influence, violence and threat. GOB focuses on a number of strategic individuals believed to be linked to organised crime, and its work is based on intelligence exchange between agencies, and network analysis. Potential GOB operations are proposed by intelligence centres and are prioritised by an operational council. They can be taken forward as national operations or regional operations. A financial aspect is always at the forefront of the intelligence, operational tactics, and investigative strategies deployed.

Södertälje

A double homicide linked to organised crime in Södertälje (a town to the south of Stockholm), was the original impetus for creation of the GOB, and demonstrates the approach of focusing on strategic individuals and network analysis. During this investigation a number of economic crimes were revealed, which led to separate investigations.

In one of them, investigators from multiple agencies focused on the criminal networks around the homicides, paying particular attention to economic/tax crimes (as welfare fraud was a principal source of proceeds, along with drug smuggling) in the context of strategic individuals who had considerable influence in the town. Strategic individuals were those who own or control a company, have undue influence, and use violence. Mapping these individuals and networks, and sharing the information in the Regional Intelligence Centres, enabled investigators to understand the criminals' modi operandi and networks. Investigators were able to work with the community to understand social and criminal structures. Financial intelligence and asset investigations through network analysis were used extensively, and the involvement of non-law enforcement authorities - including the Tax Agency and Enforcement Authority - has been crucial.

As of November 2015, 125 persons had been prosecuted as a result of this investigation, with charges including aggravated fraud, extortion, kidnapping and murder. In August 2013, 18 persons (out of 20 charged) were sentenced for inter alia murder, attempted murder and kidnapping to combined prison terms exceeding 75 years; and in June 2014, 34 out of 35 charged were convicted for inter alia aggravated welfare fraud and other fraud and 21 were sentenced to prison for a combined term of more than 47 years. Large amounts in confiscations (SEK 81 million (approximately EUR 8.5 million)) and damages (SEK 31 million (approximately EUR 3.2 million)) were also handed down, and other authorities were furthermore able to claim very large amounts of money back.

Notably, the strategic individuals at the centre of the criminal network have not been directly linked

to crimes of murder, attempted murder, kidnapping, fraud, or drugs offences, but have been prosecuted for economic crimes, such as bookkeeping offences. All available methods of financial evidence were used by the Police, Fipo, the SPA, EBM and the Tax Authority. Examples of these are: interrogation of suspects regarding their assets and their lawful capacity to acquire these; acquisition of bank information, e.g., bank statements, commitment statements, etc.; analysis of money flows, bank accounts, companies etc.; mapping the ownership of assets owned by front persons, e.g., cars, through procedures such as analysing intercepted phone communication, reviewing account information for answers to questions about who pays for insurance, repairs etc., calculation of criminal gains.

This investigation also has international connections; Europol and Eurojust have been used, as have Joint Investigation Teams and European Arrest Warrants; and cooperation with Serbia, Thailand, the US, Colombia, Spain, France, Denmark, Germany, the Netherlands, Canada, Estonia and the UK.

155. There are good tools and techniques available for the investigation of money laundering offences. Authorities use intercept material for investigation and prosecution of money laundering offences. Financial intelligence obtained as a result of coercive measures can be used in investigations of other crimes but new legal authorisations would be needed to apply further coercive measures. This can be done on the likely penalty. All evidence is potentially admissible in court (see below under core issue 9.5). There is national coordination to support the local level work – a cross-agency practical handbook has been produced which provides guidance on undertaking financial investigations to ensure their consistency and legality.

156. LEA's priorities are to prosecute offences that they identify and make crime unprofitable by the recovery of assets. LEAs also prioritise the compensation of victims. These aims are fulfilled by a follow the money approach when financial investigations are launched and LEA's need to ensure that they do not miss opportunities of identifying professional enablers during the process of following the money and seizing the assets. This may explain why there are no stand-alone prosecutions of professional enablers.

157. In the case of GOB also, the "follow-the-money" approach could be better applied. The intelligence carried out within this framework appears to have a "person-targeting" approach which works well to investigate known criminals. Investigations go beyond the "person-targeting" approach to trace and recover assets. In some cases, investigations do not go further to identify third-party money-launderers.

158. Swedish prosecutors have been quick to make use of the new ML offence and have prosecuted many cases at their disposal. The requirement to simply prove that money "derives from criminal activity", introduced by the new ML offence in July 2014, made a real difference in the prosecution of ML activity, particularly stand-alone ML. Prior to the introduction of the new ML offence, the predicate offence had to be confirmed in court, which meant that investigation and prosecution of ML was very difficult and always related to the predicate offence. Prosecutors also indicated that they can start an ML investigation more easily, and these investigations have often been useful to identify related predicate offences.

159. The table below reflects the prosecution rate of money laundering offences and this includes the processed offences that are investigated, showing that 53% of money laundering cases were prosecuted in 2015. This compares to an average prosecution rate of 10% for fraud which is one of the lowest in Sweden and 70-80% for possession of drugs which have one of the highest prosecution rates.

Table 10. **Prosecution rate, 2014–2015**

Type of offence	Prosecution rate (%)	
	2014	2015
Act on Penalties for Money Laundering Offences	65	53
ML offences	*70*	*52*
ML offences, aggravated offences	*21*	*45*
ML offences, petty offences	-	*29*
Commercial ML	-	*57*
Handling Stolen Money (incl. petty/aggravated offences)	56	n/a

160. In 2015, there were 79 court sentences where ML was the principle offence, of which 29 led to prison, where the average incarceration time was 16 months. There were also 76 court sentences where handling stolen money (the old ML offence) was the principal offence, of which 11 led to prison. The average incarceration time was 4 months for the regular crime (3 verdicts) and 9 months for the aggravated crime (8 verdicts). In addition, there were court sentences where ML or handling stolen money was not the principal offence; those included 98 ML offences and 118 handling stolen money offences. In sum, the court sentences in 2015 thus included 177 ML offences and 194 handling stolen money offences.

161. The statistics are somewhat limited due to the principle of concurrent offence and the sentencing practices in Sweden.

Box 3**. The principle of concurrent offences and sentencing practices in Sweden**

The principle of concurrent offences deals with cases when a perpetrator fulfils the requirements of more than one penal provision. Co-penalisation of one or more offences is based on the idea that the co-penalised offence is punished through the conviction of another offence to avoid that the perpetrator be punished twice for the same criminal activity. In determining whether a crime should be co-penalised with another, regard has to be given to whether the same perpetrator can be convicted of both offences, to what extent the co-penalised offence substantially affects the total penal value of the criminal activity, and whether there is a connection between the two offences (e.g. in terms of time and which interest the penal provision is intended to protect)..In the case of laundering the proceeds held by the person who committed the predicate offence (self-laundering), for example, the ML offence would normally be considered consumed by and co-penalised with the predicate offence, unless particular circumstances apply – e.g. when the perpetrator has taken part

in the predicate offence only to a minor extent but played a major role in the subsequent money laundering offence or when the money laundering activities go beyond what can be considered "normal" handling of the proceeds of the predicate offence (Government bill 2013/14:121, p. 112). When a perpetrator has committed acts which fulfil the requirements of several penal provisions (e.g. a proceeds-generating predicate offence and an associated ML self-laundering offence) he or she will, as the main rule, be prosecuted for the predicate offence only. The self-laundering of the proceeds will be considered "consumed by" or co-penalised with the predicate offence. The co-penalised money laundering offence can nevertheless be reflected in the sentence, since the offender may receive a higher penalty than would normally be rendered based on the predicate offence alone.

In addition to the principle of concurrent offences, it is practice in Sweden that sometimes judges' verdicts combine different criminal offences under one umbrella and inflict one single conviction for different criminal acts, such as drug offences and ML may be combined as aggravated drug offences. Judges tend to inflict a general conviction for the criminal activity, and do not specifically indicate each of the offences for which a perpetrator was found guilty. The reasons for the conviction can of course be inferred from the reading of the court sentence.

162. The principle of concurrent offences and the practice of criminal sentencing based on it affect the number of prosecutions and convictions regarding money laundering offences committed by a person linked to the predicate offence.

163. When the ML offence is co-penalised with the predicate offence, it is not clear the extent to which this leads to an additional sanction. While it is clear that the ML offence may be an aggravating factor in the sentencing, judges determine sentences based on a wide range of elements relevant to each individual case, and do not record what effect the ML activity specifically has on the final penalty. The fact that the ML offence is new has not yet allowed Swedish Authorities to identify how co-penalised ML has an impact on the final level of sentence. In some cases, where there are different criminal acts that constitute a violation of more than one criminal provision prosecutors will prosecute the crime which will attract the harsher sentencing, which may not be ML. Prosecutors are obliged to pursue any crime, and will make a judgment of the crime to prosecute on the basis of evidence the can obtain. However, the fact that ML offences will be in many cases considered co-penalised with the predicate offence, and that it is not clear the extent to which co-penalised ML offences increase the sentence, may represent a disincentive to prosecute ML separately.

164. The fact that judges' verdicts sometimes combine different criminal activities into one conviction suggests that stand-alone ML activity is considered by courts in more cases than the statistics would show. Beyond the principle of concurrent offences, it is not clear why judges would combine predicate offences and ML activity into one aggravated conviction (for example for the predicate offence) when the evidence is sufficient to distinguish between the two. This may be due to the fact that the new ML offence is recent, and there is not yet consolidated jurisprudence on the new ML offence, compared to the old "handling of stolen money" offence. This sentencing practice has the potential to frustrate prosecutors' efforts in pursuing stand-alone charges of ML.

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

165. Sweden has set up its investigative and prosecution resources according to the risks that are identified. It should be noted, however, that the risk analysis is in a large part based on LEAs' perceptions and suffers from significant knowledge gaps in the ML methods (see IO.1).

166. Even though reliable statistics on the types of money laundering investigations and prosecutions are not available, a review of 48 judgments since the introduction of the new ML offence in July 2014 confirms that most predicate offences or related criminal activities are narcotics offences or fraud, but other examples include doping offences, theft, robbery, extortion, dishonesty to creditors and tax fraud. The link to tax and fraud for ML activity is consistent with the risk identified by Sweden (there is a perception that high taxation may lead to higher risk of tax evasion). The amount of money assessed to have been laundered through tax evasion is hard to assess but is not believed to be large compared to other countries.

167. The review of the 48 judgments found that the ML measures most used were the storing, converting, passing on or withdrawing of funds from an account; the second most used ML measure was storing and transporting cash. This is consistent with the findings of the NRA (see IO.1). While the use of cash is certainly a risk area in Sweden and a method commonly used, not least in unregistered labour schemes, the assessment team finds that the use of cash may not be the method of money laundering most used in Sweden in absolute and relative terms, given that around 95% of transactions are conducted electronically. Other methods, through sophisticated electronic transactions and new technologies should be better investigated in ML schemes (and some efforts are already made by LEAs in this regard).

168. Sweden has taken measures to properly identify and investigate the misuse of cash, as evidenced in the many cases of ML involving cash. However there are risk areas which are not addressed as thoroughly as they should be, particularly as the role of Customs in identifying and seizing cash in ML schemes is limited (see IO.8). Some measures are already underway, in line with the national AML/CFT strategy. The Police Authority (in co-operation with the SPA) are setting up a new cash team in Stockholm, a team of plain clothes officers and AML/CFT officers who will focus on seizing cash flowing through targeted ports (air and sea).[19]

169. The risk analysis highlights that companies are also misused for example to either issue fake invoices or to screen the identities of those behind crimes (e.g. through straw persons or front men). Specific expertise from accountants, lawyers, real estate agents, and bank employees are used by criminals. LEAs have identified the use of companies, straw persons, and front men in many of their ML investigations and prosecutions. The use of false identities is a risk, and a common part of the investigation is to find the real people behind the company (in 2015, around 600 straw persons were identified in the course of investigations). To a smaller degree, ML investigations and prosecutions have focused on the use of professional launderers.

[19] The STA has developed a new methodology on how to work with cash with the aim to tax people on cash assessment and how they earn this money.

170. LEAs indicated that a cross-border element is usually present in ML schemes. Money is often transferred abroad for consumption, investment or simply to conceal its origin before being returned to Sweden. LEAs indicated that it is hard to know what money transferred abroad is used for, and indicated the lack of efficient international cooperation from certain jurisdictions as a problem in this respect (because of the time taken to receive answers through MLA and because money often flows through different countries). While Sweden often seeks international cooperation, LEAs expressed difficulties in obtaining valuable evidential and investigative information from abroad in some cases.

171. With particular regard to organised crime, Sweden has identified the retail and service sectors as highly vulnerable. This is because, in the view of the Swedish authorities, many criminals tend to spend or consume the criminal assets in goods and services, both day-to-day and luxury spending (real estate, boats, and others). LEAs find it complicated to identify and trace these assets, and few money laundering investigations appear to be made in this regard, despite the fact that the new ML offence specifically targets consumption of criminal gains without the intent to launder. Further, the authorities indicated that a reason for this complication is that great deal of the criminal assets never comes into contact with the legal sector; rather, it is spent in the illegal economy, with purchases occurring in cash or through bank accounts. This is called the "aquarium economy". The authorities maintain that consumption in the "aquarium economy" primarily includes goods/property and services purchased from other criminals, which should be considered to be ML (however, not all authorities consider this type of consumption to be ML). Currently, Sweden does not sufficiently investigate ML which occurs in the 'aquarium economy' and does not interface with the legal economy.

172. As a consequence of the "aquarium economy", Swedish authorities perceive the risk of third-party laundering performed by professionals to be lower risk, which may explain why there are no or few investigations into this kind of ML activity. This argument is not fully convincing because criminals still need the services of professionals who are not linked to the crime or to the criminal organisation. Considering that 95% of economic activity occurs through the formal financial system, it is likely that professionals are hired to launder proceeds through the formal sector. The only types of investigation and prosecution in this regard appear to target individuals or companies (front men, and a few gatekeepers) which facilitate the laundering of proceeds (some of them prosecuted and convicted for commercial ML). Sweden also argues that the lack of large scale third-party ML cases is due to the broad scope of the offence of aiding and abetting the predicate crime, as well as provisions for prosecuting for crimes together and in concert, which means that the ML is punished but not specifically so in the verdict. LEAs provided some case examples where persons only peripherally involved in the predicate offence were convicted for aiding and abetting, even though their criminal act could also be considered to be acting as facilitators and/or launderers.

173. Whether a prosecutor decides to prosecute an offender for involvement in the predicate crime or as offender for ML is often dependent on the evidence that is available for each crime. The crime for which the strongest evidence is available will be prosecuted. This can be illustrated by the cases in box 4 below, as well as the Södertälje case, set out above in **Box 2**.

Box 4. **Prosecution of third-party money laundering together with the predicate offence**

Folarin[1]

An individual used hijacked e-mail accounts to send false instructions to make payments, committing fraud worth approximately SEK 5.9 million (approximately EUR 620 000) against seven companies, banks and individuals around the world. Payments were sent to accounts held by a number of other individuals, who laundered the money for the principal defendant, Folarin, and sent it to his accounts in Sweden and Poland.

The investigation was initiated on the basis of an STR, which was submitted after an awareness-raising outreach programme by Fipo prior to the introduction of the new ML offence in 2014. The outreach had highlighted the ML methods and indicators which were involved in this activity. Further investigation by Fipo identified more linked STRs and discovered the network. PDP's were issued by Fipo, followed by seizures of SEK 1.5 million (approximately EUR 160 000), and a full investigation. Investigators have used a follow-the-money approach, through banks, payment service providers, and money mules, to identify 70 suspects in Sweden and other countries.

International cooperation was a key element of this case. This investigation was handled by the International Chamber of the SPA in Malmö. A joint investigation team with Poland started in June 2015 and the principal defendant was extradited from France. MLA requests were made to Denmark, Poland, Great Britain, Nigeria and South Africa in order to obtain further information and trace money that had been removed from Sweden. In total 70 suspects are being investigated, and 14 people have so far been prosecuted.

Folarin was convicted of gross money laundering, gross commercial money laundering, money laundering, and handling of stolen money (the old ML offence, for activity that occurred before July 2014), and sentenced to 3 years imprisonment and a 5 year ban on business activity. Damages to injured parties of around SEK 1.65 million (approximately EUR 170 000) were awarded, and an enhanced confiscation of NGN 48 million (about SEK 2 million or EUR 210 000) was ordered and has been secured in Nigeria. SEK 120 000 (approximately EUR 12 500) which had previously been seized was confiscated. Twelve other defendants were sentenced for various money laundering offences, with sentences ranging from probation to 1.5 years imprisonment. Assets amounting to around SEK 5 million (approximately EUR 525 000) have been confiscated and recovered. The sum of SEK 2 million (approximately EUR 209 000) has been frozen abroad.

e-identity fraud

One or more persons fraudulently obtained e-identifications from two victims and used these to empty their accounts: a tax account which held approximately SEK 5.3 million (approximately EUR 555 000), and an internet bank account which held SEK 165 000 (approximately EUR 17 300). This money was transferred to the accounts of ten other persons, who forwarded it to the organiser. At least one of these people had also created a company which was intended to be used in the money laundering.

In April 2015, those involved were prosecuted: one for gross fraud and the others for helping someone else convert money derived from an offence or criminal activity. Seven of the defendants

were convicted of gross money laundering, based on the amounts involved (each of whom had laundered SEK 380 000 (approximately EUR 40 000) or more) and that the criminal activity had been systematic or large scale and of an especially dangerous nature. Two other defendants were convicted of money laundering. Two of the defendants were acquitted.

Note:

1. Malmö district court judgment of 10/06/2016, B 1428-15 and B 6050-16. On 16 November, the Skåne and Blekinge Court of Appeal (judgment B 1725-16) confirmed the district's courts judgment with some minor modifications.

174. While the investigations and prosecutions of ML activity are consistent with the risks identified, the risk analysis may suffer from a circular argument because the risk analysis was essentially based on LEAs' perceptions. The NRA, as well as the risk analysis conducted by Brå, highlighted the lack of more detailed knowledge in the ML behaviours and patterns.

Types of ML cases pursued

175. Despite the fact that the prosecution and sentencing system, as well as the way data are collected, make it difficult to establish and distinguish if in a particular case the defendant has been convicted for money laundering, it is clear that Sweden has pursued different kinds of ML offences.

176. Sweden has provided many examples of prosecuting different kinds of money laundering, particularly since July 2014. ML prosecutions and conviction include the old ML offence of "handling stolen money", and the new "ML offence" (gross, normal, and petty), as well as "commercial ML" (which is when a natural or legal person is found guilty of negligent behaviour in relation to money received). It is noted that around 10% of money laundering offences in 2015 were classed as gross (at present for the offence to be considered as a gross money laundering offence a minimum assets of SEK 221 500 (approximately EUR 23 100) should be laundered).

177. The principle of concurrent offences (see **Box 3**. above) has a particular impact on the prosecution of self-laundering. Self-laundering has been criminalised since July 2014, however in terms of effectiveness, self-laundering would not be easy to prosecute. The authorities provided some cases of self-laundering and pointed to the possibility that the prosecutor would pursue only the self-laundering offence when he/she thinks that the predicate crime would not be confirmed in court, but he/she had enough evidence to prove the criminal origin of the money handled by the defendant. One advantage of prosecuting for self-laundering instead of the predicate offence is that there is no need to investigate the predicate offence; but since it is not necessary to show where the money derives from, it is not always clear whether a person is convicted for self-laundering or another type of ML.

3

Box 5. **Prosecution and conviction of money laundering with a conviction for the predicate offence (self-laundering)**

The bags of money (Göteborg)[1]

Two persons transported in two different occasions bags of cash. In the first case, one of the defendant had transported more than SEK 240 000 (approximately EUR 25 100) in cash in a private car. In the other occasion, one defendant had carried a plastic bag containing more than SEK 0.5 million (approximately EUR 52 400) in cash which he had handed over to the other defendant in a public place. The two persons were charged with gross money laundering and other offences on the basis that the measures were taken to hide the fact that the money was derived from an offence or criminal activity. To prove this, the prosecutor presented extensive evidence, both showing that the defendants were part of a criminal network involved with, among other things, narcotics sales, and also that the defendants lacked legal income matching the found money.

The City Court found that the prosecutor's evidence that the money was derived from narcotics sales was, based on this, sufficient to convict both defendants. They were sentenced to 8 and 10 months imprisonment, respectively for ML offence and one them was also sentenced for a selling narcotics. The money was confiscated.

Illegal work case – Malmö[2]

Several persons were convicted in Malmö City Court of, inter alia, gross bookkeeping crime. A number of the defendants were sentenced to long prison terms for their involvement in a major illegal work case of several million SEK.

Two of the defendants, also involved in the criminal activity above, maintained two private banks accounts (around SEK 800 000 and SEK 1.3 million respectively (approximately EUR 84 000 and EUR 136 000)) where money from the criminal activity was deposited by several different people. The money was immediately withdrawn. The court found that the operations were such that the two defendants must be considered to be habitual, the amounts such that the operations were considered major in scope, and that the defendants must have realised that their actions contributed to measures which would reasonably be expected to have been taken to hide money that was derived from criminal activity. They were sentenced to two and a half and two years' imprisonment, respectively. Both were issued with a three-year trading prohibition.

Missing Trader Fraud[3]

Mr A evaded value added tax through a company carrying out a missing trader fraud scheme (around SEK 25 million (approximately EUR 2.6 million). Mr B assisted Mr A in the promotion of the tax evasion for an amount of evaded tax up to SEK 12 million (approximately EUR 1.3 million). Mr B also took part in the management of the missing trader company and was involved in the control of the company's bank account and transactions. Mr B transferred about SEK 3.5 million (approximately EUR 370 000) from bank accounts belonging to the missing trader company/Mr A to a bank account in Dubai. Mr A was convicted of aggravated tax crime and sentenced to prison for five years and six months. Mr B was convicted of complicity in aggravated tax crime as well as gross money laundering and sentenced to two years and six months' imprisonment.

Note:
1 Gothenburg City Court, judgment 12/05/2015, B 2586-15.
2. Scania and Blekinge Court of Appeal 26/11/2015, B 2113-15; Malmö City Court judgment 29/07/2015, B 10730-14.
3. Svea Court of Appeal 11/10/2016, B 6698-16; Södertörn District Court 13/7/2016, B 14753-15.

178. Foreign predicate offences are investigated to the extent of the limitations that Sweden faces in international co-operation with other countries. An example of investigating and prosecuting foreign predicates is the "Telia case" (see **Box 8**. below), where Sweden has conducted asset tracing investigations and taken measure to secure the assets (separate ML investigations are being carried out in Switzerland). Prosecutors are aware of the limitations that they have and sometimes this can dictate their investigative strategy.

179. The range of ML prosecutions and convictions includes cases of third-party money laundering offences – the laundering of proceeds by a person who was not involved in the commission of the predicate offence – and there are a few cases of "commercial ML" – a person who, in the context of business operations or as part of activities that are conducted habitually or otherwise extensively, takes part in a measure that can reasonably be assumed to be taken for ML purposes. There is evidence of good use of financial investigations and financial tools to disrupt strategic persons although it is not fully clear why professional money-launderers which operate large scale ML are not identified. In the opinion of the assessment team, it is unclear if the "follow-the-money" tactic leads to third-party money launderers or stops when assets are found that can be seized. Swedish authorities stated that they have not seen much large third-party money laundering in Sweden, and that during investigations the focus for the prosecutor is to investigate and prosecute all possible and found criminal actions and would not be limited by any previous or parallel decision from the Police.

180. Apart from the review of the 48 judgments mentioned above, the statistics provided for types of money laundering cases that have been investigated do not fully distinguish between the different types of ML offence (e.g. foreign predicate offence, third-party ML, stand-alone ML, self-laundering); rather, they focus on the whether the ML was petty, normal, gross, or "commercial". It is therefore difficult to assess if the entire spectrum of money laundering offences is being investigated. It is imperative to have one focused skilled agency, such as Brå, to collate and interpret statistics for all which will assist in identifying strengths and weaknesses in the new legislation and system.

Box 6. **Prosecution of stand-alone ("commercial") money laundering (including self-laundering), without a conviction for a predicate offence**

The car with hidden compartments (Malmö)[1]

Three persons were stopped while travelling from Stockholm to Malmö in 2015. Their car was found to contain SEK 1 728 000 (approximately EUR 179, 000) and EUR 35 000 in hidden compartments, believed to derive from criminal activities. The Court found that none of the defendants had provided a reasonable and trustworthy explanation for the trip. It focused on the fact that one of the defendants, who claimed that the money was brought along to buy wood in Sweden for export to Morocco, was unemployed, had previous convictions, and lacked any business experience.

All three defendants were convicted of gross money laundering, and sentenced to two and a half years in prison (later reduced on appeal to two years for one defendant, and 22 months for the other two), followed by deportation. The money in the hidden compartments and the money that one of the defendants was carrying was confiscated.

3

"Tartar" - money laundering through ATM withdrawals

This case involves a money laundering scheme used to avoid payroll taxes on employers and to launder proceeds from fraudulent invoicing schemes. Companies were transferring money overseas through natural persons and a Swedish foundation to foreign bank accounts. Cash withdrawals from these foreign bank accounts were made through ATMs in Sweden, and the cash used to pay workers.

The investigation originated from an STR in October 2015, prompted by the withdrawal of large sums of cash from ATM-machines with foreign cash cards. Through analysis of bank transactions as well as secret wiretapping, investigators from EBM identified the companies involved in the scheme. The person controlling the Swedish foundation was identified, and was at the time residing in a non-EU country. Due to the swift actions from the Police in that country, the suspect was arrested and deported back to Sweden (since the suspect's passport had been revoked). A request for MLA was executed by the Police in the foreign country.

In total eight suspects were detained, two of which are still subject to coercive measures, and are facing charges including money laundering, commercial money laundering, and bookkeeping crimes. The investigation is still ongoing, partly because documents requested through MLA have not yet been delivered. ATM companies do not have to submit STR but did due to outreach work from Fipo.

Following the introduction of the new ML offence, it is possible to initiate a criminal investigation concerning commercial money laundering, without investigating the predicate offences themselves. This was impossible under the previous legislation. The strategy followed in this case has been to disrupt the money laundering scheme quickly, and to use this case to test the new commercial money laundering offence.

Money laundering through vehicle leasing

A representative of a lending company (and board member of a bank) signed vehicle leasing agreements worth up to SEK 5.2 million (approximately EUR 550 000), for a large number of customers known to be involved with crime, or with no (or a relatively small) legal income. These customers have then started to make payments on these debts. This is believed to be organised third-party money laundering: after endorsement of the contract, the vehicle is registered to the customer who can immediately benefit from the criminal proceeds, which are laundered through regular repayments.

A joint investigation was launched by the Economic Crime Authority and the International Public Prosecution Office, based on suspicions that the credit offered was inconsistent with the credit rating of the individuals concerned. The investigation is still ongoing, and is now also covering aggravated fraud and aggravated tax crime amounting to approximately SEK 1.8 million (approximately EUR 1 88 000).

Note:
1. Scania and Blekinge Court of Appeal, judgment 12/01/2016, B 2791-15; Malmö City Court judgment 26/10/2015, B 9445-14

181. The Södertälje case within the GOB is a good example of the right tools being used to address a situation. These formed part of an overall strategy that addressed the strategic part of the organisation, the relatives and enablers and the foot soldiers. They motivated the good forces within the community by addressing the issues and therefore secured the support of the community. By

using different investigative strategies, they were able to separate operations into sub-groups and thereby allocate appropriate resources. They were also able to produce quantitative data outcomes as a result of this approach. A really good example of inter-agency co-operation to achieve good results.

Effectiveness, proportionality and dissuasiveness of sanctions

182. Criminal penalties for ML offences appear low in comparison to other countries. Nonetheless, the sentencing guidelines are the same as for fraud offences, and therefore perceived to be appropriate. Although the range of penalties set out in law are in line with similar offences in Sweden, courts are not yet using the full range of penalties.

183. There is a low range of imprisonment and other measures are employed as a deterrent, e.g. probation. It should be noted that the Swedish Prison and Probation Service shows that there are a low range of repeat offenders. The review of the 48 judgments compiled by the SPA showed that 26 of those convicted went to prison.

Table 11. **Total and average prison sentence length (months), for Court Sentences with imprisonment as the Principal Sanction and distributed by Principal Offence, 2014-2015**

	2014		2015	
Type of offence	**Average prison sentence length (months)**	**Total prison sentence time (months)**	**Average prison sentence length (months)**	**Total prison sentence time (months)**
Act on penalties for Money Laundering Offences (2014:307) – in force 1 July 2014	**-**	**-**	**16**	**464**
ML offences (section 3)	-	-	*4*	*18*
ML offences (section 4)	-	-	*3*	*10*
ML offences, aggravated offences (section 5)	-	-	*21*	*378*
ML offences, petty offences (section 6)	-	-	*2*	*2*
Commercial ML (section 7, items 1-3)	-	-	*28*	*56*
Handling Stolen Money (section 6a)	**3**	**26**	**4**	**13**
Handling Stolen Money, aggravated offences (section 6a)	**12**	**160**	**9**	**71**
TOTAL	**n.a.**	**186**	**n.a.**	**548**

184. The above table shows the total and average prison sentence in months with nearly 14 months imprisonment being the average for all of crime types in 2015. However, the table below

shows that the maximum penalty of six years imprisonment for an offence of gross money laundering on its own has not yet been imposed.

Table 12. **Total and average prison sentence in months for 26 selected cases where ML is the principal offence (period July 2014 – June 2016)**

Term of Imprisonment	Number of Convictions
1-2 months	4
3-4 months	4
6 months	3
6 months to 1 year	2
1 year	2
1-2 years	7
2-4 years	7
4 years plus	0

185. First time offenders are rarely sentenced to a term of imprisonment in Sweden, although they are for certain serious crimes. For imprisonment for a first time offence on conviction, the value of the offence should generally be more than SEK 700 000 or 800 000 (approximately EUR 73 000 or EUR 84 000). The years of prison sentence may depend on the value involved, generally with the one year term for less than SEK 1 million (approximately EUR 1 05 000), and for every million above one year is added to the sentence. Prosecutors and police appear to consider confiscation and sentencing as equally deterrent.

186. The authorities pointed to the possibility that the Supreme Court recognises the new ML offence as a crime for which there is a presumption of imprisonment even for first-time offenders. These types of offences (called "*artbrott*") are identified by the Supreme Court, for example on the basis of being particularly harmful to society (e.g. tax crimes) or particularly hard to detect. LEAs indicated that they are waiting for the right case of money laundering to be brought to the Supreme Court. Recognition of ML offence as "*artbrott*" would certainly contribute to increase the effectiveness and dissuasiveness of sanctions.

187. Other matters impacting on the sentencing for money laundering are the fact that if the sentencing for the predicate offence is higher than money laundering then the focus of the prosecution will remain on the predicate offence. However, it should be noted that a coordinated money laundering investigation prior to the predicate offence being identified, and which leads to the predicate offence being identified, offers the opportunity for all parties to be indicted with the predicate offence on a conspiracy basis. Examples were presented of this scenario. This represents an opportunity for higher sanctions to be imposed and also means that it would not be counted as a prosecuted money laundering offence.

188. Corporate fines have been applied against companies used for money laundering and sham companies have been liquidated.

189. There is a concern that low sentencing decisions of today will be basis for sentencing decisions of the future, however in practice more time and data are necessary to conclude on the dissuasiveness of sanctions.

190. Overall, Sweden has an adequate range of sanctions for ML, and case examples show that the higher end of the range of sanctions has been applied in cases where ML is one of several crimes prosecuted. However, the higher end of the range has not yet been used in cases where ML is the only charge or the most serious charge. Hence, there is a concern that the application of sanctions in practice is not yet fully effective or dissuasive. This concern is particularly significant in the context of repeat offenders convicted of ML, who should be nonetheless be given heavier sentences pursuant to the Penal Code.

Alternative criminal measures

191. The concurrent aspect of the legal system means that where there are different criminal acts that constitute a violation of more than one criminal provision prosecutors will prosecute the crime which will attract the harsher sentencing. This means that prosecutors often indict the offender with the predicate offence before the ML offence where the former leads to a higher sanction (e.g. drugs or tax offences). If during the investigation of coordinated money laundering offence evidence is established of the predicate offence, then prosecutors will look to charge for conspiracy on the predicate offence which will lead to more powerful sanctions. This also means that these offences will not show up in the money laundering statistics. All the circumstances of the offence are considered for the purposes of sentencing.

192. In the area of economic crime, it is common for ML activities to be prosecuted as tax offences and/or accounting offences, or as accessories to such crimes. Examples of this occur in cases of illegal labour with false invoices, cases regarding missing trader fraud offences, as well as cases regarding currency exchanges or similar operations. This can be linked to the principle of concurrent offences, but also to the fact that these criminal schemes are such that transactions and the movement of cash occur prior to the consummation of a tax offence, complicating the process of proving that the property originates from crime or criminal activities. In order to prosecute ML from tax crimes, the offence of tax crime (enrichment through evading taxes due) has to be completed before a money laundering offence can be investigated. An example of the use of alternative measure is the case “Södertälje” mentioned above.

Box 7. **Money laundering activity prosecuted using an alternative offence**

The Slipper

Five persons were involved in a fraud scheme. The proceeds of the fraud were transferred to the bank accounts of several companies, postal orders, and similar institutions. Some of the five acted as straw persons and money-mules to cash the proceeds and return them criminal activities. The five persons were convicted for aggravated tax offence, aggravated accounting offence and aggravated fraud and sentenced to 2.5 years in prison. Assets were seized at the time of arrest, and were subsequently held and confiscated. The state claimed damages amounting to SEK 2.3 million (approximately EUR 241 000). The confiscations amounted to SEK 81 000 and 125 000 respectively (approximately EUR 8 500 and EUR 13 100).

Conclusions

193. The new ML offence in force since July 2014 has greatly improved the potential for investigation and prosecution of ML, particularly because of the need to simply prove that money "derives from criminal activity". Before July 2014, however, the predicate offence had to be confirmed in court before someone could be convicted of ML ("handling stolen money"), which severely limited LEAs' ability to investigate and prosecute ML activity, which basically focused on proving the predicate offence. Since July 2014, a relatively large number of different types of ML have been investigated, prosecuted and convicted, particularly targeting stand-alone ML. The need to prove that money derives from criminal activity also facilitated the ability of Police and prosecutors to initiate an investigation of ML, which then led to prosecution and conviction of other crimes The authorities showed high degree of commitment to the new ML offence, with prosecution rate for the new ML offence comparing very favourably to other offences, allocating resources, training investigators and prosecutors, and embedding the ML offence within their structures and practices. Improvements are still needed in relation to the understanding of the ML scenarios. This should lead to investigation and prosecution of large scale third-party ML.

194. Lack of comprehensive statistics on all convictions of ML, which is also due to the application of the principle of concurrent offences and the sentencing practice in Sweden, limits the ability of the authorities to fully understand whether the investigation and prosecution of ML lead to convictions. The sanctions may be considered low, and in practice the maximum sentence applied may not be fully dissuasive and effective, particularly where money laundering is the sole offence or the most serious offence. Prosecutors should identify the appropriate serious ML cases for the Supreme Court to establish court practice for the level of sanctions.

195. Sweden has achieved a substantial level of effectiveness for IO.7.

Immediate Outcome 8 (Confiscation)

196. Swedish authorities consider depriving criminals of their assets to be a penalty equally dissuasive as imprisonment, and therefore prioritise tracing and confiscating assets as an important part of the penalty for crimes.

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

197. Confiscation of criminal proceeds, instrumentalities, and property of equivalent value is pursued as a policy objective to a large extent in Sweden. The policies are reflected in political commitment across various governments over a long period of time, and a number of concrete measures have been implemented in later years, such as legislative improvements, and instructions and appropriations to police and prosecution agencies. Requesting confiscation is essentially mandatory if a crime has led to proceeds. This is also followed up by central LEAs, who have developed strategies and activities (such as the GOB, the creation of an asset-tracing unit within the Police, and the recruitment of forensic accountants in a number of prosecutor's chambers). LEAs have also developed guidance and training on asset-tracing investigations and prosecutions, and display a high awareness to follow the money and deprive criminals of proceeds. Swedish authorities indicated that LEAs conduct asset-tracing investigations in all major criminal investigations, and regularly use the tools to secure the assets at an early state of the investigation (see below). The Swedish authorities indicate that confiscation is pursued to a lesser degree by regional LEAs, although it should be noted that overall the majority of seizure and confiscation claims come from the local prosecutor's chambers (though the amounts may not always be very high).

198. Despite this commitment and engagement, most LEAs lack system-level statistics to properly measure and assess whether the high level policies are actually successful in leading to decisions in courts. The EBM have developed agency-level methods and tools to reasonably measure the level of success and output, but other agencies have not yet implemented sufficient tools (though a project is underway). The SPA set overall benchmarks for the number of seizure and confiscation claims which prosecutors are expected to make. If a prosecutor constantly does not meet those expectations, he/she may face consequences. Chief prosecutors will monitor confiscation cases and regularly report these to the Prosecutor General. Some figures show a positive trend in confiscation activities (e.g. number of seizure and confiscation claims are increasing, enforcement of confiscation decisions is improving), but the aggregate picture of confiscation, tax surcharges and collection of restitutions does not allow the comprehensive measurement in statistical terms of the success of the confiscation policies. Sweden estimates the overall volume of tax evasion, but not the total size of the illegal economy nor the sums thought to be laundered. There is a lack of coordinated measurement tools and statistics in the field of confiscation. In the area of tax collection, including in the administrative confiscation of proceeds of tax crime, stronger policies and tools are in place.

199. Sweden has identified the shortcoming in confiscation-related statistics, and has taken steps to improve the situation. A cross-agency strategy (2014) and six-point action plan (2015) concerning proceeds generating crimes was developed, including a project to monitor that effective, high quality work is carried out in connection with the proceeds of crime. The project report (2015) concluded that it was impossible to follow up more precisely on the final results of the authorities' joint efforts under the current authority-specific monitoring system. Work is underway to create a coordinated information management within criminal action, but the report points out that this will not resolve the problems relating to monitoring the cooperating authorities' asset-oriented work to fight crime. While the policies are clearly stating confiscation as a priority, and many measures have been

implemented, the inability to present comprehensive statistical support for the assessment of the operational results makes it difficult to fully appreciate whether the objectives in confiscation policy are being achieved. Nevertheless, the efforts shown in the available statistics below and the case examples suggest that LEAs trace, seize, confiscate, and recover assets to an increasingly successful degree.

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

200. Under Swedish legislation, proceeds of crime can be recovered through a number of measures and prosecutors would opt for the most appropriate tool in the particular case. The tools include: criminal confiscation (AML legislation), extended criminal confiscation, corporate fines, administrative confiscation of proceeds of tax crime, the imposition of duty or tax surcharges, and claims for restitution to victims. Equivalent assets can also be recuperated via the Enforcement Authority when the offender has outstanding debts registered with this authority (uncollected confiscated assets and claims, unpaid fines, etc.). To secure the assets during the investigations, a number of provisional measures are taken: prohibition of disposal of property (PDP), seizure, custody, provisional attachment, and sequestration in criminal cases; and attachment in customs cases and tax cases. Swedish prosecutors give priority to restitution claims over confiscation claims, but can claim higher amounts than necessary to cover damages.

201. Authorities observed that since 2013 it has been routine to conduct an integrated financial investigation from the beginning of any major criminal investigation, and to use provisional measures at an early stage to secure the assets. The statistics and tables below provide some evidence confirming the increased attention of prosecutors in tracing criminal assets.

Seizure and confiscation

202. The EBM maintains statistics on the number of claims for seizure and confiscation made by prosecutors and those claims awarded by judges. Comparison between claims made and approved for individual calendar years must however be viewed critically, since the claim and the court's decision do not necessarily fall within the same calendar year. The table below shows that the number of claims for confiscation awarded by judges significantly rose from 2 in 2013 to 15 in 2015, which indicates that the work done by EBM regarding proceeds of crime is yielding results. Although the total amount of claimed assets is lower in 2015 compared with both 2013 and 2014, the amounts are entirely dependent on the cases EBM pursued each year. In fact, despite the fact that EBM claimed lower amounts in 2015 compared to 2013, judges awarded higher amounts for both seizure and confiscation. The overall number of claims to secure and recuperate criminal assets, through seizure and confiscation, or through other means (see table below), also increased over time.

Table 13. **Claims for seizure and confiscation, made and awarded by EBM and SPA. The number and value of claims awarded by judges are included in parentheses**

Year	2013		2014		2015	
	No.	**Amount (million SEK)**	**No.**	**Amount (million SEK)**	**No.**	**Amount (million SEK)**
EBM seizure	16 **(1)**	131.7 **(3)** EUR 13.8 million **(EUR 314 000)**	10 **(4)**	129.3 **(50.3)** EUR 13.5 million **(EUR 5.3 million)**	15 **(9)**	56.1 **(18.5)** EUR 5.9 million **(EUR 1.9 million)**
EBM confiscation	14 **(2)**	40.2 **(3)** EUR 4.2 million **(EUR 314 000)**	13 **(8)**	40.4 **(20.9)** EUR 4.2 million **(EUR 2.2 million)**	24 **(15)**	15.8 **(7.3)** EUR 1.7 million **(EUR 764 000)**
SPA seizure	111 (n/a)	n/a	107 (n/a)	n/a	107 **(36)***	418** **(40.3)*** EUR 43.8 million **(EUR 4.2 million)**
SPA confiscation	1 076 (n/a)	251 (n/a) EUR 26.3 million	1 161(n/a)	66 (n/a) EUR 6.9 million	1 149 **(763)***	110 **(38.1)*** EUR 11.5 million **(EUR 4 million)**

Table Notes:

* SPA statistics for 2015 reflect the actual outcomes of the case in court and should be complemented with the number of claims connected to court decision. The total number of confiscation claims connected to a verdict as of August 2016 was **999**, for an amount of **SEK 54.4 million (EUR 5.7 million)**. Claims for seizure connected to a verdict were **37** for an amount of **SEK 87.4 (EUR 9.1 million)**.

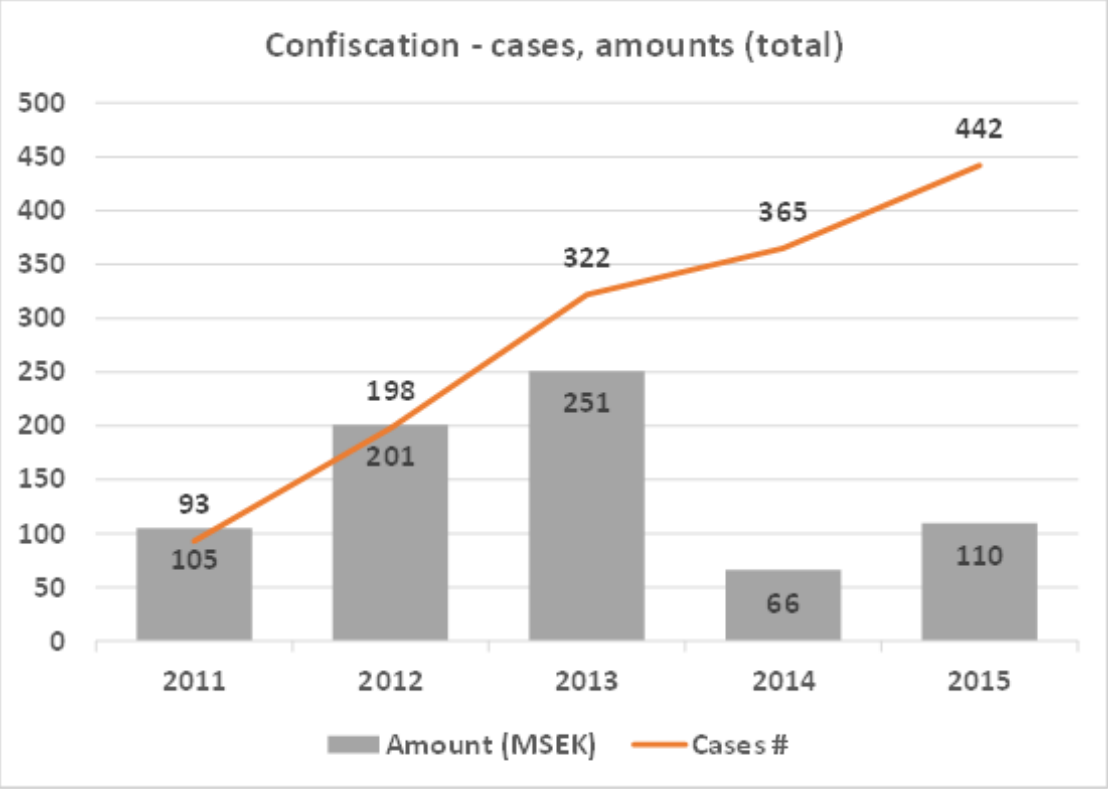
** More than half if the 2015 seizure figures consists of one ongoing large bribery case of SEK 277.1 million ("Telia case") (EUR 29 million).

203. During 2015, EBM indicated that the assistance provided by EBM to other authorities in securing and recovering assets totalled a value of SEK 64 million (approximately EUR 6.7 million). As EBM is working together with other agencies to recover proceeds of crime in the most effective way, the amounts that it claims for confiscation may be less than the combined value of the assets that the EBM secures. An effective tool to freeze money at an early stage is through a PDP which most of the time is confirmed into seizure (see IO.6 above and **Box 1**. for a practical example of use of PDP).

204. The SPA's statistics started following up the outcomes in court of their claims in a systematic manner only in 2016 (for the 2015 cases). Out of the 107 seizure claims made in 2015, 37 had been decided by judges (as of August 2016) – the rest had either been purged from their records system already, or had not yet reached a verdict. Out of those 37 cases, 36 were approved. As regards confiscation, there were 1,149 claims in 2015, of which 999 cases had been decided. In the 999 cases, the prosecutors were successful in 76% of cases. These figures show that a high percentage of claims for seizure and confiscation are approved, which suggests that prosecutors are successful in tracing assets and proving their criminal origin.

205. The figure below shows that the number of cases where the SPA has sought a criminal confiscation has significantly increased in the last few years. This reflects an increased attention paid by prosecutors to asset-tracing and confiscation.

Figure 2. **Number of cases where SPA sought confiscation, and amounts claimed***



* Please note that the number of cases where confiscation was sought is lower than the number of claims made (reported in table 13 above), as one case may involve more than one claim for confiscation.

Claims for restitution

206. Swedish prosecutors often tend to give priority to restitution claims over confiscation claims. When criminals are deprived of proceeds by court ordered restitutions, restitution to victims is assured and the values are not registered as confiscation as such. Hence, the statistics on restitutions are important to assess to get a full picture of Sweden's results. The numbers below are only from EBM and from the cases belonging to the International Public Prosecution Chamber in Stockholm. The total amounts for restitutions are likely to be significant sums of money and assets that criminals are being deprived of, but the numbers are for the most part not available. Case examples and anecdotal evidence shows that these sums are likely to be in the size of hundreds of millions of SEK per year for the past five years.

Table 14. **EBM & SPA restitutions claimed and awarded 2013–2015. The claims awarded by judges are included in parentheses**

Year	*2013*		*2014*		*2015*	
	No.	**Amount (million SEK)**	**No.**	**Amount (million SEK)**	**No.**	**Amount (million SEK)**
Restitutions – EBM	21 **(11)**	61.7 **(9)** EUR 6.5 million **(EUR 942 000)**	84 **(123)**	79.3 **(57.9)** EUR 8.3 million **(EUR 6.1million)**	142 **(108)**	32.6 **(55.5)** EUR 3.4 million **(EUR 5.8 million)**
Restitutions (International Public Prosecution Chamber, Stockholm) – SPA	42 **(19)**	52.9 **(49.6)** EUR 5.5 million **(EUR 5 million)**	9 **(12)**	38.6 **(32.5)** EUR 4 million **(EUR 3.4 million)**	116 **(52)**	31.8 **(45.6)** EUR 3.3 million **(EUR 4.8 million)**

207. However, it is not clear that the numbers correspond with the amounts gained by the criminal acts, as the sums rather reflect the losses incurred by the crime, which may be higher than the criminal proceeds generated. The sums will also include compensation for crime that did not generate any proceed but would lead to significant damage (e.g. murder).

Corporate fines

208. As an alternative to confiscation and restitution claims, Sweden indicated that prosecutors will seek to apply corporate fines as a way to recover assets from criminal activity. Sweden indicated that this tool is particularly successful in environmental crime – for example, when a company does not comply with environmental legislation, the fine would target the estimated gain made by the company. In 95% of cases, the National Unit for Environmental and Security Cases (REMA), part of the SPA, obtains judges' approval for its claims, totalling SEK 86 million (approximately EUR 9 million) between 2013 and 2015. EBM obtained approval for fines for SEK 7.8 million (approximately EUR 817, 000) between 2013 and 2015.

Table 15. **EBM & SPA Corporate fines claimed and awarded 2013–2015. The fines awarded by judges are included in parentheses**

Year	*2013*		*2014*		*2015*	
	No.	***Amount (million SEK)***	*No.*	***Amount (million SEK)***	*No.*	***Amount (million SEK)***
Corporate fine – EBM	*17* ***(6)***	*20.3* ***(3.7)*** *EUR 2.1 million* ***(EUR 387 000)***	*11* ***(5)***	*15.4* ***(1.2)*** *EUR 1.6 million* ***(EUR 126 000)***	*29* ***(11)***	*15.8* ***(2.9)*** *EUR 1.7 million* ***(EUR 304 000)***
Corporate fine (REMA) – SPA	*338* ***(335)***	***(31)*** ***(EUR 3.3 million)***	*351* ***(296)***	***(29)*** ***(EUR 3 million)***	*324* ***(229)***	***(36)*** ***(EUR 3.8 million)***

209. Corporate fines are from a legal point of view a penal reaction, not confiscation. In practice, however, corporate fines contribute to depriving criminals of proceeds, often in combination with confiscation and/or restitution. The size of a corporate fine is determined based on several factors, including the seriousness of the crime, which again may reflect the amounts of proceeds generated. In some cases, the restitutions may also reflect the sums saved by a business as a result of not complying with various legal requirements.

Recovery of the proceeds of tax crimes

210. Confiscation of proceeds of tax crime will normally be handled administratively through tax procedures by the Swedish Tax Agency (STA). This is considered to be Sweden's most significant risk when it comes to ML and associated predicates. Tax procedures are also used to confiscate other proceeds if there is insufficient evidence to pursue criminal confiscation, but possible to prove to a lower standard of proof that identified values have not been reported and taxed. Case examples of the latter were provided, showing that the tax procedures have contributed to depriving criminals of proceeds, for example from organised crime (see **Box 8**. below, Illegal Work Case – Malmö).

211. The duties of the Tax Fraud Investigation Unit within the STA consist of criminal investigations at the bequest of the prosecutor, as well as conducting intelligence operations and preventive work. This unit primarily investigates tax and accounting crimes, but can also be assigned other crimes by the prosecutor, for example ML, bribing, etc. When a tax crime has been committed, the STA investigates, issues a correction (if necessary with a provisional attachment claim) and can issue a tax surcharge of up to 40% of the proceeds of the tax evasion. Following a decision by the European Court of Human Rights in 2013 on double jeopardy of criminal and administrative reactions to the same crime, prosecutors will in some cases prosecute tax surcharges as a form of punishment in court. This explains the drop in the figures from 2013 onwards.

Table 16. **Recovered proceeds of tax crime plus tax surcharges for the last five years**

Year	*2011*	*2012*	*2013*	*2014*	*2015*
Total amount	SEK 2 449 mil (EUR 256 mil)	SEK 2 392 mil (EUR 250 mil)	SEK 2 478 mil (EUR 260 mil)	SEK 1 623 mil (EUR 170 mil)	SEK 1 523 mil (EUR 160 mil)

212. The table shows the proceeds recovered from tax crimes and tax surcharges; however, there are no statistics that discriminate between the two. Up to 40 % of the sums in the table may theoretically be the tax surcharges, but that portion is likely to be lower. In one example, a person had gained SEK 287 500 (approximately EUR 30 100) through VAT fraud, and the STA recovered the money plus a tax surcharge of 20 percent. While it is clear that the large part of the sums are recovery of proceeds of crimes, the sums also include some cases of unpaid tax recovered, where the lack of tax payment constitute a tax crime, but where the source of those funds were not criminal as such. The sums above only consider proceeds and surcharges of a punitive nature, and do not include fees for late declarations or late payments.

213. The EBM prosecutes tax crimes in close cooperation with the STA. The proceeds of the crime are normally confiscated by the STA through the process described above, but the prosecutors may choose to charge for accounting crime or other crimes if it is considered more effective (an example is provided below in **Box 8**. Illegal Work Case –Malmö).

Recovery of seized and confiscated assets

214. The table below shows that amounts of assets actually recovered based on seizures using provisional measures are increasing. This reflects a closer collaboration between LEAs and STA, and the Enforcement Authority, with the specific objective of increasing their effectiveness in completing confiscation and recovery of proceedings. It can also be explained by improvements in the selection of the provisional measures submitted for enforcement, in information-sharing on the location of assets, and asset tracing.

Table 17. **Percentage of ordered confiscations recovered by the Enforcement Authority (based on prosecutors seizure orders (KVA) and Tax Agency provisional attachments (BTS))**

	2011	2012	2013	2014	2015
KVA	33 %	59 %	39 %	32 %	49 %
BTS	33 %	38 %	38 %	49 %	55 %

Statistics Limitations and Case Studies

215. The statistics above present an incomplete picture of Sweden's confiscation activity, because the information is not sufficiently detailed to separate the different components of confiscation, and because only one SPA chambers included information on restitution claims. While the gaps in the statistics available make it impossible to get a comprehensive and detailed picture of the total amount of proceeds criminals in Sweden are deprived of, the available statistics do suggest that Sweden effectively seizes and confiscates criminal assets. Seizure and confiscation (as well as claims for restitutions, corporate fines, and the recovery of proceeds through tax procedures) is pursued to a large and increasing degree, even though the total value recovered has not yet shown an increase. The fact that the number of cases has increased, but that the amounts confiscated has not increased correspondingly, may indicate that the money is being followed in more and more cases, even minor ones. Statistics also suggest that an increasing proportion of claims for seizure and confiscation made by prosecutors are being upheld by judges: the overall number of confiscations awarded by judges has increased, and the percentage of the claims made by the SPA and awarded is high, which suggests that SPA prosecutors are successful in tracing assets and proving their criminal origin. Even though it is not possible to differentiate the recovery of (evaded) tax liabilities from the punitive tax surcharges applied, the overall value of assets recovered through tax procedures is significant, and is consistent with the high risk of tax evasion in Sweden. The percentage of criminal assets seized using provisional measures that are actually recovered has increased over time and is now around 50%.

216. Prosecutors utilise diverse paths to deprive criminals of their assets (restitution claims, confiscation, corporate fines, and tax procedures), and choose the most appropriate tool depending on the chances of success. Sweden showed further partial statistics, not included in the report, indicating that restitutions are not simply used to compensate for the harm made, but that they are used as a tool to recover the proceeds of crime. Furthermore, Swedish authorities have presented a number of case studies, for example from the GOB initiative, showing both that large sums have been recovered from criminals, and that various different tools (e.g. confiscation, restitutions, tax, corporate fines) are used together in a single case in order to recover all proceeds. Case examples were also shown to involve foreign predicates and proceeds from abroad (though separate statistics exist are not kept on the number or amounts of such cases, see also IO.2, and **Box 4**. Folarin). Some examples of ML from various predicates, and using different tools for recovering proceeds, are provided in IO.7 (Södertälje in **Box 2**.) and below.

Box 8. **Financial investigation revealing international criminal networks and enabling confiscation**

Investigation of "Telecom AB" – "Telia Case"

Sweden is investigating a case of suspected foreign bribery. A Swedish telecom company (Telia) is being investigated for alleged bribery payments to company T Ltd for around SEK 3 billion (USD 320 million). Sweden is also investigating Ms GK who effectively controlled company T Ltd. Sweden has cooperated with a number of jurisdictions and is tracing assets belonging to T Ltd in all countries that may be relevant. Sweden seized USD 30 million held in a Swedish bank, and recently decided the seizure against T Ltd for about USD 210 million held in Switzerland. Sweden has also assisted the USA and the Netherlands in the investigation of the local branch of the telecom company which resulted in a corporate fine and the confiscation of USD 795 million.

Case Ateljé

The investigation started in July 2013 with information from the United States about child pornography material being sent from someone in Sweden. The financial investigation identified transactions from the Swedish individuals' accounts to a producer of child pornography in the Czech Republic, as well as transactions to photographers in other countries. The financial investigation showed that the Swedish individual mainly used electronic payment systems and not bank accounts when sending or receiving money related to the child pornography. By following the money, the Swedish authorities saw links to several countries and found a worldwide network of persons who produce, distribute and receive child pornography material via the Internet. A search was made in three countries at the same time and information was sent to all other countries involved as well. One man was arrested in Spain, one in France, two in the USA, the photographers of the material were arrested in the Czech Republic and in Russia.

Prosecutors sought confiscation of SEK 1 million as proceeds of crime. When this case was tried in 2015, the court awarded restitutions of SEK 570 000 (approximately EUR 60 000) for the several injured parties and SEK 350 000 (approximately EUR 37 000) was confiscated. The defendant's house was seized to secure the claims.

Illegal Work – Malmö (see also in Box 5. above)

In that case, persons were convicted for ML and tax related crimes, however the proceeds of these crimes and other proceeds involved in these activities were subject to taxation.

As a result approximately SEK 9 million (approximately EUR 942 000) were "tax-confiscated", of which approximately SEK 7 million (approximately EUR 733 000) were provisionally seized. In addition, a tax surcharge of nearly SEK 1.4 million (EUR 147 000) was imposed.

Game Over[1]

The case concerned the unlawful provision of gambling in the form of gambling machines between 2011–2013. The gambling machines had been made available to the public by placing them in various shops. The machines allowed gamblers to participate in games distributed via a server in the Czech Republic. The verdicts concerned aggravated gambling offences, assisting aggravated gambling offences and gambling offences. Approximately SEK 5 million (approximately EUR 525 000), belonging to some of the 13 defendants and their company, was confiscated by the state as proceeds of crime.

Note:

1. Verdict 2014-01-24 Court of Appeal for West Sweden B 3172-13

217. The statistics do not allow assessors to quantify with precision the total amount of assets recovered from criminals. From the evidence provided, the amounts recovered are significant sums and consistent with the type of crime investigated and prosecuted in Sweden. Large amount of assets have been seized and/or confiscated when connected to a crime (e.g. the "Telia case"). Proceeds of tax crimes are largely identified, and are recovered through tax procedures. Some problems with the identification of large scale third-party ML has been noted under IO.6 and IO.7, which might impact the total amounts of assets that can be identified and recovered by Swedish prosecutors. When criminal activity is detected, Swedish LEAs efficiently trace assets, take measures to secure them, and are increasingly able to ensure awards by judges.

218. The legal and practical framework to follow the money, freeze, seize and confiscate money and assets all seem to be well developed and well used by the most important LEAs, and is supported by adequate resources and guidance. One concern which may impact the results is how far the money trail is being pursued. Some case examples show that the investigation may be concluded after the predicate crime is solved, and/or after the identified person/group of interest has been identified and successfully tied to criminal acts and proceeds. LEA representatives agreed that there is a potential to follow the money further to uncover more third-party launderers and facilitators.

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

219. Movements of currency across the border has been identified as a high risk for money laundering, yet Sweden has not taken sufficient measures to confiscate falsely or not declared or disclosed cross-border flows of cash. A report from the Police in 2010 identified a number of ML cases where couriers transported cash to the Baltic States and sent the money to bank accounts in Sweden.

220. The current legislation only provides for declarations of cash across the EU borders, which means that the legislation is currently inadequate to target the risk of undeclared cash within the EU. The national AML/CFT strategy has led to the development of a pilot project to target the activity which became operational in September 2016.

221. While this is a positive development, more work is needed to confiszcate falsely or undeclared cross-border transaction of currency within the EU, particularly where risk is higher.

222. Customs is tasked, among others, with combating cross-border crime, and receiving declarations of cash funds from travellers bringing in or taking out of the EU a minimum of EUR 10 000. Every week, Customs transmit the cash declarations to the FIU on an Excel sheet (up to 2015, the Excel sheet was transmitted every month). Customs cannot seize undeclared cash; however, it can contact the border police who have the powers to seize it. Customs indicated that it can question the traveller until the arrival of the police.

223. The border police regularly sends intelligence information on cross border transactions to EBM. Cases were provided, such as one where border police identified a growing number of money mules and did an intelligence-gathering operation. This also led to enhanced controls to detect undeclared cash.

224. In practice, Customs' controls on cash flows have been few, and rarely produced results in uncovering ML or TF activities. In 2015, Customs uncovered 1 case of inbound undeclared cash (value of approximately EUR 15 000). Customs identified 7 cases, in 2014 (value of approximately EUR 300 000) and 10 in 2013 (value of approximately EUR 210 000). Customs reports that in 2015 the sum of SEK 4.4 million was seized over 76 occasions. In 2016, more than SEK 1.6 million (approximately EUR 168 000) has been seized over 74 occasions. In one control operation targeting cash couriers at the airport, Customs conducted checks on 142 passengers, and identified no cases of undeclared cash. During the control, Customs identified two persons carrying smaller amounts of cash. The Swedish Law Enforcement Authority, participating in the operation, made two seizures: one of SEK 6 500 (approximately EUR 680) on a passenger arriving from Turkey, and one of SEK 5 500 (approximately EUR 576) on a passenger bound for Dubai.

Table 18. **Cash declarations received by Customs**

	Inbound	Outbound	Overall value (EUR)*
2013	373	360	392 million
2014	317	534	540 million
2105	329	601	700 million

Note:

* The overwhelming majority of the sums is declared by commercial operators in the retail sector at the border between Sweden and Norway.

225. Customs acknowledged their little involvement in AML activities, asserting that it was not prioritised to the same extent as narcotics and weapons, but did emphasise that the possibility to report suspicious activities to other LEAs is in place and is often used. However, a corollary to

investigating illegal narcotics and weapons is following the financial trail, which Customs does as a matter of course. In 2015, Customs conducted 54 financial asset investigations leading to confiscations of SEK 5.4 million. The corresponding confiscated totals for 2014 and 2013 were SEK 1.1 million (approximately EUR 115,000) and SEK 14.2 million (approximately EUR 1.5 million) respectively. Customs also mentioned its participation in cash control operations Athena 3 (2012) and Athena 4 (2014), two European-wide cash control operations. Customs, together with co-operating LEAs, analyse any relevant information such as patterns, modi operandi, countries of interest, etc. as a base for planning the operations.

Box 9. **Example of Customs investigation into narcotics leading to seizure and confiscation of bitcoin and SEK, as well as enhanced confiscation of the perpetrator's other assets**

In autumn 2015, Customs discovered that narcotics was being sold and transported by post. After surveillance and investigation, two men were arrested in January 2016, charged with having sold narcotics to more than 2 000 buyers. The two men had used an industrial building in Gothenburg to package and sell narcotics via the darknet to buyers in Sweden and 15 other countries, receiving payment nearly exclusively in bitcoin. Analysis of the history of the suspects' bitcoin wallets showed that the turnover of the narcotics business had exceeded SEK 6.6 million (approximately EUR 691 000); Customs seized bitcoin to the value of SEK 130 000 (approximately EUR 13 600) as well as SEK 160 000 (approximately EUR 16,700) in cash. On 15 August 2016, the Gothenburg District Court sentenced the main suspect to 10 years in prison for aggravated drugs, smuggling, doping, weapons and money laundering offences. The cash and bitcoin, along with various drugs and two weapons, were confiscated, and the court further ordered the provisional attachment of SEK 2 million (approximately EUR 210,000) of the perpetrator's assets—the figure corresponds to his estimated profit from the narcotics sales. If the Enforcement Authority is unable to seize assets equivalent to SEK 2 million (approximately EUR 210 000), the perpetrator will be in debt to the state upon his eventual release from prison. The verdict is expected to be appealed to the Court of Appeal for Western Sweden—both by the perpetrator and by the prosecutor, who wanted a sentence of 12 years in prison.

The accomplice was sentenced to 2 years and 6 months in prison. Criminal investigations of other suspects continue.

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

226. The available statistics and anecdotal evidence suggest that proceeds are confiscated generally in line with the predicate crimes identified as higher risk, and in line with Sweden's policies and priorities. Particularly, the proceeds of tax crime – the offence generating the highest proceeds in Sweden – is effectively pursued and recovered through tax procedures. Sweden does not estimate the size of the illegal economy or the sums thought to be laundered (although it estimates the volume of tax evasion), and as mentioned above, there are difficulties in measuring the aggregate results. While it is clear that the relevant agencies pursue confiscation in line with the policies, these

policies are rather general, and there are no system-level performance indicators. The Government could use better benchmarks or tools to determine whether the confiscation policies are successful and are in line with the ML/TF risk profiles.

Conclusions

227. Sweden has a well-developed practical and legal framework for confiscation, based on high-level commitment to pursue the recovery of proceeds. The Government's policy to make crime unprofitable is pursued through a number of legal means, and the statistics suggest that, when criminal activity is detected, Swedish LEAs do efficiently trace assets, take measures to secure them, and are increasingly able to ensure that judges award the confiscation of criminal assets. Even though complete information on the sums recovered from criminals are not available, the evidence presented and the case examples provided indicate that these represent significant sums which are broadly consistent with the crime environment. In particular for tax crimes, which are the most significant proceeds-generating crimes in Sweden, significant assets are recovered using tax procedures.

228. The lack of clear statistics on the assets recovered from criminals make it challenging to quantitatively assess the degree to which Sweden achieves the objectives of its confiscation policies. Despite the incomplete statistical picture, the case examples presented by Sweden indicate that LEAs do effectively trace and recover criminal assets and meet the agency-level objectives. Depriving criminals of their proceeds is also clearly an integral part of investigators' and prosecutors' work, and is supported by dedicated staff and processes and is actively managed as a performance objective. The Government's policy to make crime unprofitable is actively pursued by LEAs, and the assets actually recovered appear consistent with the Swedish crime environment.

229. More detailed policies and measurement tools/statistics should be developed to establish more clearly whether the system is delivering effective results. This represents a moderate improvement.

230. **Sweden has achieved a substantial level of effectiveness for IO.8.**

CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Key Findings and Recommended Actions

Key Findings

Terrorism financing investigation and prosecution – TF offense (Immediate Outcome 9)

- Sweden has only prosecuted a small number of TF cases. This is largely in line with expectations, given Sweden's size and level of TF risk. It also reflects the difficulty of successfully conducting prosecutions for terrorist financing under the old criminal offence, which was in force up to April 2016. The new TF offence, in effect since April 2016, appears to address these problems, but it is too early for its practical impact on effectiveness to be widely felt. The speed and the cross-party consensus with which the new TF offence was adopted also show the political priority which is given to combating terrorist financing in Sweden.
- Swedish authorities prioritise combating terrorist financing and have developed methods and capacity to pursue it. Financial investigations are conducted alongside all counter-terrorism cases, and authorities seek opportunities to disrupt terrorist financing activity even when it is impossible to obtain a conviction for TF. There is active and well-coordinated inter-agency and international cooperation, including through dedicated liaison staff, and TF is reflected in Sweden's measures to prevent terrorism and violent extremism.
- Sweden appears to have in place all the elements needed for a substantial level of effectiveness. However, Sweden's CFT framework was only completed recently, with the introduction of a revised TF offence in April 2016, and therefore Sweden does not yet have a long track record of successful TF prosecutions. Sweden still needs to build experience and precedents for applying the new TF offence in practice. There is also scope to improve outreach to the financial sector and supervisors.

TF related targeted financial sanctions and NPOs (Immediate Outcome 10)

- Sweden's implementation of targeted financial sanctions (TFS) against terrorist financing is ineffective, mainly because of serious technical deficiencies that are inherent within the framework of applicable EU regulations (as described under the discussion of R.6), and Sweden's failure to use either mechanism to propose or make designations. Sweden has no mechanism to use TFS at a national level in response to terrorist threats affecting Sweden. Sweden has never on its own proposed a designation to the UN under resolution 1267, or to the EU under common position 2001/931/CFSP, and has no mechanism to make its own designations pursuant to resolution 1373. Sweden also suffers excessive delays in the transposition of UN sanctions, and gaps in the ability to sanction EU internal terrorists.
- Sweden has a solid and effective framework of measures to prevent the misuse of NPOs. While there is very limited formal oversight or supervision, this is complemented by strong self-regulatory initiatives and voluntary engagement with government agencies. Rigorous self-

regulatory measures apply to NPOs that account for a significant portion of the financial resources under control of the sector, and additional oversight by SIDA applies to those which represent a substantial share of the sector's international activities.

- Although Sweden has a good understanding of the terrorist financing risks, it cannot and has not used TFS effectively to mitigate the risks, including those arising from foreign terrorist fighters and returned foreign terrorist fighters. This appears to weaken authorities' ability to prevent terrorist financing flows.

Proliferation financing (Immediate Outcome 11)

- Sweden implements TFS regarding proliferation financing through EU measures. There are delays in the transposition of UN designations into EU sanctions lists - although the practical effect of these delays has been mitigated by the fact that EU lists are more extensive than the UN lists, and by requirements for prior approval of transactions with Iran. Overall, persons and entities designated by the United Nations Security Council Resolutions (UNSCRs) on proliferation of weapons of mass destruction (WMD) are identified, deprived of resources, and prevented from raising, moving, and using funds or other assets for the financing of proliferation. TFS relating to proliferation are in a technical sense not implemented without delay, owing to the time taken to transpose UN designations into EU regulations. However, in the case of Iran, sanctions were implemented without delay as a result of the more extensive EU sanctions regime, and in the case of DPRK, the risk posed by delays is largely mitigated by the negligible trade and financial links between Sweden and DPRK.
- Financial institutions and DNFBPs routinely screen customers and transactions against EU and UN TFS lists, and supervisors review the application of such controls. However, smaller FIs and DNFBPs do not seem to have an appropriate level of awareness of their obligations.

Recommended Actions

Immediate Outcome 9

- Pursue TF investigations through to prosecution for TF offences, and seek to apply dissuasive penalties, so as to build experience and establish precedents for prosecution under the revised TF offence

Immediate Outcome 10

- Urgently introduce legal powers in Sweden which will enable authorities to apply TFS relating to terrorism or proliferation, (i) as a bridging measure while UN sanctions are awaiting transposition into EU regulations; (ii) to EU internal terrorists who are not subject to asset freezing measures under EU regulations; and (iii) on a national basis, at the instigation of Swedish authorities
- Establish a body or mechanism responsible for identifying potential targets for designation, developing proposals for designation, and considering whether to propose designation to the EU or UN, or to use national designation powers.

- Use TFS in practice when an appropriate case arises, so as to properly establish the legal and procedural basis for using them, enabling them to be routinely considered by security and counter-terrorism authorities in relation to individual cases.
- *(for IOs 9, 10, and 11)* Establish regular fora or mechanisms for communication with supervisors and the private sector about TF and PF risks and obligations, to encourage closer collaboration and better information-sharing in both directions

Immediate Outcome 11

- Sweden should enable TFS related to PF to be implemented without delay in cases where the entity has not previously been listed by the EU. Sweden should consider establishing a system enabling assets of persons and entities designated under the relevant UNSCRs to be frozen temporarily, while waiting for UN decisions to be transposed into decisions of the EU Council. Sweden should raise awareness of TFS related to proliferation among small- and medium-sized reporting entities

231. 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.5-8.

Immediate Outcome 9 (TF investigation and prosecution)

232. Sweden faces terrorist financing threats in relation to fundraising for terrorist groups and violent extremists active in Sweden or other countries, and in particular in relation to foreign terrorist fighters. As noted in relation to IO.1, Sweden's National Risk Assessment for terrorist financing was completed in 2014, shortly before the full emergence of ISIL in Syria, and therefore is not a good reflection of the risks faced today in Sweden. A subsequent follow-up report has expanded the national understanding of risks relating to the financing of FTFs. Since 2012 Swedish authorities have noted a shift in the terrorist threat from support to participation in overseas terrorist groups. Foreign terrorist fighters and particularly returned FTFs, as well as lone wolves who have not left Sweden, make up the most significant terrorism and TF threat in Sweden (see **Box 12**).

233. Säpo and other authorities involved in counter-terrorism nevertheless have a clear understanding of the current threats, based on their own analysis and on threat assessments produced by the National Centre for Terrorist Threat Assessment (NCT), a multi-agency analysis centre involving Säpo, the Swedish National Defence Radio Establishment, and the Swedish Military Intelligence and Security Service (Must). The NCT produces terrorist threat assessments, including an annual assessment of the terrorist threat to Sweden and Swedish interests abroad, which are updated continuously and also address terrorist financing. A TF threat assessment was produced by Säpo in October 2015. The risks that have been identified are both current and relevant.

4

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

234. Sweden has only prosecuted a small number of TF cases. This is largely in line with expectations, given Sweden's small size and moderate level of TF risk, in comparison with other countries. The emergence of ISIL and the associated risks from FTFs has significantly changed the TF risk environment in Sweden, but is recent, and TF cases related to these risks are just starting to reach courts. The small number of prosecutions may also reflect the difficulty of successfully conducting prosecutions for terrorist financing under the old criminal offence, which was in force up to April 2016. Successfully prosecuting TF under the pre-2016 offence required prosecutors to prove intent that the funds would be used for terrorism.

235. Authorities provided two case studies in which terrorist financing investigations were ultimately unsuccessful because investigators could not prove intent, as they were not able to trace the final recipient of funds within Somalia (one of which is described in **Box 11**, below). Only one case resulted in a conviction for TF under the pre-2016 offence. This was completed in April 2005 and was described in Sweden's previous Mutual Evaluation. Authorities note that even though prosecution was impossible in several cases, they nevertheless disrupted the TF activity.

236. Sweden introduced a revised criminal offence of terrorist financing in April 2016, responding to new UN resolutions and revisions to R.5. Among other changes the new offence allows conviction of a person who knowingly or intentionally provides funds to a terrorist individual or group, rather than only for a specific terrorist act. This will overcome one key deficiency of the pre-2016 offence. Since August 2015 the range of preventive and disruptive measures available was expanded, by allowing a Prohibition on Disposal of Property (PDP) to be applied by Säpo in TF cases. In total Sweden has convicted two individuals of terrorist financing, in relation to a single case in April 2005. In other cases, persons of interest have been convicted for other offences, e.g. economic crime (see paragraph 253).

Box 10**. Prosecution for an alternative offence resulting from a Terrorist Financing investigation**

Several individuals were suspected of using their position in a non-profit organisation to redirect charitable donations to terrorists in Syria and Iraq, and using anonymous social media accounts to provide instructions on how money could be directed to purchase weapons. The investigation of TF was integrated with investigation of wider support networks and sought to disrupt both. Investigators used techniques including secret communication, surveillance, communications control, and electronic seizures - in particular of data traffic with social media- which was used to link the individuals to the social media account.

One individual was prosecuted as a result of this investigation. This activity occurred prior to the introduction of the revised TF offence, and it was ultimately impossible to prove that he collected money which was used for terrorist purposes (as was required under the old TF offence), only that he had encouraged others to do so. He has therefore not been charged with TF but instead with provocation offences under the *Act on Criminal Responsibility for Public Provocation, Recruitment and Training concerning Terrorist Offences and other Particularly Serious Crime* (2010:299). The trial remained ongoing (as of January 2016).

237. Sweden's criminal code includes offences of encouragement of terrorist crimes, which apply to encouragement of terrorist financing. This is relevant to emerging TF methodologies such as crowdfunding through social media, as it allows prosecution of those who publicise calls for funding or provide information about how to provide funds, even if they do not themselves provide funding. Sweden has also criminalised providing or receiving funds for persons who have the intention to travel for terrorist purposes. This new offence can be used to disrupt travel of FTF and their facilitators.

TF identification and investigation

238. It is clear that terrorist financing is embedded within Säpo's priorities and significant resources are allocated to it. Säpo's priorities include stopping or disrupting terrorists and their facilitators, financiers and recruiters. Terrorist financing cases are investigated by a specialised unit of TF investigators at Säpo, and by other units which also have training in financial investigation and terrorist financing. Financial investigation is also supported through cooperation with other agencies including police, EBM, and prosecutors. Säpo has embedded liaison staff from key agencies to ensure efficient communication and intelligence/information exchange and assessment.

239. Säpo have developed methods to work proactively with financial intelligence in all cases. All CT investigations include a financial dimension - there is always some investigation of TF in relation to CT cases, and financial intelligence is routinely used as a source of intelligence in all CT investigations. Financial intelligence is viewed as a building block of the investigation and used routinely alongside communications or other information.

240. Terrorist financing investigations routinely include information from the FIU. This includes both cases identified and disseminated by the FIU as terrorist financing on the basis of an STR, and cases opened using the FIU's power to launch an "initiative case" even in the absence of an STR, at the suggestion of Säpo. The FIU has opened a total of 45 such TF cases since 2011. These cases have made use of Fipo's powers to request information from banks and other reporting entities, prior to the launch of a formal preliminary investigation. These powers can also be used in response to requests from foreign countries.

241. TF investigations can potentially also make use of Säpo's *prohibition on disposal of property* (PDP) powers (Fipo also has PDP powers, as described in the assessment of IO.6). This mechanism gives the facility to stop the money before a formal investigation whilst it is in its pre-investigation phase. Säpo was provided with this power very recently and had therefore not used it at the time of the on-site visit in relation to terrorist financing investigations. It is believed that the new legislation that came into force on 1 April 2016 will make it easier to do this.

Box 11. **Foreign Terrorist Fighters**

Since 2012 Swedish authorities have noted a shift in the terrorist threat from support to participation in overseas terrorist groups. To date around 300 foreign terrorist fighters have left Sweden for Syria, and many have since returned to Sweden. This is around ten times the total number involved in conflicts in Iraq, Afghanistan and Somalia. Foreign terrorist fighters and particularly returned FTFs make up the most significant terrorist threat and TF threat in Sweden - both individually because they are radicalised and have received paramilitary training, and socially since they return with credibility and contacts, and can inspire or recruit others. Fundraising for FTFs is based on social networks of family and friends, as well as on petty crime, but is not large scale or organised.

Swedish authorities' approach is to stop FTFs from leaving Sweden, or to otherwise ensure they are prevented from reaching Syria. Prior to the introduction of the new laws in April there were limited tools for doing this. Since 1 April 2016 there is a new offence criminalising travel for terrorist purposes (and the financing or encouragement of this act). This will enable the prosecution of FTFs and their facilitators, though no cases have yet reached this stage. The change also allows Fipo and Säpo to use PDPs quickly, while the suspect is travelling, to disrupt their travel plans. Additional measures are also used to disrupt the finances of FTFs while they are outside Sweden, e.g. by cutting welfare payments.

A risk based approach is taken in assessing and addressing the risk posed by returnees. Returning FTFs may be interviewed by Swedish authorities, to understand their motivations for returning (e.g. disillusionment, visiting family, or recruitment), and as a way to deter them from engaging in terrorist activities. Disillusioned former FTFs m ay also be referred to other agencies and organisations that can assist their reintegration into society.

TF investigation integrated with- and supportive of- national strategies

242. Sweden's national counter-terrorism strategy was adopted in August 2015. The Strategy sets long term priorities focused particularly on prevention, including measures to counteract radicalisation and recruitment to extremist and terrorist groups. One key element of this is the work of the National Coordinator against Violent Extremism (see **Box 13**. below). The other main strands of the Strategy are pre-emption (focused on counteracting the capability and opportunity of terrorists to mount attacks) and protection (focused on protecting individuals and society from attacks). Säpo's priorities include stopping terrorist attacks in Sweden and preventing the facilitation of terrorist activity elsewhere. The national strategy is the basis for specific goals for the relevant agencies and units, set through an annual planning process.

243. Combatting terrorist financing is a key priority within the *pre-empt* strand of the national counter-terrorism strategy, which sets the objective to "*Improve the efficiency of work to detect and counter the funding of terrorism and better integrate it with other counter-terrorism work*". The strategy strongly emphasises cutting off the financing of terrorism as an important opportunity for Swedish authorities to act to pre-empt terrorist acts, and highlights the importance of cooperation

between the relevant authorities, in particular Säpo, the police, and the FIU. This appears to be well-supported in practice. The national counter-terrorism strategy also emphasises the need to improve information exchange with market actors and with supervisory authorities, in both directions, though this appears to be less-well established in practice (see below).

244. Strategic coordination of Sweden's counter-terrorism activities (including terrorist financing) is done through the National Counter-Terrorism Cooperative Council (NCTCC). The Council does not have a formal mandate but is a network of fourteen heads of agencies which work together at national level to improve coordination and improve the efficiency of the agencies' work to combat terrorism.

245. The Security Service (Säpo) is Sweden's main counter-terrorism authority. Until 2015 Säpo was formally part of Sweden's Police Authority. Since 1 January 2015 it has been established as an independent agency, with responsibility for counter-espionage, counter-terrorism, counter-subversion, dignitary protection, protective security, and counter-proliferation. Counter-terrorism is Säpo's top priority. Functionally Säpo acts as both an intelligence agency and a law enforcement agency, and has full police powers.

246. Since Säpo has become an independent authority it has expanded its capabilities, developed methods to work pro-actively with financial investigation in counter-terrorism cases (as noted above) and integrated financial investigation into all investigations, for example, the two major counter-terrorism investigations conducted in 2010 (into a suicide bombing in Stockholm) and 2011 (into an attempted attack by Swedish residents on the offices and staff of Jyllandsposten in Copenhagen) both included financial investigations of the perpetrators, and of the transactions involved in preparing and conducting the attacks. It has enhanced its capability against TF. Following its establishment as an independent agency, Säpo continues to cooperate closely with the police, and can draw on police support for operations.

247. Säpo works with a dedicated National Security Unit (NSU) within the Swedish Prosecution Authority (SPA), which is responsible for overseeing investigations and conducting prosecution of specific offences including terrorism and terrorist financing (and proliferation). This unit is composed of specialised prosecutors, who manage sensitive cases separately from the rest of the SPA (but can also draw on SPA support when needed, including other specialist prosecutors and forensic accountants).

248. Cooperation with the police is prioritised in the ordinance establishing Säpo. As noted above in relation to investigation of TF, practical measures are in place to ensure strong cooperation with key agencies, including standing arrangements for operational support by the Police (NOA). Säpo has taken steps to ensure sound cooperation on TF is possible with other relevant agencies, including work with EBM. Threat assessments identified that the proceeds of economic crimes within EBM's responsibility can be used for TF. EBM lacked knowledge of TF and there was a lack of systematic intelligence transfer between EBM and Säpo. This has been addressed through a six months action plan during which Säpo educated EBM investigators on TF. Similar awareness-raising has been done with Customs and the Tax Agency. Cases provided to assessors demonstrate effective operational cooperation between Säpo and other investigative agencies on terrorist financing cases and the financial investigation of FTFs.

4

249. Säpo has conducted outreach to financial institutions on terrorist financing risks and vulnerabilities. One example is payday loans: An analytical debrief of FTFs showed returnees have taken out payday loans before they leave. Banks were informed and this information was also publicised through radio interviews with TF experts from Säpo; twitter; and the Säpo website. Säpo have taken part in the production and dissemination of an e-learning programme for the private sector thereby giving them the ability to reach and educate large numbers of employees of the private sector around the risks of TF and, together with Fipo, conducted workshops in 2015 and 2016 with the money remittance sector addressing the risks that they may face.

250. Communication and coordination between Säpo and supervisory authorities is not yet sufficiently well-established. Säpo's contact with the FSA is regular, but less so with other supervisors. Initial steps have been taken to address this: Säpo now sits on the coordinating supervisory body for the AML/CFT and this body sets an action plan on communication of TF risks to reporting entities. Nevertheless, this is only one channel to disseminate information on TF risks, and further coordination with supervisors may be desirable to ensure financial institutions and DNFBPs have an up-to-date understanding of the risks and implement preventive measures appropriately. This could also enhance authorities' ability to exploit financial intelligence and apply appropriate disruptive measures.

Box 12. **National Coordinator against Violent Extremism**

A national coordinator to safeguard democracy against violent extremism was appointed in 2014, in order to develop preventive measures against violent extremism and in particular to promote cooperation with and between local and municipal authorities. The coordinator takes a bottom-up approach focused on engaging all relevant actors at a local or municipal level - building awareness of the risks of violent extremism, and their relevance and impact at local level, then developing local action plans to deal with those risks. A range of stakeholders are involved, including local authorities and providers of public services; schools; civil society; and each municipality nominates a contact person who coordinates activity locally. To date the unit has visited 260 out of the 290 municipalities.

The goal of the programme is for all municipalities to have preventive measures against violent extremism embedded, so that they can recognise and deal with it early. This includes entering into dialogue with potential extremists, encouraging them away from radicalisation. The Coordinator has sought to provide knowledge and support for local practitioners, to give them the confidence to have active conversations with potential extremists. This activity fits alongside other initiatives including support provided through NPOs for people seeking to leave extremist groups or environments, and a hotline (operated by the Red Cross) to provide advice to people concerned about friends or family members who may have links to violent extremist ideologies. The hotline is confidential and cannot provide any intelligence to the relevant agencies, although there is a separate hotline where the public can report information to Säpo, and a support line provided by the Coordinator for families concerned with extremism.

The coordinator's remit is not limited to terrorist threats or specific types of ideology, but includes all ideologies that promote violence which could affect democracy. The Coordinator is an initiative overseen by the Ministry of Culture, so it is not seen as an initiative led by law enforcement or security authorities. Nevertheless, the National Coordinator is joined-up with national counter-

terrorism authorities: Säpo is part of the reference group providing strategic assessments to the Coordinator. This initiative has also, in effect, established a municipality-by-municipality means of identifying and addressing risk within the community, which can be a potentially valuable source of intelligence to counter-terrorism authorities. This is a good example of preventative work that fits in with the national CT strategy, providing good support for Säpo. Nevertheless there is scope to make more use of the opportunities created by this initiative to gather practical intelligence - e.g. through more extensive intelligence-sharing between the relevant agencies

Effectiveness, proportionality and dissuasiveness of sanctions

251. It is not clear that the sanctions being applied to persons convicted of the TF offence are effective, proportionate, and dissuasive. As noted in the analysis of technical compliance, Natural persons convicted of TF are punishable with imprisonment for up to two years in normal cases, or for between six months and six years in gross cases. These penalties are consistent with the sanctions applied for other comparable crimes in Sweden: the same range of penalties applies for money laundering or for public provocation, recruitment, or training for terrorism. While terrorist acts are punishable with 4 years to life imprisonment.

252. It is impossible to assess whether the sanctions actually applied in relation to TF cases are effective, proportionate, and dissuasive, because of the small number of convictions obtained. For the two TF convictions obtained (in 2005), the sentences applied were 5 years and 4.5 years of imprisonment. Nevertheless, the low range of available sanctions is a concern for future potential serious TF cases. The limited range of sanctions available under Swedish law, compared to other countries (including neighbours) could potentially contribute to making Sweden a more attractive location for terrorist financers and facilitators. Swedish law also includes alternative offences which could apply to some cases of TF activity and which carry higher penalties, e.g. the offence of preparation of a terrorist offence, pursuant to the Terrorist Offences Act, which is penalised with up to 18 years imprisonment.

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

253. Swedish authorities do seek opportunities to disrupt terrorist financing activity when it is impossible to obtain a conviction for the offence of terrorist financing. This is done principally through investigation and prosecution for alternative criminal offences. This is particularly relevant given the difficulty of obtaining a conviction for terrorist financing prior to the amendment of the TF offence in April 2016. To facilitate this disruption activity, Säpo sits on all relevant national strategic and operational forums, including the GOB (described in relation to IO.7) where disruption opportunities have been used by other law enforcement agencies. There is evidence of good cooperation between all law enforcement agencies with all recognising the importance of addressing TF.

254. Sweden's judicial rules on the admissibility of evidence mean that information obtained through covert means (e.g. by Säpo in its role as an intelligence agency) can in principle be admitted in a Swedish court (though it might not be used for other reasons). This could reduce the likelihood

that counter-terrorism agencies would be compelled to disrupt a terrorist threat before they have assembled sufficient admissible evidence to prosecute.

255. Swedish authorities do investigate potential terrorist financing activity, with a view to bring a prosecution under the TF offence. Cases can arise where an investigation identifies TF activity, but there is not sufficient evidence to successfully prosecute for a terrorist financing offence (as was sometimes the case under the pre-2016 TF offence, which had a high evidential threshold), or where there is an urgent need to disrupt the activity, even though evidence gathering is incomplete. In such cases, Swedish authorities explore whether it is possible to prosecute for other offences. This may involve prosecution for an alternate offence based on evidence already obtained through the investigation of the TF offence, or further investigation by another authority (with financial investigation support provided by Säpo to the relevant authority) prior to prosecution. The dedicated National Security Unit (NSU) within the Swedish Prosecution Authority (SPA) is responsible for decisions on whether to continue investigations for TF offences or to pursue alternative criminal charges as a means to disrupt TF activity. Investigations by Säpo of terrorist financing activity have led to investigations and prosecutions for fraud, tax evasion, and benefit fraud by EBM and other agencies. There have been more than a dozen cases in 2015-16 where other offences have been used to disrupt TF activity. These include persons investigated for TF who were convicted of aggravated accounting and tax crimes (one party imprisoned for 4½ years and another for 2½ years); and aggravated fraud and accounting crime (with imprisonment for 2 years).

Box 13. **Persons of TF interest prosecuted for other offences**

Säpo noticed in 2013 that a person of interest (for potential involvement in TF) was investigated and found to be selling mobile phones with connections to Finland. After cooperating with Swedish and Finnish authorities, the actor was sentenced to three years in prison, reduced to two years and eight months upon appeal (final verdict in June 2016) for aggravated accounting and tax crimes.

Box 14**. Investigation/disruption of potential terrorist fundraising**

Three men were arrested in February 2008 on suspicion of terrorist financing, having been involved in a fundraising activity in Stockholm, allegedly to finance terrorist acts in Somalia. SEK 65 000 (approximately EUR 6 800) had been raised through charitable donations by individuals of Somali descent, and sent to Somalia. Based on intelligence, Swedish authorities believed the funds were diverted to purchase weapons. The investigation involved a period of surveillance prior to the arrests; interrogation of the suspects; simultaneous raids by Norwegian and Swedish police, and the tracing of international wire transfers.

Ultimately it was not possible to gather sufficient evidence to prosecute: the offence in force at the time required proof of intent. This could not be obtained because of the difficulty of translating unambiguously from monitored conversations; and because it was not possible to trace the ultimate destination of the funds (due to lack of cooperation from authorities in another jurisdiction, and because the destination was in ungoverned territory). While prosecution was not possible, the investigation and arrests did disrupt the activity.

256. When authorities do not identify an alternative criminal offence which can be pursued as a means to disrupt the persons conducting terrorist financing activity, they can use preventive measures, including Prohibitions on Disposal of Property (PDPs), which target the funds directly, giving the ability to "freeze" any funds and prevent travel whilst an investigation commences. The funds can be "frozen" for the duration of the investigation. This expands the range of disruption tools available. Since the new TF offence took effect on 1st April 2016, PDPs can potentially be used when someone is suspected of travelling for terrorist purposes, making it more difficult for them to travel (although this has not yet been done in practice).

257. Authorities also liaise with relevant bodies able to exercise vigilance or apply their own measures, including local government, banks and other financial gatekeepers, and international CT networks. Analysts look for networks within investigations to identify persons if interest and look for different ways to disrupt them. An example of this would be Säpo visiting money service remitters and advising them of their vulnerabilities when they had been identified as being used.

Box 15**. TF - Crime links**

GOB investigation

This operation began in April 2014 and focused on identity-related crime by a "person of strategic importance" identified as a target under the GOB initiative, and his network. There have been connections between this case and cases concerning TF and FTFs in known Eastern criminal groups. The network was involved in intimidation and threats against front men; then setting up false businesses and using false identities in order to take advantage of benefits and grants from public agencies. Proceeds were transferred through the UK and Latvia, to a range of other countries including Turkey, China, Hong Kong, and the UAE.

This has been a very large-scale case, involving cooperation between the Police, Säpo, EBM, and Tax Agency and others, as well as collaboration with authorities in eight other countries. So far three individuals have been convicted as a result of this operation, and 53 refusals of immigration issued. The case has also led to the large-scale recovery of proceeds through tax increases, attachments, recovery claims, and sequestration of assets.

Operation Navet

Navet was an operation which targeted identity relation crime and where there were concerns that parts of the operation were linked to TF. The criminality consisted of establishing businesses using false identities with the purpose of taking advantage of the benefits and grants from public agencies. Five people have been prosecuted with three being sentenced to imprisonment for a total of 5 years and 10 months. Three people were also banned from engaging in business activities for a total of 15 years.

Conclusions

258. Sweden has only prosecuted a small number of TF cases. This is largely in line with expectations, given Sweden's small size and the nature of its TF risks, in comparison with other countries. The emergence of ISIL and the associated risks from FTFs has significantly changed the TF risk environment in Sweden, but is recent, and TF cases related to these risks are just starting to reach courts. The small number of prosecutions may also reflect the difficulty of successfully conducting prosecutions for terrorist financing under the old criminal offence, which was in force up to April 2016. The small number of convictions obtained makes it difficult to assess whether the sanctions actually applied in relation to TF cases are effective, proportionate, and dissuasive.

259. The new TF offence, in effect since April 2016, appears to address these problems, but it is too early for its practical impact on effectiveness to be felt. The speed and the cross-party consensus with which the new TF offence was adopted also show the political priority which is given to combating terrorist financing in Sweden.

260. It is clear that terrorist financing is embedded within Säpo's priorities and significant resources are allocated to it. Säpo have developed methods and capacity to work proactively with financial intelligence, and conduct financial investigations alongside all counter-terrorism cases, and has a culture of pursuing the money, and of collaborating actively with other agencies on any financial investigation with potential links to terrorism, including those related to organised crime. Swedish authorities investigate terrorist financing activity with a view to prosecuting for TF offences, but also seek opportunities to disrupt terrorist financing activity when it is impossible to obtain a conviction for TF. There are also examples of successful international cooperation on investigations and prosecutions.

261. Combatting terrorist financing is a key priority within the national counter-terrorism strategy, and appears well-coordinated at policy level. At operational level there is good cooperation between agencies, including through dedicated liaison staff. Outreach to the financial sector has shown its value, but communication and coordination between Säpo and supervisory authorities is not yet sufficiently well-established.

262. Following recent reforms - in particular the introduction of a new TF offence - Sweden appears to have in place all the elements for a substantial level of effectiveness. At the time of the on-site visit, the new offence had been in place for only two months, but there are early indications that the new offence will have a positive effect.

263. Sweden has achieved a substantial level of effectiveness for IO.9.

Immediate Outcome 10 (TF preventive measures and financial sanctions)

Implementation of targeted financial sanctions for TF without delay

264. Sweden's implementation of targeted financial sanctions (TFS) against terrorist financing is ineffective, mainly because of technical deficiencies that are inherent within the framework of applicable EU regulations (as described under the discussion of R.6), and Sweden's lack of a mechanism to propose or make designations under either EU regulation.

265. Sweden implements targeted financial sanctions (TFS) against terrorism through a common EU framework of Regulations (which are directly applicable in Sweden) and EU Council Decisions. EU mechanisms are used to implement both UN sanctions under UNSCRs 1267/1988 and 1989 and their successor resolutions, and to apply sanctions at EU level pursuant to UNSCR 1373. Sweden does not have any independent legal powers to designate individuals or entities for TFS at national level.

266. Targeted Financial Sanctions under UNSCRs 1267/1988 and 1989 and subsequent resolutions are not implemented without delay. This is due to the time taken at EU level to transpose new UN designations into the relevant EU legal instruments. These delays have reduced in recent years: in 2013, transposition of designations under UNSCR 1989 took 7 to 29 days; and designations under UNSCR 1988 took between 7 days to 3.5 months.[20] Since 2015, an expedited procedure has been adopted by the European Commission for implementation of new listings, which has reduced the delay to approximately 4-11 working days of the UN decision. Nevertheless, even the shortest possible time for transposition into EU law is not consistent with the requirement to implement sanctions without delay. This is a serious impediment to Sweden's effectiveness in preventing terrorists using funds.

267. The freezing obligations of resolution 1373 do not apply to EU internals, although the Treaty of Lisbon (2007) provides a legal basis to introduce a mechanism to do so. Sanctions adopted under EU Regulation 2580/2001[21] are immediately applicable in all EU member states. However, as noted in the analysis of technical compliance, freezing measures under this regulation can be applied only to persons linked to terrorist activities posing a threat to international peace and security and not to "EU Internal Terrorists".

268. Sweden has recently clarified the channels for receiving foreign requests for freezing action under UNSCR 1373, in the context of the FATF Handbook on requesting freezing action. No requests have been received in practice. Requests from third countries for Sweden to take freezing action would be passed to the EU for consideration under EU mechanisms.

269. Sweden has never made any use of targeted financial sanctions to respond to terrorist threats to Sweden, and lacks the means to do so. Sweden does not have powers to designate individuals or entities for TFS on a national basis. As a member of the EU and UN, Sweden could in principle propose entities for designation under the EU or UN TFS regimes. However Sweden has only once made such a proposal to the UN (in 2002, when Sweden co-sponsored a designation proposal to the 1267 Committee), and has never made such a proposal to the EU. Sweden has not assigned anybody or competent authority with the responsibility for identifying targets for designation under EU or UN TFS.

270. Swedish counter-terrorism authorities do not have the capacity to apply TFS for practical purposes, and this weakens their ability to respond to terrorist threats. They are aware of UN and EU TFS regimes, but they do not consider the use of TFS in practice as a tool for managing terrorist financing risks. In Sweden's case, the lack of proposals for designation does not appear a

20 In the third round of mutual evaluations, these delays ranged generally between 10 to 60 days.

21 Through Common Positions 2001/930/CFSP and 2001/931/CFSP

consequence of the lack of good targets who meet the relevant criteria for designation: at the end of 2015, around 300 Swedish residents had travelled to Syria to fight for ISIL, and around 140 of these foreign terrorist fighters have subsequently returned to Sweden. While Swedish authorities have other tools to manage individual cases, it is possible that the practical inability to apply TFS is limiting their ability to respond to the terrorist threat.

4

271. Sweden is considering measures to address these weaknesses. A Government Committee of Inquiry has been mandated to prepare legislative proposals by 31 December 2017 on "bridging measures" at national level to address both the delays at EU level and the gaps in the EU powers to apply TFS to "EU Internal Terrorists". It will also analyse and submit proposals for how an effective system could be created to identify at national level persons and entities for decisions on targeted financial sanctions against terrorism and the financing of terrorism in line with Sweden's international commitments. At the time of the on-site this Committee had not yet been established in practice, though it has since been established.

272. Swedish authorities do not have any mechanisms to communicate UN or EU designations to financial institutions and DNFBPs, and rely on EU mechanisms to communicate new designations to regulated entities. EU designations are published in the EU Official Journal and website, and included in a consolidated financial sanctions database maintained by the European Commission, with an RSS feed.

273. In practice, the larger reporting entities and the MVTS providers check and rely on the UN lists before they are transposed into the EU legislation. Implementation of sanctions screening is inspected by supervisors in the course of their supervision, and fines have been issued for weaknesses in TFS implementation. (Refer to IO.4 for an elaboration on screening performed by reporting entities.)

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

274. Sweden has a large and diverse NPO sector, including over 148,000 individual NPOs. These can have a variety of different legal forms - with the most significant types being Non-profit associations, and Foundations. Different bodies are responsible for oversight of the different legal forms.

275. In 2008, Sweden reviewed its NPO sector, including a mapping of its size, activities, and an assessment of ML/TF risks, as well as the adequacy of laws and other relevant features. The risks posed by NPOs were also considered in Sweden's 2014 NRA on TF, which identified 'Fundraising for Beneficiaries Abroad' as a high risk area for TF. This assessment is borne-out by the TF cases noted above involving misdirection of donations to NPOs. A follow-up exercise is planned for 2016 which will focus on TF risks to the NPO sector.

276. Swedish authorities have conducted outreach to the NPO sector regarding TF risks, in particular through a multi-party forum organised by the Swedish Agency for Youth and Civil Society (MUCF). This forum was presented information on TF risks to the NPO sector based on Sweden's NRA and on FATF analysis during 2015, and continued to discuss TF issues at 2016 meetings. There has also been outreach to supervisory authorities for NPOs. Säpo has conducted meetings regarding

TF with several County Administrative Boards (CABs - the supervisory authorities for foundations) and presented at the CABs' AML/CFT conference, attended by foundation administrators. Säpo has also visited SIDA, MUCF, SIK and NPOs in order to raise awareness regarding TF risks.

277. Sweden's NPO sector is traditionally lightly regulated, with very little ongoing oversight of individual NPOs after their initial registration. Instead, Sweden relies primarily on self-regulatory initiatives to ensure the good governance of the NPO sector. The most significant mechanism is *Swedish Fundraising Control* (SIK), a non-profit organisation providing payment services to NPOs through direct debit accounts. This organisation has 423 members, including the largest NPOs which represent a majority of public fundraising in Sweden. The largest of these are also members of the *Fundraising Council for Volunteering Organisations* (FRII) (with 145 members, accounting for 75% of private fundraising through direct debits). Members of SIK are required to abide by a voluntary code, including internal controls, and to be audited and submit compliance reports, which are monitored by SIK and FRII. While these are focused on general good governance and the impact of NPOs activity, they also include measures to prevent misuse of funds.

278. NPOs also face oversight from government agencies if they act as delivery partners for government programmes. The Swedish International Development Agency (SIDA) makes use of NPOs to deliver development programmes using Swedish aid resources, and applies extensive oversight to any NPOs which receive SIDA funding. Within Sweden NPOs are frequently used as delivery partners for government assistance, and face oversight by the relevant government agencies. Notably, NPOs play a significant and active role in preventive work against terrorism and violent extremism. The Swedish Agency for Youth and Civil Society (MUCF) provides funding to civil society organisations for preventive initiatives to combat violent extremism, and to provide support for individuals who want to leave violent extremist movements. The National Coordinator against Violent Extremism (See **Box 13**, above) also plays an important role in preventing the misuse of NPOs, by encouraging awareness and oversight by municipalities of smaller, locally-active NPOs.

279. Based on the measures above, Sweden has good oversight of major fundraising NPOs, as well as major NPOs which are internationally active (in conjunction with SIDA) or which provide government-funded services. Nevertheless, there may be scope to further develop awareness and oversight of smaller NPOs at local and regional level - for example through continuing to apply the municipality-based approach developed by the National Coordinator against Violent Extremism.

Deprivation of TF assets and instrumentalities

280. Swedish authorities are not proactively using TFS to deprive terrorists and terrorist financiers of their assets. No persons linked to Sweden are currently subject to TFS, but some assets belonging to non-residents have been frozen in Sweden. As of June 2016, SEK 6 951 (EUR 746) was frozen under EU Regulation 753/2011 (under UNSCRs 1267/1989/1988), and SEK 21 025 (EUR 2 257) was frozen under EU Regulation 2580/2001 (EU TFS pursuant to UNSCR 1373) - a total of EUR 3 003.

281. As noted above, Sweden has exposure to terrorism and TF risks as a result of the 300 foreign terrorist fighters who have travelled from Sweden to Syria and of the 140 who have returned to

Sweden. It is not clear that effective steps have been taken to freeze the assets of those who remain in Syria, to prevent assets being transferred to them, or to prevent returned FTFs from providing financial support to terrorism.

Consistency of measures with overall TF risk profile

282. The use of targeted financial sanctions against terrorist financing in Sweden is not consistent with the risk profile. In particular, Sweden's most significant exposure to TF risks is through foreign terrorist fighters and returned fighters. However, Sweden has inadequate legal authorities and inadequate practical capacity to manage this risk using targeted financial sanctions.

Conclusion

283. Sweden has a solid and effective framework of measures to prevent the misuse of NPOs. While there is very limited formal oversight or supervision, this is complemented by strong self-regulatory initiatives and voluntary engagement with government agencies. Rigorous self-regulatory measures apply to NPOs which account for a significant portion of the financial resources under control of the sector, and additional oversight by SIDA applies to those which represent a substantial share of the sector's international activities.

284. Sweden's use of TFS as a tool to combat TF is limited. Sweden has no mechanism to use targeted financial sanctions in response to terrorist threats affecting Sweden. Sweden has never proposed a designation to the UN under resolution 1267[22], or to the EU under common position 2001/931/CFSP, and has no powers to make its own designations pursuant to resolution 1373.

285. Sweden also suffers serious weaknesses in its implementation of TFS applied by the EU or UN, because of technical deficiencies that are inherent within the framework of applicable EU regulations. These lead to excessive delays in the transposition of UN sanctions, and leave a gap in the applicability of EU sanctions to EU internal terrorists.

286. Although Sweden has a good understanding of the terrorist financing risks, it cannot and has not used TFS effectively to mitigate the risks, including those arising from foreign terrorist fighters and returned foreign terrorist fighters. This appears to weaken authorities' ability to prevent terrorist financing flows.

287. Sweden has achieved a moderate level of effectiveness for IO.10.

Immediate Outcome 11 (PF financial sanctions)

288. Sweden is exposed to risk of proliferation financing both as a regional financial centre and as an advanced manufacturing economy, which includes a number of high-technology industries and many companies which produce military or dual-use goods.

22 Although Sweden did co-sponsor such a designation in 2002.

289. Sweden has for many decades had a strong trading and business relationship with Iran and it continues to be an important export destination for Swedish companies. Sweden also has links to Iran through its relatively large Iranian diaspora community. Sweden has little or no trade with DPRK, and no North Korean residents. Sweden nevertheless hosts a DPRK Embassy, though this reflects Sweden's role in the Neutral Nations Supervisory Commission (established under the 1953 Korean Armistice agreement), rather than trade links.

Implementation of targeted financial sanctions related to proliferation financing without delay

290. An effective system of financial sanctions regarding proliferation depends on the immediate implementation of the UNSCRs, monitoring compliance with the measures imposed, co-ordinated action by the authorities concerned to prevent the measures being circumvented and preventive action. Sweden implements without delay (as required under FATF Recommendation 7) the targeted financial sanctions defined in the UNSCRs relating to combatting PF with regard to Iran but does not do so with regard to DPRK. The implementation of targeted financial sanctions for PF in Sweden is based on the European legal framework set out in Regulation 329/2007 (for UNSCR 1718 concerning the Democratic People's Republic of Korea – DPRK) and 267/2012 (for UNSCR 1737 concerning the Islamic Republic of Iran). These measures apply freezing measures to a broad range of funds and property.

291. With regard to Iran, these mechanisms do not suffer from technical problems in the length of time for transposition. Since Regulation 267/2012 was issued in March 2012, there were only two occasions where the UN added designations to the list (two entities and one individual on 19 April 2012, and two entities on 20 December 2012). The EU applies sanctions to a significant number of entities that are not designated by the UN, as they are designated associates of, or otherwise associated with, other UN and EU-designated individuals and entities linked to Iran. In both cases when new designations were made by the UN, these individuals and entities had already been listed in the EU framework (see Regulation 1245/2011 of 1 December 2011, and Regulation 54/2012 of 23 January 2012), and subsequently incorporated into Annex IX of Regulation 267/2012. Their designation by the UN had the effect - within the EU Regulation - of moving those persons and entities from Annex IX ("the EU Annex") to Annex VIII ("the UN Annex"). Delays in transposition have therefore not had any practical effect on either sanctions regime.

292. For DPRK, the UN added individuals and entities to the list four times between March 2012 and November 2015. Five (out of 14) of the entities had already been listed in the EU Framework. On three other occasions, the designations by the UN (of 22 January 2013, 7 March 2013, and 28 July 2014) took approximately 4 weeks, 6 weeks, and 10 weeks, respectively, to be incorporated into the EU framework. The most recent additions to the UN list of sanctioned persons and entities through UNSCR 2270 (2016) were transposed into the applicable decision by the Council of the European Union within two days of their designation by the UN. Despite recent improvements, there remains a problem with delays of up to several months in transposing new UN designations into EU Regulations.

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

293. Sweden has successfully identified funds or other assets belonging to designated persons and entities (and those acting on their behalf or at their direction) and prevented such persons and entities from operating or from executing financial transactions related to proliferation.

294. Freezing obligations under European regulations are applicable to all natural persons and all legal persons within the EU, and take effect immediately on publication of the regulations in the Official Journal of the EU. Freezing obligations apply to all types of funds, and the regulations prohibit making available, directly or indirectly, funds or economic resources for designated persons or entities, or for their benefit, unless authorised or notified in compliance with the relevant UN resolutions (Regulation 329/2007 Art. 6.4 and Regulation 267/2012 Art. 23.3). In October 2015, assets frozen pursuant to the EU sanctions against Iran (including under UNSCR1737 and its successor resolutions) were SEK 3 897 888; EUR 189 443, and IRR 13.6 billion (with an overall total value of EUR 997 000). As of June 2016 (following the unfreezing of assets consistent with the Joint Comprehensive Plan of Action (JCPOA) and UNSCR 2231 (2015)) the amount frozen was SEK 107 281; 189 443 EUR; and no frozen assets in IRR. No assets are frozen in Sweden under DPRK sanctions regimes.

295. Swedish export control authorities have a good understanding of the risks of proliferation and proliferation financing, including from diversion and sanctions evasion. They have been active in investigating and disrupting potential cases, and have good operational cooperation with other authorities. In addition to the implementation of targeted financial sanctions measures, Swedish authorities seek to proactively investigate cases of proliferation, proliferation financing, and sanctions evasion, and there appears to be effective communication between export-control authorities and financial crime authorities in this regard, and several cases have been initiated on the basis of an STR. Two cases described during the on-site involved the falsification of documents in relation to the export of controlled goods. An additional case involved the evasion of targeted financial sanctions.

Box 16. **Investigation and disruption of proliferation financing**

Attempted Smuggling of Vents (Lund Verdict)

A company in Lund (in southern Sweden), sold vents to an entity in Iran, in contravention of export control laws, using false documentation. This was detected as a result of an STR submitted by the bank handling the transaction. A subsequent investigation conducted by Customs, with assistance from Säpo, led to prosecution and conviction under the Act on Certain International Sanctions (1996:95), and the reporting of the incident to the UN Sanctions Committee.

Umeå case

A minor Swedish firm with a Swedish-Iranian owner in Umeå, northern Sweden, acted as a middle man for financing illegal procurement of sanctioned PDA products on behalf of Iran in a third country. An STR was submitted in December 2008 when the firm's bank noticed a sharp increase in the amounts of money handled. Säpo's subsequent investigation indicated that billions of SEK were

received from Iran and forwarded to entities in other countries. The investigation was pursued through cross-border cooperation, and although the Swedish firm could not be prosecuted for sanctions offences, the prosecution led to conviction for aggravated accounting offences, and disrupted the activity. The firm's owner was also subject to civil tax recovery.

FIs and DNFBPs' understanding of and compliance with obligations

296. Financial institutions appear to understand and comply with targeted financial sanctions relating to financing of proliferation with respect to screening against lists of sanctioned entities, though they have little awareness of the wider risks of sanctions evasion and do not take any steps to mitigate these. The FSA has taken some action to increase awareness, by arranging seminars in 2011 about targeted financial sanctions and proliferation financing, with participation from Säpo, the MFA and the ISP. Lists of designated persons and entities are communicated to financial institutions and DNFBPs through the publication on the EU site, and are included in the consolidated lists used for automated screening purposes. Swedish authorities do not provide separate notifications at national level. The FSA and financial institutions have confirmed that proliferation-related sanctions are included in the lists used for real-time and periodic screening. However, smaller FIs and DNFBPs did not seem to have an appropriate level of awareness of their obligations to implement PF-related sanctions through screening.

Competent authorities ensuring and monitoring compliance

297. Sweden's Financial Supervisory Authority (FSA) investigates as part of its regular supervision whether regulated entities have an adequate basis for compliance with the EU Regulations. Inspections generally include checks on compliance with the EU Sanctions Regulation, but do not address wider PF-issues (e.g., inspections of trade finance activities or methods of sanctions evasion). The FSA can draw on support from a specialised section within Säpo in case of suspected breaches. Breaches of TFS on proliferation can be prosecuted as criminal cases under the *Act on Certain International Sanctions.* The FSA monitors and ensures compliance by FIs with their obligations regarding proliferation related TFS. Competent authorities report that, in general, screening against sanctions lists is being implemented well by obliged entities.

298. Specific sanctions have been applied for breaches of PF-related TFS requirements. On April 2013, the FSA issued a remark and an order to impose an administrative fine of SEK 30 million (approximately EUR 3.1 million) for the reason that a bank did not have sufficient internal governance and control of the risk that funds or economic resources are being made available, directly or indirectly, to or for the benefit of the natural or legal persons, entities or bodies listed in the EU sanctions regulations through about 58 transactions. In May 2015, the FSA also issued a warning and an order of an administrative fine of SEK 50 million (approximately EUR 5.2 million) for similar reasons to a bank. Other supervisors appear to have limited awareness of sanctions obligations and the potential risks of sanctions evasion, and do not conduct specific outreach on this subject.

Conclusion

299. Sweden implements TFS regarding proliferation financing through EU measures. There are delays in the transposition of UN designations into EU sanctions lists - although the practical effect of these has been mitigated by the fact that EU lists are more extensive than UN lists, and by requirements for prior approval of transactions with Iran.

300. Financial institutions and DNFBPs routinely screen customers and transactions against EU and UN targeted financial sanctions lists, and supervisors review the application of such controls. However, smaller FIs and DNFBPs do not seem to have an appropriate level of awareness of their obligations.

301. Overall, persons and entities designated by the United Nations Security Council Resolutions (UNSCRs) on proliferation of weapons of mass destruction (WMD) are identified, deprived of resources, and prevented from raising, moving, and using funds or other assets for the financing of proliferation. TFS relating to proliferation are in a technical sense not implemented without delay, owing to the time taken to transpose UN designations into EU regulations. However, in the case of Iran, sanctions were implemented without delay as a result of the more extensive EU sanctions regime, and in the case of DPRK the risk posed by delays is largely mitigated by the negligible trade and financial links between Sweden and DPRK.

302. Overall, Sweden has achieved a substantial level of effectiveness for IO.11.

CHAPTER 5. PREVENTIVE MEASURES

Key Findings and Recommended Actions

Key Findings

- Financial institutions and DNFBPs generally comply with their AML/CFT obligations. Risk understanding among financial institutions and DNFBPs is varied: large entities are aware of their ML/TF risks, but smaller institutions do not seem to have the same understanding of ML/TF risks unless these are explicitly highlighted in the NRAs. Therefore not all FIs and DNFBPs have put in place risk-based measures to mitigate ML/TF risks.
- Large banks, especially those that encountered enforcement actions by the FSA, have made significant efforts to enhance their AML/CFT compliance and strengthen their compliance resources.
- Very few STRs are filed by most DNFBPs sectors, despite the ML/TF vulnerabilities identified (such as TCSPs, lawyers, and real estate agents). This may indicate low awareness of the risks and obligations.
- Financial institutions and DNFBPs generally conduct adequate CDD and monitoring of their customers. However, the measures taken with regard to beneficial ownership are not commensurate with the risks. Financial institutions and DNFBPs seem over-reliant on information held in company registers when identifying a beneficial owner and in verifying the identity of the beneficial owner and do not investigate whether there is a person in control. There is also insufficient awareness of the risks identified by Swedish authorities related to the regular use of straw men in criminal schemes.

Recommended Actions

- Even though there is a legal requirement for institutions to do a risk assessment, judging from the varying degree of risk awareness, FIs and DNFBPs (in particular the smaller entities) should focus more on the inherent risks in their assessment.
- FIs and DNFBPs should more proactively understand and mitigate the higher risk areas identified, such as the use of strawmen, the necessity to also identify if there is a person in control of a legal entity, and the use of new technologies.
- Authorities should provide the obliged entities with more granular guidance on implementing preventive measures, and typologies on possible ML/TF suspicious activities, to enhance FI and DNFBP understanding and mitigation of their risks, and to improve the quality and quantity of STRs.

303. 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)

Understanding of ML/TF risks and AML/CFT obligations

304. Awareness of AML/CFT obligations is generally well established among the FI and DNFBP sectors. Entities interviewed during the onsite knew about the AML/CFT Act under which they are required to conduct their own risk assessments, CDD and other preventive measures, and to file STRs. Nevertheless, their level of risk understanding is varied: large entities are aware of their ML/TF risks, while this is generally not the case for smaller institutions. The latter are not very aware of their ML/TF risks unless these are explicitly highlighted in the NRAs (see Chapter 2).

305. The assessment team found that most entities interviewed focus on cash as a large risk factor because it was highlighted in the NRA as a main risk and is generally considered a high-risk area among authorities. Most entities other than the big FIs had a low level of awareness of risks that were not associated with cash, whereas this is a valid issue considering the diminishing need for cash in Sweden. FIs and DNFBPs should have a higher focus on activities and transactions that are not cash-related.

306. On the whole, little additional attention is paid to identifying other ML/TF risks beyond those stated in the NRA, but there are differences between different entities. The larger banks seem to have frequent (informal) contact with the authorities accounting for a better understanding of possible risks and have identified several risks, such as risks regarding overseas operations given their large presence in the Baltic financial markets, as well as the risks posed by real estate transactions, cash intensive businesses, false IDs, and virtual currencies. On the other hand, smaller institutions have less interaction with authorities and as a consequence have demonstrated a lower understanding of the possible ML/TF risks that they face. In particular, FIs and DNFBPs do not seem to sufficiently use fraud and other criminal typologies to enrich their knowledge and assessment of ML/TF risks, for which the law enforcement authorities can do more to provide such information to them.

307. This is consistent with the findings in the FSA's document "A Better Risk Assessment" of April 2013, where the FSA concluded that there is a general need for greater awareness about risk, a deeper risk analysis, and more targeted measures. According to the report, many institutions appear to experience difficulties in identifying and assessing ML/TF risks in their own operations and applying control measures. Consequently, the institutions' risk assessments and procedures were found to be not always satisfactory. The FSA have, since the report was published, taken further actions to increase the risk awareness on specific topics, e.g., a report on tax crimes related to the use of currency exchangers and a report/seminar on TF risks.

308. Among the DNFBP sectors, the understanding of ML/TF risks is also varied. For example, the state-owned casino sector has a good awareness of their ML/TF risks and vulnerabilities. The real estate sector has identified risk factors specific to real estate transactions, such as when refunds of down payments are made to different accounts; the focus is on red flags that might indicate higher risk situations but does not encompass a broader understanding of the ML/TF risks faced by the real estate sector. Some of the other sectors did not appear to realise how their professions or business may be vulnerable to being misused by criminals to launder proceeds of crime.

309. All sectors indicate that they lack concrete information including from the FSA, Säpo, Fipo and other LEAs to develop a deeper understanding on their ML/TF risks. Although the FIs and DNFBPs generally were satisfied with the TF risk information that they were provided during a one-off Säpo/Fipo seminar in November 2015 on terrorist and TF threats and typologies, they requested to have up-to-date typologies shared on a more frequent basis in light of the relatively quick development of TF trends.

310. FIs and DNFBPs can benefit from proactive sharing of developments by authorities that may impact their own ML/FT risk assessments and promote wider awareness of ML/TF risks. For example, some (smaller) banks seemed unaware of the risks associated with the Central Bank's exercise to exchange all SEK banknotes to a newer version, which may indicate that information from the authorities is not reaching all relevant institutions.

Application of risk mitigating measures

311. Implementation is uneven: many FIs and DNFBPs have not put in place adequate measures to mitigate the specific ML/TF risks that Sweden is facing, e.g. with respect to tax crimes, fraud, organised crime, misuse of corporate structures, as described below. The limited understanding among some FIs and DNFBPs of specific ML/TF risks that Sweden is facing is an obstacle to effective risk mitigation. On an individual level, some entities have much better risk mitigation measures, but this is not consistent across all FIs and DNFBPs.

312. The larger banks and large MVTS providers are generally aware of their obligations and are also in frequent contact with the authorities. This is particularly the case for the large banks where the FSA has identified shortcomings and issued sanctions, where the banks have subsequently made significant efforts to enhance their compliance and risk mitigating measures. The level of risk understanding at these larger banks is stronger, and consequently they have also applied additional measures where necessary to mitigate those risks.

313. Smaller FIs and DNFBPs are aware of their obligations and will apply those in accordance with the law. But their knowledge of their ML/TF risks (beyond what is in the NRAs and other reports) is limited. Although some supervisory authorities have issued guidance to certain sectors and on specific risks, smaller FIs and DNFBPs receive limited additional guidance on risk from the authorities. The application of additional measures to address specific risks by these sectors is very limited.

314. FIs and DNFBPs generally conduct adequate CDD and monitoring of their customers. However, given the risks identified by Swedish authorities related to the use of straw men (where criminals use other people to execute financial transactions – see also Chapter 1) in criminal schemes, the measures taken with regard to identifying true ownership are not commensurate with the risks, mainly because there is insufficient awareness among many FIs and DNFBPs of the use of straw men.

Application of CDD and record keeping requirements

315. FIs and DNFBPs generally apply the CDD measures to identify and verify their customers, e.g., by using the electronic Bank ID for retail customers, and the social security number that all Swedish residents have. For customers that are Swedish companies, in addition to declarations from the client, they will rely on information contained in the SCRO register, although the register does not include information on shareholders which must be obtained from the company itself.

316. No institutions have issues with record keeping requirements, and all are aware of the fact that they should refuse or terminate the client relationship if the CDD process cannot be completed, but not all interviewed would systematically consider if it was suspicious for ML/TF and to file an STR.

317. According to the institutions, beneficial ownership is identified based mainly on legal ownership. Checking for control or decisive influence is complicated and there are no specific instructions on this for their staff. It is then dependant on the account manager's own level of comfort to detect if someone beside the legal owner(s) could have a decisive influence. As such, the determination of the beneficial owners is less accurate than it should be. This is substantiated by information from the police and prosecutorial authorities: in several ML investigations, beneficial ownership information was not available from FIs or DNFBPs, or their information was not accurate.

318. Some financial institutions and DNFBPs seem over-reliant on information held in company and other registers to identify the beneficial owner and verify the identity of the beneficial owner, and some seem not aware of the necessity, in light of the risks identified, to investigate further in order to determine whether there is a (different) controlling person of a legal entity. The authorities note that it could be due to a number of reasons, such as lack of understanding of the meaning of "control" in the definition of beneficial owner, insufficient appreciation of the risks, and weaker internal controls for identifying beneficial ownership.

319. Some banks also indicated issues with respect to the determination of beneficial ownership of accounts where client funds are managed by their lawyer, as the lawyer would not disclose the actual owner to the bank unless authorised by the client. According to the lawyers, this can occasionally happen if the lawyer's client did not pre-approve the provision of customer information to third parties, and the lawyer would subsequently have to seek approval from their client. The SBA confirmed that information about the beneficial owner of a client funds account in the name of the law firm falls within the professional secrecy and cannot be revealed without the consent of the client[23], and according to the AML/CFT Act[24], the beneficial owner of a client fund account (a client) needs not to be verified if the information can be made available at the request of the bank. The extent that this results in such accounts being opened without accurate identification of beneficial ownership, or FIs refusals to open such accounts, is not clear and should be jointly examined by the authorities and resolved as necessary (e.g. by specific guidance to lawyers and to banks on what is required to open such accounts).

---

23 Chap. 8, Sect. 4, Para 1 and Chap. 36, Sect. 5 Code of Judicial Procedure, as well as case law.

24 Chap. 2, sect. 5, para. 9

Application of other preventive measures

320. All institutions met were aware of the enhanced measures generally required for PEPs, and have systems in place to check for PEPs, and their family members and close associates. They were all aware of the recent fines in 2015 imposed on two of the largest banks in Sweden for non-compliance with AML/CFT requirements, including on PEPs, high risk customers, and correspondent banking relationships. Most PEPs that are identified are domestic PEPs and only a few are foreign PEPs. Larger FIs have higher exposure to PEPs given their size and international operations, and utilise commercial lists to screen for PEPs both at the on-boarding stage as well as periodically on existing customers. Smaller FIs and DNFBPs that do not have structured screening programmes are nevertheless aware of requirements and undertake enhanced measures.

321. Large banks have taken substantive steps to reassess their correspondent banking relationships for reasons such as mitigating ML/TF risk as well as to streamline costs of maintaining relationships. One bank indicated that their correspondent banking relationships were halved as a result of the remediation (from approx. 3,000 to 1,500). One bank had indicated that it had not previously realised the risks of correspondent banking relationships, while another bank has since developed 50 risk factors that it now uses to determine the risk of a correspondent institution.

322. Sweden's financial system is highly innovative technologically. Consequently, FIs both utilise new technologies, e.g. mobile real-time payments, and are aware of other developments and their ML/TF risks, e.g. virtual currencies. The larger FIs assess the risks of their new products and mitigate the ML/TF risks. This is however not yet consistent; for example, one FI that was interviewed was not aware of how prepaid cards can be misused for ML/TF. Awareness of developments in the area of new technologies and their ML/TF risks may be improved with a broader understanding of ML/TF typologies relating to new technologies, for instance conveyed through feedback/guidance from the FIU, LEAs, and/or the FSA.

323. All FIs and DNFBPs are aware of the requirements in relation to EU sanctions, and have measures or processes in place to comply. In practice, the major banks and MVTS providers check and rely on the UN lists before they are transposed into the EU legislation. This was confirmed by private sector representatives met during the on-site, who do this for reputational reasons and because they work with non-European countries. However, this practice is not necessarily followed consistently by smaller FIs or by DNFBPs who have no international business presence, and are unwilling to risk civil liability for taking freezing action in relation to a customer's funds/assets before having a firm legal basis upon which to do so. Implementation of sanctions screening is inspected by supervisors in the course of their AML/CFT supervision, and regulated entities have been fined for weaknesses in their implementation of TFS The robustness of the screening procedures can be improved, as one of the larger banks was found by the FSA to only screen very few SWIFT message types which left many parties unscreened. According to the bank, this has since been expanded exponentially (from 3 to 37 message types).

324. FIs are generally aware of the risks associated with customers or transactions related to high risk countries. They reference the FSA's website which publishes a link to FATF's public statements, which is supplemented by their own assessments of country risks.

5

Reporting obligations and tipping off

325. According to the FSA's December 2014 "Risk classification; money laundering and terrorist financing – the supervised entities' risk-mitigation measures", the FSA discussed with the FIU the usability of the STRs for the risk classification of entities. During this discussion, the FIU shared that several large financial institutions filed poor quality reports that were unusable by the FIU. However, the FIU has indicated that the quality of the STRs has improved over the past two years, particularly for those filed by larger institutions.

326. Most DNFBPs are filing very few STRs, despite the high vulnerabilities in some DNFBP sectors (such as TCSPs, lawyers, and real estate agents). This may be indicative of a low awareness of the risks they face. The supervisory authorities recognise this issue and have been trying to improve the level of reporting by focusing on suspicious activities and reporting requirements in their inspections. For example, the FMI is aware that real estate agents file a low number of STRs and suspects that this is not due to a lack of knowledge, but rather that the agents have high levels of expectations of a certain level of 'evidence' before deciding to file an STR.

327. However, with limited guidance on typologies, red flags and indicators, insufficient information shared from the FIU and LEAs, and limited or no interaction with the relevant supervisor, it will be difficult for reporting entities in general to effectively recognise suspicious transactions and enhance the number and quality of the STRs. Larger institutions that have (informal) contact with the FIU have been able to receive information that assists in their filing of STRs, and are generally satisfied with the level of information they receive. TF seminars and outreach organised by Säpo were found by attendees to be useful in developing typologies and transaction monitoring scenarios.

Table 19**. Number of STRs filed**

Reporting Institutions	2011	2012	2013	2014	2015
Banks or Credit Market Companies	7 727	6 099	6 223	5 074	5 700
Deposit Taking Operations	0	0	0	2	6
Consumer Credit Companies	-	-	-	0	6
Life Insurance Firms	74	33	13	29	42
Insurance Brokers	0	0	0	1	4
Securities Firms	20	5	9	1	7
Investment Fund Managers	2	3	0	1	3
Alternative Investment Funds	-	-	0	0	0
MVTSs	1 637	1 863	3 614	3 144	3 415
Electronic Money	-	-	11	92	148
Currency Exchanges	1 607	1 063	9,74	400	430
Other Financial Businesses	17	9	18	100	37
Financial Sector	***11 084***	***9 075***	***10 862***	***8 844***	***9 798***

Reporting Institutions	2011	2012	2013	2014	2015
Casinos	292	328	306	315	313
Estate Agents	8	5	2	0	3
Authorised/Approved Auditors	4	5	4	4	3
Other Accountants	3	3	4	6	10
Tax Advisers	0	0	0	0	0
Lawyers	0	5	3	4	4
Independent Legal Professionals	0	1	0	1	0
TCSPs	0	0	0	0	0
DPMS[25]	13	10	3	8	36
DNFBP Sectors	***320***	***357***	***322***	***338***	***369***

328. FIs and DNFBPs are aware that they should avoid tipping off. To prevent this, reporting entities in Sweden generally take the approach of centralising STR reporting, where the account manager that identified the transaction is not aware that an STR has been filed, and does not have access to records of STRs filed. Smaller entities that do not have centralised STR reporting functions nevertheless recognise that tipping-off is an offence.

Internal controls and legal/regulatory requirements impeding implementation

329. FIs and DNFBPs interviewed had internal controls and procedures for AML/CFT compliance. The levels of controls were found to be satisfactory taking in to account their differences in size, risk level, and scope of operations. FIs with an international presence implement policies and procedures at the group level. One of the banks that were fined by the FSA had subsequently enhanced its global approach to AML/CFT for its large overseas operations in the region, and elsewhere in the world.

330. Some banks highlighted data protection issues with regard to storing lists that did not concern their own customers. According to these banks, this causes problems with, for instance, using the list of names from the "Panama Papers" as a risk indicator, and also with screening the non-customer party of a SWIFT MT-700 message (used for letters of credit). Data protection was also highlighted as an impediment to FIs sharing information between themselves on potentially suspicious ML or TF activities by their customers, which could otherwise lead to better detection and filing of STRs.

25 DPMS are regulated under the category of high value dealers in Sweden. The number of STRs reflected here is for the whole category of high value dealers.

Conclusions

331. The level of risk understanding and compliance with AML/CFT preventive measures in the FI sectors is generally more advanced than among the DNFBPs. Among them, large entities are aware of their ML/TF risks, while smaller institutions mainly rely on those highlighted in the NRAs. Overall, there are insufficient mitigating measures in place relative to the risks of beneficial ownership and an overreliance on company registers. Additionally, given the regular use of straw men in criminal schemes as identified by the authorities, there is a lack of awareness on the risks of hiding true ownership. The level of STR reporting in some sectors is also very low.

332. **Sweden has achieved a moderate level of effectiveness for IO.4**.

CHAPTER 6. SUPERVISION

Key Findings and Recommended Actions

Key Findings

- The Swedish supervisory system covers all obliged entities and all of the fundamental elements of an AML/CFT supervisory system are in place. However not all the supervisory authorities supervise the sectors fully in line with the risks.
- Supervisors' understanding of ML/TF risks use the 2013–14 NRAs as a starting point, which do not provide a comprehensive picture and analysis of Sweden's risks. The FSA has made efforts to understand the TF risks by commissioning additional research and is updating its knowledge of risk from external sources, such as the media and international fora. The FSA and the other supervisors, however, receive limited risk information from other authorities to improve their efforts. Most of the other supervisors have not assessed any additional ML/TF risks that may occur in their sectors.
- The FSA has issued fines and warnings, and revoked licences, for AML/CFT non-compliance at some of their largest banks (of the 79 onsite inspections, 18 led to sanctions decisions). The public nature of the sanctions has had an effect on the level of compliance in the sector as was confirmed by some of the FIs interviewed.
- Among some of the other supervisors, the current methods of assessing the ML/TF risks of their supervised entities are basic and do not allow for effective risk-based supervision. The priority given to AML/CFT supervision has been uneven across DNFBP sectors, and focused AML/CFT supervision is not conducted on a regular or sustained basis. Only a few DNFBP supervisors, such as the CABs, use a more risk-based model. DNFBP supervisors have imposed sanctions to varying degrees, most of which are at a much lower extent than the FSA.
- While all supervisors have issued AML/CFT regulations and some authorities have issued additional guidance, the level of understanding of AML/CFT obligations by some of the private sector is not consistent and some of the guidance provided does not give sufficient detail

Recommended Actions

- Sweden needs to increase the resources of the FSA's AML unit in order for it to undertake appropriate onsite and offsite supervisory actions commensurate with the risk and size of Sweden's financial sector.
- Improve supervisors' understanding of risks in their specific sector(s), supported by better inter-agency communication between law enforcement and supervisors, and use this understanding to take a more tailored risk-based approach towards supervising the reporting entities.
- More substantial, structured guidance on risks and AML/CFT requirements is necessary, including through inter-agency engagements with the private sector to collect input and respond to questions.

- CABs need to keep improving their assessments of the risks of the wide range of sectors under their charge, in particular those less known sectors (such as TSPs) and then focus their supervisory resources as appropriate.
- Supervision of the DNFBP sections (e.g. lawyers, CSPs, and real estate agents) should be increased to match the vulnerabilities identified in the NRAs.

333. 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.26–28 & R.34–35.

Immediate Outcome 3 (Supervision)

Licensing, registration and controls preventing criminals and associates from entering the market

334. All supervisors except the SBA check by means of criminal records to assure that criminals and their associates do not own or hold a significant function in an institution. Out of the three relevant supervisors (the FSA, the CABs and RN), only the FSA checks if the funds that are used to acquire an institution or a significant interest in an institution are from a legitimate source. However, with respect to "*financial institutions*"[26] and deposit companies the FSA cannot request criminal records. The legislation does not provide for that possibility.

335. The FSA has a general licensing process where fit and proper tests are carried out both at the time of the licensing and throughout the licence period. Application assessment can differ depending on the FSA unit that is in charge of the licence (e.g. banking, insurance, investment funds, securities, consumer conduct) and the law applicable to the specific licence. During the licensing process, the FSA will assess several documents, such as the applicant's policies and procedures, and meet the applicant's owners and/or senior management in person (where the FSA's AML Unit may join). Based on the assessment of documents, the meeting and, if necessary, an onsite inspection, the FSA decides if the application is approved.

336. To assess the suitability of owners and senior management, the FSA will collect tax information, police records regarding financial and tax crimes, and seek information from foreign supervisors. In assessing the police records, if the person under assessment has committed a crime, the FSA will take into account the time passed since the crime, the seriousness of, and the type of crime. The FSA states that they will in general reject an application when there is a criminal record.

26 "Financial institution" is a specific class of licence in Sweden for the business of currency exchange, or other financial operations (such as the granting of loans, financial leases, guarantees or letters of credit, or providing financial advice, means of payment or currency trading services)

337. The FSA rarely formally reject applications. Instead, the FSA has observed that applicants usually either take steps to comply, or withdraw their applications when the FSA requires additional information or corrections in their communication with applicants. During 2010–2015, there have been a number of assessments that have led to rejection or retraction of applications.

- Investment funds: in total six rejections, and between 5–15 retractions annually.
- Securities: one rejection, 3–8 retractions per year.
- Banking: no rejections, 3–5 retractions per year.
- Insurance: no rejections during 2014–2015, one retraction average per year.
- Consumer Conduct Unit (MVTS): 9 rejections, and for the period of 2012–2015, 7 cases of lack of suitability or previous convictions (e.g. for economic crime) of managers, board directors, or owners.

338. To detect entities that operate without a license or registration, the FSA receives information from other authorities, such as the SCRO, the Police Authority, Säpo and the STA, whereby the FSA will then conduct its own investigations and take action if necessary.

339. For real estate agents, the FMI requests a transcript from the criminal records register from the Police Authority and checks if the applicant has any prior convictions, as well as ensuring that the applicant does not have any significant debt in the Swedish Enforcement Authority's (KFM) register. Property crime, economic crime and violent crime are among those offences that are primarily considered. All registered real estate agents are re-assessed every 5 years. There have been 3 cases in the last 5 years where an agent's registration has been revoked as a result of not being "fit and proper".

340. When assessing applications for auditors/audit firms, the RN collects information about the applicants from the STA and the criminal records register of the Police Authority. On average, there are 350 applications per year of which most are approved. Re-assessments are conducted every 5 years.

341. Entities under supervision of the County Administrative Boards (CAB) – i.e. independent legal professionals, accounting and tax professionals, TCSPs and DPMS – have no licensing requirements. Instead, they are required to be registered with the SCRO, whereupon the CABs perform fit and proper tests of all newly registered entities. This includes whether an obliged entity or the Board of Directors have failed significantly to meet their obligations with regard to their professional duties or committed any serious crimes. Re-assessments are performed on a yearly basis in addition to this. The CABs will take action to compel a legal person to replace disqualified persons in managerial positions. The review of directors is conducted using information from the Police Authority, STA, SCRO and KFM. Because of the absence of a shareholder register, the CABs have to individually request such information from its registered entities. 5,000 companies were assessed in 2013 and 2014, and 10,500 in 2015.

342. The number (over 10,000 have registered) and range of entities under its remit constitutes a constant challenge for the CABs to know how many entities are obliged to register with it, as well as in monitoring and interacting with them. The CABs cooperate with the STA to identify unregistered

entities that fall within their remit, e.g. through the use of SNI codes[27]. The CABs have authority to take action to compel obliged entities to register with them or cease the relevant operations.

343. There are TCSPs active in Sweden, not all of which have registered with the SCRO's AML register. The authorities have undertaken steps to identify unregistered company service providers, and continue to do so. As for trust service providers, the authorities do not previously seem to have had much knowledge of the sector, and consequently there is more to be done to identify and compel TSPs' AML/CFT registration.

344. AB Svenska Spel, and its wholly owned subsidiary Casino Cosmopol, are fully owned by the state and have a monopoly to provide casino games. The process of finding and assigning suitable members of the Board includes thorough background checks, checks of criminal records and credit reports. The Ministry of Enterprise and Innovation is responsible for appointing the Board of Svenska Spel. In addition, there are fit and proper checks, including a check of criminal records, for the Board of Casino Cosmopol, which in turn is appointed by Svenska Spel.

345. For lawyers, the Swedish Bar Association (SBA) will request character references with respect to the suitability of applicants from existing lawyers. Applicants without the necessary support will not be admitted to the Bar. Information on criminal records is not available to them but the SBA will receive information from courts if an advocate or associate lawyer is convicted of a criminal offence.

Supervisors' understanding and identification of ML/TF risks

346. The supervisors' understanding of ML/TF risks is based mainly on the 2013–14 NRAs, more recently supplemented by the 2015 ML NRA. These do not in isolation provide a comprehensive and current picture and analysis of the relevant risks. While some supervisors such as the FSA have a more developed understanding of the risks in their sectors, other supervisors seem to rely on the NRAs, e.g. focusing on cash, as it was highlighted as high risk in the NRA. The CABs also use various reports and obtain information through the work against organised crime (the GOB cooperation, through the Regional Intelligence Centres) to enhance their understanding of the risks.

347. The FSA is largely aware of the risks in Sweden using the NRAs as a starting point. Additional work on risk analysis and typologies has been carried out (for instance with EBM) in order to improve the understanding of the ML risks. Supervision has consequently been increased with regard to MVTS and exchange houses. The FSA has enhanced its understanding of TF risks by commissioning a study on international TF risks and methods by the Centre for Asymmetric Threat Studies (CATS) at the Swedish Defence University. The FSA also performs media coverage analysis and follows international developments and reports to determine if there are new risks, e.g. the Panama Papers. The FSA receives limited risk information from other authorities on prospective risks in the financial sector, as a result of insufficient structures for information sharing between

[27] The company register of Statistics Sweden (SCB) contains companies, authorities, organisations and their respective locations in Sweden and is organised according to SNI codes. SNI is the Swedish standard for classifying industries (see www.scb.se/en_/Documentation/Classifications-and-standards/Swedish-Standard-Industrial-Classification-SNI/).

authorities and weaknesses in Fipo's strategic analysis. This weakens the FSA's ability to anticipate and understand new and emerging risks.

348. The method used by the FSA to assess and categorise the ML/TF risks of individual financial institutions for supervision purposes is basic and does not address important inherent risks within the financial sector. The assessment focuses on the entities' size, cash and cross-border transactions, and the number of STRs filed and does not otherwise reflect the degree of risk inherent in the FI's activities or customer base. The FSA is currently developing a new model to assess the risk of institutions.[28] For this, a database based on a number of questions (e.g., number of PEPs, customers in tax havens, effectiveness of implemented monitoring scenarios) and an analytical tool are in development. As guidance and support in choosing what information to include in the periodic reporting, the FSA sent a questionnaire to 58 financial institutions in May 2016. The periodic reporting and the new risk classification tool will start functioning during 2017 when there are new regulations.

349. Supervisors such as the Swedish Estate Agents Inspectorate (FMI), the Supervisory Board of Public Accountants (RN) and the Swedish Bar Association (SBA) do not have a risk assessment method to assess the ML/TF risk of their supervised entities, Their understanding of ML/TF risks is mainly based on the NRAs, which for example identify the real estate industry as a sector where potentially large scale ML may occur, taken in context of their sectors, e.g. RN is aware that the risks of cash are less relevant for accountants. The SBA sees the main ML risks of lawyers' activities to be lawyer-managed client accounts, real estate transactions, and company formations, and have identified vulnerabilities and red flag indicators based on international guidance documents, as well as their own assessment and assessment of law firms.

350. The County Administrative Boards (CABs) have developed in 2015 a risk classification model whereby three different risk categories are analysed based on responses to a questionnaire: operational risk (products, services, customers, distribution channels), system risk (size of the company, external control by an auditor), and AML/CFT measures adopted. All entities are classified individually. The CABs are in the process of applying this system in their supervisory programme. The participation in the Regional Intelligence Centres helps the three CABs to identify high-risk entities to be supervised as well as obtaining information about modus operandi and current trends of organised crime. The greatest ML/TF risks the CABs have identified are associated with cash retail, consultancies, post box companies, "office hotels" and foreign branch offices. However, the authorities' understanding of TSPs and their risks needs to be developed.

351. The Swedish Gambling Authority (LI) has good awareness of the possible ML risks that can affect the sector as a whole, e.g. cash handling, and currency exchange, as well as risks that are specific to the Swedish context. LI has assessed the risks of 'restaurant casinos' (approx. 40 licenses with 400 locations) to be low in light of the restrictions on the very small size of stakes allowed and the prescribed odds.

[28] According to the FSA, the new model to assess the risk of institutions will for example also include mitigating actions, inherent risk, external risk factors and information from LEAs.

352. LI is also aware of the many television advertisements in Sweden for online casinos. However, according to LI, these online casinos are licensed overseas under EU regulations, such as in Malta, and broadcast from outside Sweden. LI commented that they are therefore not able to halt these advertisements for these foreign online casinos, and Swedish authorities have not been able to prevent these entities from doing business with Swedish residents.

Risk-based supervision of compliance with AML/CTF requirements

353. The Swedish supervisory authorities' efforts in conducting AML/CFT supervision have been uneven over the years. Risk-based approaches to AML/CFT supervision is not practised by most supervisors (other than the FSA and CABs), as set out below; while some have only recently developed it or are in the process of improving basic systems. The priority given to and the intensity of AML/CFT supervision are also uneven among sectors, and do not fully match the risk areas identified in the NRAs (e.g., there seems to be an insufficient focus on straw men among some supervisors).

Financial Sector

354. The FSA has a risk-based approach to AML/CFT supervision but its risk classification tools are weak, and its AML Unit is under-resourced, with only 8 specialised AML/CFT staff for more than 2,000 entities with very different risk profiles. The FSA has therefore focused on the large banks, the main MVTS providers, and some exchange houses. There have been 79 AML/CFT onsite inspections since 2010, out of more than 2,000 entities. Additionally two offsite surveys have been sent: one in 2011 to 373 entities and another in May 2016 to 58 entities. The FSA also performed approximately 300–350 fit and proper investigations per year for entities already licenced. AML/CFT related issues can also be a topic for the regular meetings between representatives on different organisational levels from the FSA and the obliged entities. This is insufficient for a financial sector the size and risk of Sweden's. Although it is understandable that the FSA focuses on the larger FIs (which cover a large share of the total assets held by banks) in a risk-based approach one would expect that more FIs to be subject to some form of (either onsite or offsite, or both) supervision over the past years.

Table 20. **Number of FSA Onsite Inspections (2010 – mid 2016)**

	Year decision taken or ongoing examinations							
	2010	**2011**	**2012**	**2013**	**2014**	**2015**	**2016 (mid)**	**Total**
Bank	1	5	2	1	2	2	4	**17**
Foreign branch of Swedish bank								
Swedish Branch of foreign bank		1	1					**2**
Fund company			1					**1**
Investment firm		6						**6**
Insurance broker								

	Year decision taken or ongoing examinations							
Life insurance company				2				**2**
Financial Institution		1	2	10	6	13	4	**33**
Registered payment provider	s		1	4			1	**6**
Credit market company			3	1	1			**5**
E-money issuer				2				**2**
Payment institution						1		**1**
Foreign payment institution							1	**1**
Total per year	**1**	**13**	**10**	**20**	**9**	**16**	**10**	**79**

355. FSA inspections are planned annually, where the sectors, themes and institutions to be inspected for the next year are analysed. Room for ad hoc or event-driven inspections is also made in the annual plan of supervisory activities (e.g. the Panama Papers investigation in 2016). The current risk classification tool that provides the basis for determining the priorities is based on four parameters: (1) turnover, (2) whether the institution handles cash and (3) cross-border transactions, and (4) number of STRs filed. Other information is also used for the prioritisation of supervisory activities, such as information and reports from other authorities, media, court cases, new trends and risks, STR information, information from other units at the FSA, tips from the public and indicators the FSA receives from the financial sector. The tool is basic and does not take into account relevant risk factors such as the institution's customers, products and services, geographical exposure, control weaknesses, etc. The FSA then extensively prepares for the inspections, and through that process decides on what areas to examine (e.g. PEPs, private banking, offshore risks, TF risks, corruption risk, governance, international presence) for the inspected institution. The authorities conveyed that the current risk classification tool is going to be replaced during 2017 by a more dynamic and extensive tool based on periodic reporting from the FIs, including questions on mitigating measures, which should allow the FSA to take a better risk-based approach towards the supervision of its institutions.

356. The FSA has also conducted ad hoc inspections when there is an event/incident. Such an examination can be initiated because of information received from another authority, e.g. Fipo, EBM, Säpo (see IO.1 on domestic cooperation and coordination), media reports, or information from a foreign supervisor (usually other Nordic supervisors). Inspections generally include checks on compliance with the EU Sanctions Regulations, but do not address PF issues (e.g., inspections of trade finance activities or methods of sanctions evasion).

357. The whole inspection takes a fairly long period of time[29] partly because of an extensive internal preparation and decision-making process. For instance, the inspections of the 4 large banks

29 The FSA has advised that (after the onsite visit – hence not included in this assessment), they have since enhanced their on-site investigations process and have applied it to four savings banks between September to November 2016, where the FSA could sum up their findings in weeks after the visits, instead of months as before.

started at the end of 2013, with the onsites in autumn 2014, and the enforcement decision taken in May 2015. The inspections of 4 exchange houses started in the autumn of 2015; the conclusions were sent to 1 of them during Q2 2016, whereas the process for the remaining 3 institutions had not yet concluded at the time of the onsite visit.

358. Although the knowledge and expertise of the 8 staff members in the FSA's AML Unit is adequate, this unit does not have sufficient resources to conduct adequate risk-based AML/CFT supervision on 2,000 entities. At the time of the onsite visit the unit was busy with the follow-up examinations of the 2015 decisions regarding the four large banks, performing activities as a result of the "Panama papers" case, working on the inspections of one large MVTS (including 9 of its agents) and 4 exchange houses, cooperating with one other (Nordic) supervisor on the inspection of a Swedish branch of a foreign bank, sending a questionnaire to 57 savings banks and starting up the inspection of 4 savings banks. In addition, the AML Unit is in charge of developing regulations and working on EBA guidance and FATF issues. This means that the unit is overextended and doing its utmost with the limited resources.

DNFBP sectors

359. The Swedish Estate Agents Inspectorate (FMI) integrates AML/CFT supervision into its regular supervision. These inspections normally start from a complaint received or if there are issues with respect to the registration. There is no specific AML/CFT risk-based approach to its supervision. In 2015, the FMI performed AML/CFT inspections of 32 real estate agents that were selected based on their location, i.e. in five larger cities. In several cases, it was established that the real estate agents did not have sufficient measures in place to meet the requirements of the AML/CFT legislation.

360. The Supervisory Board of Public Accountants (RN) typically starts an investigation based on complaints received, information in the news, or international requirements. In its regular supervision (such as inspections and systemic supervision), RN prioritises so-called public interest entities (e.g. listed companies and financial institutions) and accountants that have a high number of assignments or have had previous disciplinary measures. While this has elements of a risk-based approach, it is not specific in relation to AML/CFT. According to RN, mandatory inspections regarding the international standards for public accountants are conducted every 3 years, and include AML/CFT issues.

361. The County Administrative Boards (CABs) have a large and highly diverse range of entities under their remit – independent legal professionals, accounting and tax professionals, TCSPs and DPMS. The CABs previously conducted inspections based on the size of the entities or of the sectors (e.g. bookkeeping and accountancy consultants sectors, which in some instances could have included ML/TF risks). This was, however, not adequately tailored to the ML/TF risks of the various sectors and entities. This improved in 2015 when they developed a model on the risks inherent in the majority of supervised entities based on data collected, which has allowed the CABs to start a risk classification system and a corresponding risk-based supervision system. However, this new system has not had the time to translate into supervisory results. Presently, the numbers of AML/CFT onsite inspections by the CABs are very low compared to the high number of entities under their remit

(estimated over 30,000 whereof 10,000 are registered with the SCRO). In addition to the onsite inspections, there have also been some offsite inspections (2012 – 89; 2013 – 216; 2014 – 321; 2015 – 84).

Table 21. **Onsite Inspections by CABs (2012–November 2015)**

Category	2012	2013	2014	2015
High value dealers	7	15	5	23
Accountants	8	27	35	9
Tax advisers	0	3	5	1
Company Service Providers	0	7	12	3
Independent legal professionals	0	1	2	1
Total	**15**	**53**	**59**	**37**

362. Since Casino Cosmopol has only four subsidiaries, the Swedish Gambling Authority (LI) does not have to take a risk-based approach to prioritise its inspections. LI has meetings with the management at each casino as well as with the central management for all four casinos once a year where AML/CFT issues are discussed. Supervision is performed by a combination of onsite visits and desk-based controls. Within the inspections, LI takes a risk-based approach to focus the scope of the inspection, for instance by focusing on the quality of the risk assessments or the quality of the STRs. LI monitors the developments and events that take place at Casino Cosmopol by means of a database where deviating events are registered. The casinos submit reports to LI on a monthly basis, which inter alia contain information about the number of STRs submitted to Fipo. LI visits the casinos anonymously about 40 times per year. Those visits include checks of AML/CFT procedures.

363. The Swedish Bar Association (SBA) does not undertake AML/CFT supervision on the basis of ML/TF risks of its entities. In 2009, the SBA conducted an investigation with regard to compliance with the AML/CFT Act of the 35 largest law firms where it in some cases found instances of internal regulations or procedures that could be improved marginally. The examinations by the Bar related mainly to collecting information in writing, while some physical inspections of law firms also occurred. In 2016, the SBA began an inspection program including AML/CFT obligations. The SBA plans to have inspected 100 law firms with approximately 3,800 lawyers by the end of 2016.

Remedial actions and effective, proportionate, and dissuasive sanctions

364. All supervisory authorities have adequate enforcement powers ranging from warnings to revoking licences or injunctions to cease business, and sometimes monetary fines available. The FSA has for example revoked licences, used the highest monetary fine available at the time in one case, as well as lower levels of sanctions in other cases. Although in that instance the maximum fine was low relative to the size of the bank, Sweden has since changed its laws in August 2014 to increase the maximum fine from an absolute figure to a maximum of ten percent of turnover. Except for the FMI, most of the other DNFBP supervisors have been less willing to impose sanctions for AML/CFT non-

compliance, or lack a sufficiently graduated range of applicable sanctions to be proportionate and dissuasive. Several supervisors have published the enforcement measures taken.

365. The FSA has issued fines and warnings for AML/CFT non-compliance at some of their largest banks. In the period 2010–2015, the FSA issued 18 sanctions: 3 banks, 9 financial institutions, 1 credit market company, 1 registered payment service provider, 2 fund companies and 2 insurance brokers. The licences of 1 large entity and several small ones were also revoked. The FSA has used a wide range of sanctions, such as injunctions, warnings, revoking of licenses, and fines.

366. In the FSA's 2015 comprehensive AML/CFT inspection of all four major Swedish banks, one bank was given a "warning" and the then-maximum fine of SEK 50 million (approximately EUR 5.2 million), while another received a "remark" and a fine of SEK 35 million (approximately EUR 3.7 million). In the former case, the FSA indicated in the decision to revoke the bank's license was an option given the severity of the breaches, but was not taken as the bank had already commenced on an extensive action plan to address its deficiencies. The FSA noted that the decision was made under the old regulations and under current regulations, the level of fines would likely be higher (up to 10 percent of turnover – in that instance possibly up to SEK 5.6 billion, approximately EUR 586 million).

367. In another case from 2014, the FSA revoked the license of a large credit market company that had a strong position on the currency exchange and cash management market for consumers with 25 offices across the country. Enforcement decisions are published by the FSA on their website, which the FSA believes, and confirmed by some of the FIs interviewed, to increase awareness and compliance of other actors on the financial market.

Box 17. **FSA sanctions on major banks**

Nordea Bank AB (2013, EU sanctions, enhanced CDD)

The FSA issued Nordea a "remark"[1] and a fine of SEK 30 million (approximately EUR 3.1 million) in 2013 upon finding a lack of controls for compliance with EU sanctions regulations, failure to immediately notify the FSA about 58 freezing measures taken in accordance with EU sanctions, as well as weaknesses in its AML/CFT measures. **The investigation began in 2012, and was initiated as similar deficiencies were found by the FSA in a 20**09 investigation.

Nordea Bank AB (2015, major AML/CFT deficiencies)

The FSA issued Nordea a "warning" and the maximum fine at that time of SEK 50 million (approximately EUR 5.2 million) in 2015 as it found large, systematic deficiencies in AML/CFT controls throughout all of the inspected business areas (foreign PEPs, correspondent banking relationships, private banking customers, and customers that are legal persons with a tax domicile outside the Nordic countries). The deficiencies were related to central pillars of the AML/CFT framework such as the risk assessment of customers, customer due diligence measures, and transaction monitoring.

The severity of the breaches was assessed to be sufficient to justify a revocation of the bank's licence, but it was determined that a "warning" was sufficient in light of the significant actions that the bank

had taken and was taking to correct the deficiencies. The investigations began in 2013 and the sanction was decided in 2015.

Svenska Handelsbanken AB (2015, AML/CFT deficiencies)

The FSA issued Handelsbanken a "remark" and a fine of SEK 35 million (approximately EUR 3.7 million) in 2015 as the bank was found to have extensive and systematic AML/CFT deficiencies, during the FSA's investigation of the four major banks from 2013–2015 (including the above Nordea case).

The two other major banks were also subject to inspections. They were not sanctioned but have nevertheless been subject to additional supervisory action as a consequence of the results of the investigations.

Note:
1. A "remark" is of a lower level than a "warning".

368. In 2015, the Swedish Estate Agents Inspectorate (FMI) carried out a thematic AML/CFT inspection, where out of the 32 inspected real estate agents, 12 agents were sanctioned, consisting of 7 warnings and 5 reminders. AML/CFT issues also figured in several other cases: between 2007–2015. The Disciplinary Board of the FMI decided on 206 supervisory cases where AML/CFT issues were also involved; these led to 155 warnings and 14 reminders. According to the FMI, agents risk losing their authorisation if they repeat the mistake and none of the agents warned for AML/CFT failings have repeated the failures.

369. Since 2010, the Supervisory Board of Public Accountants (RN) has had 6 disciplinary cases regarding AML/CFT: 2 included failures with respect to filing unusual transactions and 4 included CDD deficiencies. In three cases, RN withdrew the accountants' authorisation, while the other cases received "warnings".

370. The County Administrative Boards (CABs) take measures and sanctions (such as compelling or notifying companies to rectify issues, and conditional fines). Although the CABs have taken approximately 45 enforcement decisions since 2010, these are only to a limited extent related to non-compliance with AML/CFT requirements. According to the CABs, this can be explained because only since August 2015 has legislation been in place that enables the CABs to take measures and impose sanctions related to non-compliance with AML/CFT requirements.

371. In the casino sector, sanctions consist of "notifications" or fine-enforced injunctions. The Swedish Gambling Authority (LI) aims to encourage entities to rectify issues voluntarily. On one occasion, LI issued an injunction with a conditional fine based on deficiencies in the context of registering and checking the identity of visitors.

372. The Swedish Bar Association (SBA) issues warnings, reprimands, or fines or disbars lawyers. With respect to AML issues, two lawyers were disbarred in 2003. Since then, there have been no further enforcement measures for AML/CFT against lawyers.

Impact of supervisory actions on compliance

373. The supervisory authorities for the most part have done few inspections, and it is difficult to draw firm conclusions on the impact of supervisory actions. The level of inspections could contribute to the low levels of STR filing in some sectors. Nevertheless, most supervisory authorities have in their activities identified lack in control measures at reporting entities over the years and have taken actions to improve their compliance, including by publishing the results of enforcement actions.

374. The FSA has a good understanding of how to perform AML/CFT inspections and what is required of financial institutions, and in spite of the low number of staff in the AML Unit and the low level of additional guidance provided to the sectors and institutions, the FSA's activities, especially the enforcement actions on the largest banks, have had an impact given the range and number of financial institutions under its charge.

375. The FSA has been following up with the four large banks on reforms and remediation measures being undertaken to address problems identified in the two enforcement decisions taken in 2015 (see **Box 17**. above). Through these follow-ups, which consisted of three on-site visits at each two of the sanctioned banks and quarterly supervisory meetings with the other two banks, the FSA concludes that their supervisory actions have had significant effect on AML/CFT compliance of the banking sector. This is the case in particular for the two sanctioned banks where there have been follow-up inspections on specific parts of the remedial efforts, but also for other banks in Sweden. The FSA shared that because of the publication of the enforcement decisions, other banks are strengthening their AML/CFT procedures through, for instance, expanding their compliance department resources, higher levels of CDD checks and more effective monitoring systems.

376. The Swedish Estate Agents Inspectorate (FMI) publishes the results of its disciplinary measures on FMI's website in anonymized form, and through monthly e-mail newsletters to estate agents. According to the FMI, this contributes to the level of awareness of awareness of AML/CFT legislation among real estate agents.

377. Besides the questionnaire to assess the risks of the entities under the County Administrative Boards' (CABs) remit, the CABs have not been able to reach a large majority of the entities with inspections or enforcement actions as the relevant legislation only entered into force in August 2015. As such, their effect on compliance by their supervised entities could not be assessed.

378. The Swedish Gambling Authority (LI) has a close supervisory relationship with the state-owned Casino Cosmopol, and have found that their supervisory findings are adequately addressed by the casino.

379. The Swedish Bar Association (SBA) and Supervisory Board of Public Accountants (RN) believe that their actions have had an effect on the level of compliance in the sector. The assessment team however finds it difficult to verify the effects of their supervisory actions in their sectors given the number of inspections and enforcement actions have been very low.

Promoting a clear understanding of AML/CFT obligations and ML/TF risks

380. All supervisors have issued AML/CFT regulations and some authorities (FSA, CABs, SBA, FMI) have issued additional guidance. However, the level of understanding of AML/CFT obligations by the private sector is not consistent, which may be due to some of the guidance provided not giving sufficient detail.

381. The FSA provides information to financial institutions for instance during seminars and meetings, and in answer to specific question from institutions. The guidance provided is high level and does not include application of AML/CFT requirements in depth, such as enhanced due diligence – in part because the FSA does not have sufficiently granular information from law enforcement or Fipo to provide more detailed advice. The FSA's meetings and seminars with relevant associations, for instance the one-off TF seminar to present the 2015 follow-up to the TF NRA, are generally well received by the sectors.

382. Publications by the FSA aimed at the private sector have had differing levels of detail. For example, the FSA sent in March 2016 a brochure to exchange houses providing an overview of the basic CDD requirements including a list of possible indicators of suspicious transactions. However, the FSA's April 2013 guidance "A Better Risk Assessment" describes the ML/FT risk assessment and AML/CFT requirements at a very high level without any examples of good or bad practices, which is not sufficiently helpful for financial institutions to understand their obligations.

383. The Swedish Estate Agents Inspectorate (FMI) has issued guidance for real estate agents with information on the legal AML/CFT requirements and provides high risk scenarios and cases. Further information is provided through its newsletters and website, and at twice-yearly industry meetings.

384. There is no specific AML/CFT guidance by the Supervisory Board of Public Accountants (RN) to public accountants. The industry organisation FAR has developed an AML/CFT checklist to assist accountants in conducting CDD, which was approved by RN. There are training requirements for accountants which keep them up to date with AML/CFT regulations.

385. The County Administrative Boards (CABs) have a challenge in ensuring that the large number and wide range of entities within their supervisory remit are reached. The CABs have conducted several informational campaigns with positive outcomes according to the authorities, including a brochure and fact sheet on AML/CFT requirements, and a ML awareness campaign together with STA in 2012. In 2013–2016, the CABs conducted targeted outreach to companies that they assessed to fall within the remit of the AML/CFT Act to inform them of their obligations.

386. The Swedish Bar Association's (SBA) guidance, including several case studies, is elaborate and should in general help a lawyer in understanding the requirements. The guidance highlights vulnerabilities, red flags and the risk-based approach. These vulnerabilities and red flags are based on international guidance documents. Additionally, the Bar also provides training courses, so far covering 25% of its members, and has also provided seminars and newsletters to enhance AML/CFT compliance.

387. While the Swedish Gambling Authority (LI) has not issued any formal guidance, supervisors have a close relationship with the state-owned casinos and provide guidance through their regular interaction.

388. The Coordination Supervisory Body (all supervisors, SCRO, Säpo and Fipo) has since January 2016 been working on a 22-page guidance brochure on STR reporting which will include lists of risk indicators and ML/TF scenarios. However, the brochure was not yet published at the time of the onsite and could not be assessed.

Conclusions

389. The supervisory AML/CFT system in Sweden covers all obliged entities and all elements of an AML/CFT supervisory system are in place. There are weaknesses in applying risk-based supervision across all relevant entities. In some instances this is due to insufficient resources to ensure that all relevant entities are subject to supervisory action. Some supervisors, such as the FSA, show a more developed understanding of risk and vulnerabilities of their sectors and individual institutions, but this is in some cases quite basic and does not allow for effective supervision in line with the risks. Some of the DNFBP supervisors' understanding of ML/TF risks is predominately based on the 2013–14 NRAs, which do not provide a comprehensive picture and analysis of Sweden's risks. To some extent this can be attributed to insufficient knowledge and experience-sharing between supervisors and the law enforcement authorities. As such, the Swedish supervisory system only takes a basic risk-based approach.

390. Sweden has achieved a moderate level of effectiveness for IO.3.

CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS

Key Findings and Recommended Actions

Key Findings

- The misuse of legal persons is a vulnerability identified by Sweden, due to the use of false identities, corporate structures, and straw persons in money laundering. Sweden has yet to perform a full assessment of the ML/TF risks associated with all types of legal entities.
- Basic information on most types of legal entities is easily accessible from registries. Sweden also makes available publically the information held in the registers, as well as corporate and personal information. However, some legal entities such as NPAs and some types of foundations are not obliged to register. There also remain a substantial number of foundations that are still not registered although required to.
- While sanctions are applied against persons found to not maintain accurate information in the registry, they are not dissuasive, nor are registrants inspected in a systematic manner.
- Some beneficial ownership information is available from registries (for simple ownership structures) or from financial institutions (from CDD measures). However, these are not sufficient and do not ensure that beneficial ownership information is available in all cases. This impedes efforts to make Swedish legal persons less attractive to misuse by criminals. Nevertheless, beneficial owners may be identified by competent authorities through investigative measures using other sources of information

Recommended Actions

- Sweden should do a full risk assessment of the misuse of all the legal persons for ML/TF, including non–profit associations, of which not all are currently subject to registration requirements.
- Even as Sweden is establishing a central register of beneficial ownership, Sweden should consider measures to ensure the accuracy of information in the register, e.g.: verification of the information at the time of registration; post-registration testing of records; and public access to the register
- To complement the law enforcement work in this area, the FIU and LEAs should provide information on criminal typologies on the misuse of legal entities to SCRO and the CABs, and to work with them on measures to mitigate the use of straw-persons and front companies.
- Sweden should take measures to improve the accuracy of the SCRO's register, for example by conducting random sample testing of company registrations, thematic reviews based on indicators of companies used in criminal typologies in Sweden, or mechanisms to cross-check records across relevant databases held by in different authorities, including the STA.
- Sweden should increase its measures to ensure that the remaining unregistered foundations comply with the registration requirements

391. 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.

Immediate Outcome 5 (Legal Persons and Arrangements)

Public availability of information on the creation and types of legal persons and arrangements

392. Information on the creation and types of legal persons is publicly available at the SCRO's websites[30], which provide information and procedures for creation of sole traders, limited companies, partnerships, and economic associations.

393. Information on the creation of foundations can be obtained at the CABs, where registered foundations are listed in a public database[31], and at the STA's website[32]. Information on the creation of Non-Profit Associations (NPAs) is available on the SCRO's and STA's websites as well.

394. Swedish law does not provide for the creation of trusts or other legal arrangements, and is not a party to the Hague Trust Convention. As such, trusts do not have any legal status or validity in Sweden. There is no restriction on trust activities being conducted in Sweden using foreign trust law.

Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities

395. Swedish authorities have identified the use of front companies, false IDs, and straw persons (i.e. where legal owners or directors are not the actual beneficial owners/controllers as a means to hide the true owner of companies) in criminal schemes. Other types of legal entities, such as foundations, were not excluded as possibly being used for ML and TF. The 2013 NRA on ML noted that companies could be used for ML, and this was further explored in the 2015 NRA on ML by Brå which identified the use of companies in different criminal typologies. However, these do not assess the ML/TF risks of the different types of legal entities in Sweden, including the evaluation and understanding of the vulnerabilities and the extent to which legal persons are being used. No separate formal risk assessment on legal entities was conducted, although LEAs have an understanding on the common legal entities used in criminal typologies through their investigative work.

396. The EBM assesses the risks related to legal persons created in Sweden being used for economic crimes in its intelligence reports. Its 2014 Status report noted that according to SCRO, there have been an increase in delayed, non-submitted and incorrectly completed annual reports, partly due to some 28 percent of Swedish limited companies making use of the exemption from audit requirements; 74 percent of those exempted companies have as a result never been audited. This affects the reliability of information collected by the authorities.

---

30 Swedish Companies Registration Office(Bolagsverket), www.bolagsverket.se/ and Swedish government agencies collaboration www.verksamt.se/

31 Public database (Länsstyrelsernas), http://web05.lansstyrelsen.se/stift/StiftWeb/SSearch.aspx

32 Swedish Tax Agency (Skatteverket), www.skatteverket.se/privat.4.76a43be412206334b89800052864.html

Mitigating measures to prevent the misuse of legal persons and arrangements

397. Sweden's context has several factors that lower the risk of misuse of legal entities. Sweden has a strong tradition in the transparency of information, including the public availability of information held in the company registers, as well as corporate and personal information (e.g. tax returns of individual companies and natural persons). Swedish residents have national identification numbers which are necessary for all important or official activities, e.g. opening a bank account. In addition, nominee directors are expressly not allowed by law, while nominee shareholders are restricted to capital market intermediaries (such as Central Securities Depositories; CSDs). Changes in share ownership are only valid once it is reflected in the company's share register, which are legally required to be available to the public on request.

398. As a result, legal ownership and control of most Swedish legal persons is highly transparent. A problem is however, as the authorities have identified, that straw persons and front companies are regularly used in major crime types (e.g. tax crimes, fraud, organised crime). Whenever the Tax Agency (STA) does encounter false corporate records, they would highlight it to EBM for enforcement action. While authorities, such as EBM and STA, have actively pursued the use of legal persons in their investigations (see more under IO.7), there have not been corresponding measures taken on the preventive side, whether in terms of enhanced controls during registration and ongoing checks of corporate records, or strengthened enforcement of non-compliance (such as in the case of unregistered foundations). In addition, where the legal persons have foreign elements (e.g. intermediate or ultimate owners), identifying the ultimate legal and beneficial owners can be challenging.

399. In addition, as Sweden has not assessed the ML/TF risks of all types of legal persons, it cannot be determined whether the country has taken appropriate measures to mitigate the specific vulnerabilities of the different types of legal persons in Sweden.

400. The non-registration of foundations was an issue in the 3rd round FATF ME in 2006. All but one type of foundations have been required to register since 2015. In addition to addressing the deficiency highlighted in the 3rd round report, the legislative changes strengthened the prevention against the misuse of foundations in general, and included other measures such as the introduction of requirements specific for fundraising foundations. Due to the recent introduction of the new requirements, the authorities estimate that 30% of foundations that are required to register have yet to do so. NPAs continue to not be required to register, except under specific circumstances such as when conducting a trade, the decision for which was not based on an assessment of the ML/TF risks. While the authorities view NPAs as less risky than foundations for ML/TF, the exemptions of NPAs and for the remaining category of foundations from registration was not based on an assessment of risks.

401. Although trusts are not recognised in Sweden, there is no prohibition for trust activities to be conducted. This is affirmed by the banks which have trustees as clients, although not common, as well as the registration of trust service providers at the SCRO. The authorities have not assessed the ML/TF risks of trust-relevant activities in Sweden, nor is there information on the size and scale of such activities. The CABs have, however, since September 2015 initiated an examination of the level of trust-service activity in the course of their supervision of the TSP sector.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons

402. Sweden does not require companies themselves or company registries to obtain and hold beneficial ownership information. Where the persons on record happen to also be the beneficial owners, the authorities would be able to quickly identify and obtain beneficial ownership information. The authorities indicate that this is likely the case for partnerships and registered foundations. While FIs and DNFBPs are required to identify beneficial ownership in their CDD, LEAs are delayed in their ability to seek out such information that may be held by the FIs and DNFBPs as they sometimes do not know which banks hold accounts for a specific person, at least until they start to trace the money flows. The LEAs did not appear to rely much on the beneficial ownership from CDD by FIs and DNFBPs, which in several ML investigations the LEAs found to not be accurate. A central register of bank accounts or of beneficial ownership information – which Sweden intends to create in the context of the implementation of the Fourth EU AML Directive – could assist LEAs in obtaining information more expediently and enhance the effective use of such information.

403. To determine beneficial ownership, LEAs conveyed that they obtain various sources of information, using investigative techniques such as surveillance, wiretapping, IT-tools, and document seizures, in order to follow the money to determine who the controller of the funds is (whom LEAs view as most likely to be the beneficial owner). LEAs have in a number of cases successfully uncovered straw persons, and identified and prosecuted the true beneficial owners. Coercive investigative measures are however limited in their use to cases where an investigation of a serious offence has already begun, are costly and time-consuming, and thus only partly addresses the concerns on beneficial ownership information.

404. Most basic information on registered legal entities is contained in government registries and is easily accessible by competent authorities, who are generally satisfied with the quality and reliability of the information in the registers. Shareholder information of most companies is not held in government registries, but are held either at the companies itself, or maintained by a register at a CSD. This is not an issue for publicly-listed companies, nor in the case of close companies, i.e. companies where four persons or less own more than 50% of the total stock, which are required to register ownership information with STA. There will be some delay where LEAs have to seek the information from the CSD register or the company office, although the competent authorities have not found this to be a significant impediment.

405. The authorities recognise the use of straw persons as a common typology, which decreases the reliability of the information held at the registers. The SCRO has stated that its ability to identify straw persons is very limited. While company registration information is checked and screened against certain lists, e.g. for bankruptcy and business prohibition, similar to the company registration regimes of many countries there is no systematic or proactive risk-based monitoring of compliance.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements

406. Trusts and other legal arrangements are not recognised in Sweden, but as explained above there are trust-relevant parties in Sweden. Information on trust-relevant parties is therefore only available from CDD information collected by the FIs. Such information is therefore limited to cases where the trustee has established a business relationship with an FI in the capacity as a trustee.

407. Trust service providers (TSPs), as well as company service providers, are covered under the AML/CFT Act, and are required to register with the SCRO. Information on trusts serviced or created by them, and on some of the trust-relevant parties (i.e. the trustees and beneficiaries[33]), should be held by the TSPs according to their AML/CFT obligations. However, as described in IO.3, the authorities have a limited knowledge of this sector, and have limited capabilities to ensure their compliance with AML/CFT requirements.

408. Where a trustee is a tax-resident in Sweden, the STA could have information on the settlor(s) and beneficiary(ies) of the trust as Swedish tax law requires trustees to keep information for the STA to determine the tax liability of the trust's asset and income. Competent authorities may then be able to access the information held by STA, or obtain it from the Swedish trustees, in the course of their investigations. However, the authorities note that it can be difficult to clarify which natural persons are associated with a particular trust.

409. As a result, competent authorities have limited ability to access information on the Swedish elements of legal arrangements created under foreign law. While some information is available at FIs, and should be available at TSPs, the assessors are unable to conclude that access to basic and beneficial ownership is adequately timely, accurate, or current.

Effectiveness, proportionality and dissuasiveness of sanctions

410. The SCRO is able to apply sanctions for non-compliance, such as for failure to maintain the shareholders' register, or for accounting offences like updating of corporate information at the company registry. The SCRO has deregistered companies for serious non-compliance. The assessment team was provided with three cases of court convictions with (low) penalties for intentional wrongful registration over the past 5 years. However, these are reactive as there is no system to perform verification of new and existing records. There are scarce statistics on the number and range of sanctions applied, and the assessment team is therefore unable to conclude that sanctions are effective, proportionate and dissuasive.

411. Foundations that are found to have failed to comply with their requirement to register and provide information have been sanctioned by the CABs. e.g. by injunctions, suspending a board member temporarily, and conditional fines. The authorities provided statistics indicating between two to three thousand injunctions (of which a small number with conditional fines) are given every year, out of 16,240 registered foundations.

33 See TC Annex Criterion 10.11

412. As described in IO.3, inspections (and consequently sanctions) on FIs and DNFBPs, and the application of beneficial ownership CDD by them, are infrequent.

Conclusions

413. In the context of Sweden, basic information on most legal persons is recorded either in government registries or by the entities themselves, and these records are publically available; hence, complex legal structures and their legal owners can easily be traced. Sweden is not seen as a centre for company incorporation and does not have heightened risks in that respect. However, straw persons (i.e. where legal owners or directors are not the actual beneficial owners/controllers) are identified by the authorities as regularly used in criminal schemes which can affect the reliability of the information on record. The authorities recognise the frequent misuse corporate structures in the major predicates in Sweden of tax crimes and fraud. Beneficial ownership is also only collected by FIs and DNFBPs as part of CDD (which is elaborated in Chapter 5 on IO.4).

414. Sweden has achieved a moderate level of effectiveness for IO.5.

CHAPTER 8. INTERNATIONAL COOPERATION

Key Findings and Recommended Actions

Key Findings

- Swedish authorities prioritise international cooperation and have established effective systems and processes to support it. Cooperation is very close with the Nordic and Baltic regions, but extensive cooperation also takes place with EU members and other countries worldwide.
- Sweden provides mutual legal assistance and extradition/surrender to countries using European mechanisms (e.g. European arrest warrants, Eurojust), and through dedicated international chambers of public prosecutors and a central authority at the Ministry of Justice.
- Case management systems along with the SPA's internal directives ensure the timely processing of incoming cases, which are generally well prioritised.
- Law enforcement cooperation is a particular strength. The Police has established a well-resourced Single Point of Operative Contact (SPOC) to receive, action, and follow-up on requests for cooperation. Sweden also uses a network of liaison officers to facilitate cooperation, including both Swedish liaisons and shared Nordic liaison officers. Investigators and prosecutors make effective use of joint investigative teams to investigate ML and recover the proceeds of crime.
- FIU to FIU cooperation takes place through shared platforms and appears to currently be prioritised effectively by the FIU.
- Sweden's FSA collaborates closely with foreign supervisors when supervising Swedish financial institutions which operate in other countries, through supervisory colleges and joint on-site inspections, as well as coordination on investigations and sanctions cases.
- Sweden actively seeks international cooperation when intelligence or evidence is needed from foreign partners, including to trace money abroad and authorities have successfully prosecuted some cases involving international criminal networks through cooperation with foreign counterparts.
- Sweden is able to provide available beneficial ownership information on legal persons to requesting states though there are certain limitations concerning the identification of beneficial owners particularly when foreign legal persons are involved.
- Sweden maintains statistics in relation to MLA and extradition/surrender matters handled by the MOJ and the SPA, as well as statistics from the Swedish desk at Eurojust; however, the statistics could be broken down further to indicate the types of crime the requests relate to.

Recommended Actions

- Sweden should enhance the quality of statistics including with regard to MLA requests made through direct contact, the types of crime for which the requests are made and the value of assets frozen as a result of international cooperation. Sweden should also keep track of exchange of basic and BO information on legal entities and arrangements.
- Sweden should strengthen international cooperation among DNFBP supervisors

415. 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 Cooperation)

416. Due to Sweden's position as a financial centre for the Nordic and Baltic regions, which exposes its financial system to ML/TF risks originating outside Sweden, international cooperation is an important aspect of the AML/CFT system. The authorities request and provide a broad range of cooperation with third countries (particularly the Nordic region and the EU, but also other countries worldwide) to strengthen the fight against crime, including for money laundering (ML), associated predicate offences and terrorist financing (TF). With Nordic and EU countries, cooperation normally occurs with direct contacts between competent authorities; with other countries, communication occurs via the Ministry of Justice.

417. The responses and feedback received from 13 countries[34] noted that requests for cooperation made to Sweden were generally responded to in a timely manner and information provided by the Swedish authorities was of good quality. The feedback covered cooperation by Fipo, the Police Authority, the Swedish Prosecution Authority, Customs, and supervisors.

Providing constructive and timely MLA and extradition

418. Sweden has in place a comprehensive structure to provide constructive and timely MLA and extradition/surrender. Sweden privileges direct communication between competent authorities, particularly with Nordic and EU countries. The requests made by direct communication make up a large portion of the total number of MLA and surrender cases. When direct contacts are not established (generally with non-Nordic, non-EU countries), communication occurs via the Ministry of Justice, which then forwards the requests to the Swedish Prosecution Authority (SPA) for processing.

419. Regardless of whether the request is made directly to the Swedish competent authority or to the Ministry of Justice, the SPA's three International Prosecution Chambers deal with most of requests. EBM and some SPA public prosecutors working in specialised chambers (such as the National Security Unit) also engage in international cooperation. The concentration of non-Nordic international cooperation in a few offices creates long-standing expertise and competence. Likewise,

[34] Belgium, Canada, Finland, France, Hong Kong China, Japan, Latvia, Lebanon, Macao China, Mexico, Norway, Turkey, United States

direct contacts between competent authorities expedite communication by cutting unnecessary bureaucratic steps.

420. The quality of the responses is ensured by the fact that the requests are dealt with by staff with training and specialisation in international cooperation (usually a legal expert, under the supervision of a prosecutor responsible for quality checks). Their work is supported by several templates, handbooks, and manuals developed by the SPA and EBM,[35] which facilitates the understanding of foreign legal systems. Prosecutors noted that requests are rarely rejected and that more information is often sought from the requesting partner if needed. The requirements for dual criminality only apply in cases of coercive measures, and there is no indication that this has created a problem in the provision of assistance related to AML/CFT. Some authorities noted that the new ML offence established in 2014 has increased the possibility of cooperation with regard to self-laundering. Peers were generally satisfied with the quality of information received.

421. The provision of timely assistance is ensured also through case management systems available to prosecutor's offices. The internal directive of the SPA (ÅFS 2007:12) recommends that assistance should be provided within two months. The SPA and EBM monitor the status of each request for legal assistance through a system called Cåbra. The system communicates with the police's case management system and allows all directives, evaluations and reminders to be issued electronically. Decisions and documentation are entered in this system. Cåbra indicates when a request for MLA is about to hit the deadline of two months. The International Public Prosecution Office in Stockholm, which deals with most of the incoming requests, also has a separate system for monitoring requests for legal assistance which provides an overview of all incoming MLA requests and their status.

422. Sweden provided statistics on the volume, timing and quality of international assistance related to ML and TF. The exact number of MLA requests related to ML and TF cannot be established with certainty, as the Ministry of Justice does not break down the requests received by offence. This information is kept by SPA, who indicated that in 2015 public prosecutors, including EBM, received 32 requests for international cooperation related to ML, including European Arrest Warrants and Nordic Arrest Warrants. Of these 32 requests, the International Public Prosecution Office Stockholm and the International Public Prosecution Office Malmö received in 2015 17 and 7 MLA requests respectively. The SPA indicated that the total number of MLA requests on ML could be more than 32 as it is possible that some prosecutorial chambers did not report all MLA cases to the SPA. On TF and/or terrorism, Sweden received 16 MLA requests, all dealt with by the National Security Unit of the SPA. MLA requests related to ML or TF represent a small proportion of the more than 1 000 requests that Sweden receives every year.

423. The timing of the answers is generally good. According to the SPA, incoming requests to the International Public Prosecution Office in Stockholm are dealt with in an increasingly efficient manner, with most cases being processed within two months (for example, in 2015, the International Public Prosecution Office Stockholm was able to handle 310 cases out of 447 within 60 days, with an average time of 43 days). Occasional delays in answering a request are not due to lack

35 The SPA has developed handbooks on Extradition, European Arrest Warrants, Nordic Arrest Warrants, Legal Assistance, Joint Investigation Teams, and Transfer of Legal Proceedings.

of resources or prioritisation, but rather to the time taken to collect information (e.g. bank information), an inability to contact the relevant person, the complexity of the request, or the need to complement information from the requesting country. Peers indicated that the information received from Sweden was generally timely.

424. The case studies provided onsite showed that Sweden responds to various types of requests for cooperation including those related to asset identification, freezing, confiscation, provisional attachment and evidence collection. Statistics show that from 2012 to 2015 the Swedish authorities handled an average of 52 cases a year on international tracing of assets. In some cases, the Swedish authorities have ordered that property confiscated at the request of another state or its value should be handed over to the requesting state. The provision on asset sharing has also been applied in many cases. Sweden did not provide statistics on the value of seizures and confiscations made on the basis of the requests for MLA. Sweden can enforce a foreign judgment for confiscation in case of EU and Nordic countries, as well as in cases where a multilateral or a bilateral treaty exists. All types of information, including bank information, can be provided.

425. International cooperation is particularly strong and developed with EU and Nordic countries, which also cover the majority of international requests received. Within the EU, Sweden is active through, e.g. Eurojust; and Sweden implemented a number of EU instruments that permits mutual recognition of the decisions of other countries within the EU in a range of areas of cooperation.[36] International cooperation with Nordic countries is further strengthened by joint Nordic liaison officers dispatched around the world (to China, Colombia, Dubai and Turkey, among others).

426. As for requests for extradition/surrender, European and Nordic Arrest Warrants are managed via direct contacts among competent authorities and Swedish prosecutors adhere to the deadlines prescribed by European and Nordic Arrest Warrants. In relation to all offences, in 2015, 47 individuals were surrendered to countries pursuant to a Nordic Arrest Warrant; there were 142 surrender cases pursuant to a European Arrest Warrant. Extradition requests concerning countries outside the EU or the Nordic region are made via the Ministry of Justice. These requests are subject to the Government's decision. These cases are handled by the SPA and the Supreme Court, where the defendant does not consent. If a person consents to extradition, a simplified system applies. There are in general no legal deadlines in these cases and the SPA has not prescribed deadlines for processing these cases so the process may be slower.

427. Domestic legislation prevents extradition of Swedish citizens outside EU and Nordic countries. Where a third country requests the extradition of a Swedish citizen, Sweden will consider opening an investigation or prosecution on behalf of the requesting country. The Swedish authorities pointed to a number of cases where they have opened an investigation on Swedish nationals after receiving information from abroad. However this can give rise to risks that prosecution may be impossible for other reasons (e.g. because of the difference in the application of statutes of limitations between Sweden and the requesting jurisdiction).

[36] These include the Framework Decision on the European Arrest Warrant, the Framework Decision on Freezing Orders and the Framework Decision on Confiscation

428. There are multiple channels available for international cooperation regarding terrorist financing: the lead agency in Sweden – Säpo – is both an intelligence agency and a law enforcement authority, and works in conjunction with a specialised group of prosecutors which handles national security cases (as described under IO.9). Cooperation on TF cases can be pursued through judicial channels including mutual legal assistance; through law enforcement cooperation, and through intelligence cooperation channels –depending on the type of cooperation required. Cooperation on TF makes use of Nordic and EU cooperation mechanisms, liaison officers, and bilateral relationships with relevant authorities in other countries. Swedish authorities therefore have close and direct links with counterparts in Nordic and EU countries, and use central authorities or dedicated liaisons to cooperate outside the EU/Nordic groups.

429. Requests for MLA regarding terrorism cases are received by the National Security Unit within the Prosecution Authority and actioned immediately. The unit has standing arrangements to draw on additional prosecutors if needed to handle a high volume of cases, and does not have a backlog of cases. Säpo establishes direct contact with their partner organisation in the relevant country, in parallel to the MLA channels, to ensure fast communication.

430. The strength of the Swedish system stems from the prevalence of specialised and regionally organised units within the SPA, the predominance of personnel with the requisite skill and training, the availability of appropriate tools and support function to facilitate international cooperation as well as a well prioritized system of processing incoming requests. This makes it a good system to provide timely and constructively MLA and surrender/extradition in each case. However, there is no mechanism to monitor the functioning and efficiency of the international cooperation system for AML/CFT as a whole. It should be noted that the feedback provided by partners was generally very positive, which confirms the ability of Sweden to provide constructive and timely international legal cooperation. Even though the structure and the case management systems appear to be adequate to handle each case, the efficiency of the overall system could be improved by establishing an overview of how the system for international cooperation in the AML/CFT functions as a whole.

Seeking timely legal assistance to pursue domestic ML, associated predicate and TF cases with transnational elements

431. Sweden seeks legal assistance for international cooperation to pursue domestic ML, associated predicate offences and TF cases which have transnational elements. As Sweden indicated, many ML/TF cases in Sweden have a transnational element. Swedish requests for MLA and extradition/surrender to other countries, including under European and Nordic Arrest Warrants, are made by the prosecutors at the relevant public prosecution office. Sweden generally conducts a parallel financial investigation to "follow the money" and this suggests that legal assistance can be sought much earlier during the investigative process. Prosecutors often receive assistance and support from the European Judicial Network points of contact, Eurojust and advisory from the international unit. There are ongoing efforts to raise awareness of these support functions to further enhance the processing of outgoing requests for international legal assistance.

432. Sweden actively seeks legal assistance from foreign partners, including to trace money abroad, and authorities have successfully prosecuted some cases involving international criminal

networks through cooperation with foreign counterparts. Between 450 and 600 MLA requests are sent abroad each year, and there were 23 and 27 extradition requests in 2013 and 2014. There were 55 cases of MLA requests related to ML offences in 2015, which is a considerable increase compared to 2013 (3) and 2014 (22), which can be explained by the introduction of the new ML offence in 2014 (see IO.7). (See also Folarin in **Box 4**.)

433. The Swedish authorities indicated their satisfaction with the cooperation received, particularly in Europe, although in some cases it has been difficult to obtain valuable evidentiary and investigative information. Some difficulties were also encountered in the execution of claims, as some countries do not mutually recognise claims made in a final court sentence.

434. To sum up, Sweden makes active use of international cooperation to pursue criminals and their proceeds. It has requested MLA and extradition to other countries in a significant number of cases, demonstrating that it makes good use of these tools to investigate and prosecute ML and TF.

8

Seeking other forms of international cooperation for AML/CFT purposes

435. Sweden makes use of other forms of international cooperation for AML/CFT purposes, particularly through the SPOC system (see below). The FIU frequently requests the assistance of foreign counterparts, about 100 times a year, including to obtain banking information. Financial supervisors collaborate with supervisors of foreign branches on the investigations and sanctions of the parent Swedish banks, particularly with Nordic counterparts. The Swedish authorities leverage international networks like the Camden Asset Recovery Inter-agency Network (CARIN) and use a network of liaison officers to facilitate cooperation, including both Swedish liaisons and shared Nordic liaison officers. Investigators have made effective use of joint investigative teams to investigate ML and recover the proceeds of crime. Sweden has provided a number of examples of informal cooperation (see also *Södertälje* in Box 2., *Folarin*, in box 4., and *Case Ateljé*, in Box 8.).

Box 18. **Example of International Cooperation**

A family in the Stockholm region was systematically abusing the Swedish welfare system via systemic assistance fraud. The family received large amounts of welfare money for the care of a relative. The Swedish CARIN contact received information that the recipient of the money was on holiday in Spain, while receiving welfare money to care for her relative. The CARIN contact communicated with their Spanish colleague to ascertain whether the person had stayed in a hotel. 30 minutes later they received an answer that the person had been staying alone at a hotel while the relative remained in Sweden. The information proved that the person had received the welfare payment fraudulently.

Box 19. **Example of Cooperation Linked to Confiscation of Proceeds of Crime**

A person in western Sweden was suspected for a significant amount of time in relation to a case concerning aggravated narcotics offences with national and international links. The proceeds of the trade in narcotics were used to purchase motorbikes, to renovate leisure houses in Sweden, and to purchase property in Spain. Via a request from Sweden to Spain, using the CARIN network, the Spanish police was able to identify the property in Spain and its legal owner, which in fact was the suspected drug dealer. In the appeals court, the prosecutor made a claim to confiscate the property as proceeds of crime. The appeals court awarded the confiscation of the property.

Box 20. **Example of Operative Cooperation**

During an operative police meeting, which are held in alternating Baltic Sea states and CARIN and ARO representatives of most Baltic Sea states participate, a case was discussed in order to determine if certain suspected crimes occurred in other countries than Sweden. The suspected crimes included aggravated tax offences, as well as aggravated accounting offences. There were also some suspicions of narcotics offences. The meeting provided "hits" immediately in that criminal activities in a Baltic state were suspected. Collaboration between Swedish CARIN and Asset Recovery Office representatives of Baltic States showed that criminal activity in Sweden (including aggravated tax offences and aggravated accounting offences) also occurred in one Baltic State. Further intelligence operations indicated that it was likely that large transfers have been made from Sweden to that state. EBM opened parallel criminal investigations without delay. Significant cash transfers were detected between Sweden and the Baltic state, but also to a state in Asia. These were significant amounts which ended up in foreign accounts and were subsequently returned and withdrawn from Swedish currency exchange offices. The transactions constituted sufficient evidence to press charges with several convictions.

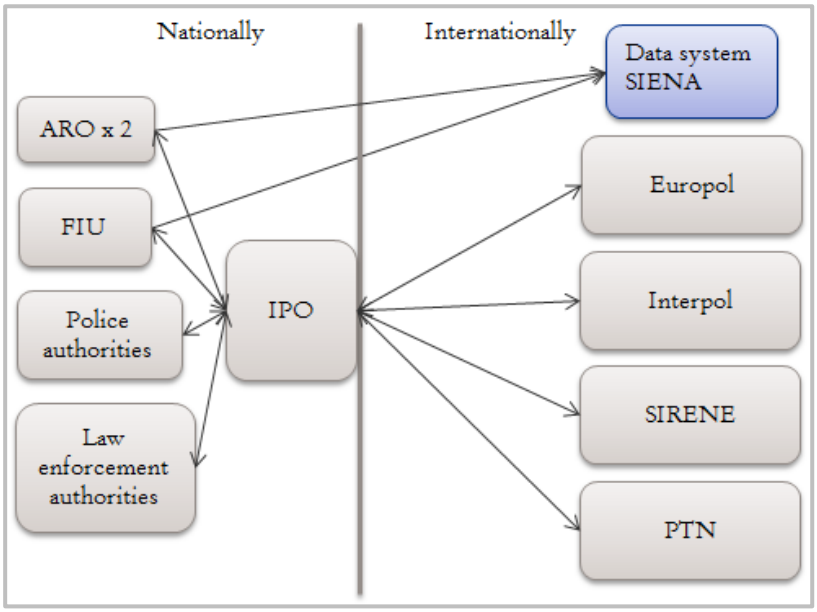
Providing other forms international cooperation for AML/CFT purposes

436. Sweden provides other forms of international cooperation for AML/CFT purposes in the field of law enforcement, financial intelligence, taxation, customs, and financial supervision.

Law enforcement

437. The Police Authority's National Operative Unit (NOA) houses the unit for international police cooperation (International Division), which constitutes a Single Point of Operational Contact (SPOC), for streamlining international police cooperation. The SPOC was established as a clear and simple point of contact for foreign partners irrespective of the type of request required. It allows requests from foreign authorities that may not understand the Swedish structure of authorities to quickly reach the right recipient.

Figure 3.**Delimitations and Priorities of the SPOC Process**



438. The SPOC system receives, prioritises, actions, and follow-up on incoming requests and information. When information or requests arrives, it is recorded in DAR (one of the Police Authority's case management systems) and a case is created. Each case is dealt with on the basis of the level of priority. If the first review of the incoming message leads to the decision that the information does not require further measures, the information in the message is archived in the system. In case of outgoing requests, an object and a case are created in the case management system when a request is issued by the Swedish Police. If the object existed previously, cross references are made between the existing case and new cases. A written request on the case is sent to the foreign police authority. Upon receiving a response, it is entered under the same case and forwarded to the original requester. If no additional questions have been received in the case, it is closed and normally purged after three years. Examples of cases include the establishment of IDs, register checks, the exchange of intelligence and investigative information, as well as warrants for suspected individuals.

439. The number of incoming messages to the SPOC has increased steadily by an average of 7-9% over the last five years. In 2015, a total 250 753 messages (which includes requests from foreign authorities, as well as responses to previous requests to foreign authorities) were received by the SPOC. The incoming messages gave rise to approximately 94 600 cases in 2015. While there are no statistics on the Police Authority's response rate, the large number of cases indicates that the police engage actively with these requests. There are 53 dedicated officers coordinating the SPOC process, with 38 in the front office (25 of which working 24/7), and 15 case handlers. The SPOC is an example of an efficient procedure that includes all types of requests and answers in the field of international cooperation.

Table 21. **SPOC Statistics**

2015

Form of Co-operation	Cases	Incoming messages	Outgoing messages
Europol	3 724	23 155	6 432
Schengen	29 615	83 542	45 323
Interpol	51 759	122 738	58 708
Liaison officers	624	2 053	n/a
Prüm	8 893	19 265	n/a
Total	**94 615**	**250 753**	**110 463**

2014

Form of Co-operation	Cases	Incoming messages	Outgoing messages
Europol	3 184	20 164	5 354
Schengen	23 893	71 334	41 001
Interpol	46 021	110 670	49 195
Liaison officers	577	2 238	n/a
Prüm	5 729	11 630	n/a
Total	79 404	216 036	95 550

2013

Form of Co-operation	Cases	Incoming messages	Outgoing messages
Europol	2 781	16 931	4 716
Schengen	21 174	67 327	17 991
Interpol	41 162	99 212	32 816
Liaison officers	545	1 806	n/a
Prüm	1 050	2 157	n/a
Total	66 712	187 433	55,523

440. The Asset Recovery Offices (ARO) at NOA and EBM also play an important role in international cooperation in terms of tracing assets at an international level. ARO uses the SIENA system to ensure secure communications and has implemented internal deadlines and systems of prioritization within this system to ensure rapid responses to requests. The ARO also leverages international networks like the Camden Asset Recovery Inter-agency Network (CARIN) and use a network of liaison officers to facilitate cooperation, including both Swedish liaisons and shared Nordic liaison officers. Investigators and prosecutors have made effective use of joint investigative teams to investigate ML and recover the proceeds of crime.

FIU to FIU

441. Fipo provides information to other FIUs both spontaneously and upon request. FIU to FIU cooperation takes place through shared platforms (FIU.net and the Egmont Secure Web) and appears to be prioritised effectively by Fipo.

442. Three peers however indicated that additional information from reporting entities had not been provided by Fipo, and in fact, up until 2015, all requests for additional information were systematically rejected. Fipo would reject the requests on the basis that they did not meet the legal requirement in Sweden. Fipo's position stemmed from a misunderstanding of the legal requirement and/or a miscommunication with the foreign FIU (Fipo should have approached the requesting FIUs to provide additional elements that would substantiate their suspicions).

443. Following a change in Fipo's management in 2016, the earlier interpretation of the law has been revised. Now, all requests for information from a foreign FIU which are based on a foreign STR, or concrete information, are treated in the same way as when Fipo deals with an STR received from a domestic reporting entity. Fipo indicated that, in order to obtain additional information from reporting entities for foreign purposes, it would open an "initiative case" (see I.O.6). For an "initiative case" to be initiated, a foreign FIU must demonstrate that there is ground for suspicion, which in practice means that it should provide at least two sources of intelligence. According to Fipo, a request for additional bank information was received from a foreign FIU in April 2016. Fipo provided publicly available information and requested additional elements, such as more information about the time period for the transactions and a clarification on whether there was an on-going criminal investigation, which would allow Fipo to trigger an initiative case and obtain the bank information. The issue seems resolved.

STA - International Cooperation in Taxation

444. STA's special competency offices for international tax requests and the exchange of information engages with other countries in respect of taxation of foreign-owned Swedish companies, taxation of foreign companies and taxation of natural persons with mainly limited tax liability. Sweden can exchange information on request in the area of taxation with 127 jurisdictions.[37] In 2015, the STA sent information to 52 jurisdictions and received information from 42.

TV - Customs

445. TV's international operations engage in information exchange both within the EU and outside the EU. TV occasionally receives requests for assistance in suspected ML cases. Based on the request received, TV either responds directly or in consultation with EBM. TV has not received any requests related to TF. TV has not made any requests of its own.

Supervisory information

446. Sweden's FSA collaborates closely with foreign supervisors when supervising financial institutions which operate in other countries. Cooperation is very close with Nordic financial

37 http://eoi-portal.org/jurisdictions/SE#agreements.

supervisors given the integration of the financial systems and Sweden's role as a regional financial hub. Information and best practice is shared through direct contacts, committee meetings, provision of guidelines, workshops and through the supervisory college. Home-host cooperation on handling of AML/CFT issues occurs and there is regular exchange of information on AML/CFT-issues. There is coordination of supervisory activity and the FSA has conducted joint onsite inspections. There has been close collaboration with foreign branches on the investigations and sanctions of the parent Swedish bank. There is also some informal cooperation among supervisors in the gambling sector.

International exchange of basic and beneficial ownership information of legal persons and arrangements

447. Competent authorities are able to provide basic and beneficial ownership information on legal persons as these are largely available in the public domain and there are mitigating factors, such as transparency measures, to prevent the misuse of legal entities and arrangements (see IO.5 above). EBM, SPA and the Police Authority have assisted foreign authorities to identify beneficial ownership of legal persons in Sweden by carrying out extended searches of the registers which involves conducting research on information in the open domain and those provided by other authorities where the information is not restricted. For example, in a recent case of suspected ML, where information was not found in the pubic registers, EBM conducted open source intelligence within the CARIN framework with the help of the Internet Collection Unit. The requesting state considered the response provided by Sweden to have provided valuable information. Even in cases where coercive measures were needed to find the beneficial owners, Sweden was able and willing to use them in response to a foreign request. There are no statistics on how often basic and beneficial ownership information is provided to foreign countries or on the timeliness of the response.

Conclusion

448. Sweden has many of the characteristics of an effective system in the area of international cooperation and only minor improvements are needed. Sweden is party to several bilateral and multilateral agreements, but is also able to cooperate in the absence of agreements. Competent authorities regularly approach various networks and bodies for information to enhance the quality of their work and increase effectiveness. Swedish authorities have implemented good case management systems and Swedish legislation and internal directives requires expediency in these cases. The SPOC system employed by the Police Authority is an example of an effective procedure that receives all types of requests and answers in the field of international cooperation. Another good example is the network of Nordic Liaison Officer (PTN) in which Sweden has contributed actively. The difficulties related to the exchange of additional information to foreign FIUs appear to be resolved.

449. Swedish authorities assist other countries with all types of requests for cooperation such as asset identification, freezing, confiscation and exchange of financial intelligence, supervisory information as well as basic and beneficial ownership information. However, Swedish authorities need to complement the qualitative information and case studies with statistics that specify the types of assistance requested, the number and value of assets frozen and arising from international

cooperation and the value of assets repatriated or shared. This would allow a high-level management of the international cooperation system for AML/CFT as a whole.

450. Overall, Swedish authorities provide MLA and exchange information in a constructive and timely manner and proactively seek international cooperation when required.

451. Sweden has achieved a high 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 numerical 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 2006 available at www.fatf-gafi.org/countries/s-t/sweden/.

Recommendation 1 – Assessing Risks and Applying a Risk-Based Approach

These requirements were added to the *FATF Recommendations*, when they were last revised in 2012 and, therefore, were not assessed during Sweden's third mutual evaluation which occurred in 2006.

Criterion 1.1- Sweden conducted a national risk assessment for ML in 2013 and for TF in 2014. These have been supplemented by several agency- and sector-specific reports on e.g. economic crime, organised crime, and ML and TF typologies.

Criterion 1.2- The Swedish Government tasked a group of 16 government agencies and a self-regulating body, led by the FSA, to conduct the 2013 and 2014 ML and TF national risk assessments. Representatives from the private sector and other government authorities also participated in the discussions. Outside of the 2013-2014 NRA process, the assessment of ML/TF risk in Sweden takes place on the operational level by the authorities who cooperate in several areas, but these are not coordinated, nor do they involve all parties who were part of the NRA.

Criterion 1.3- The Swedish authorities are required by the Government Assignment (*Government Decree Fi2012/4457*) to conduct updates to their analysis annually in order to provide a basis for risk-based measures. Since the 2013-2014 national risk assessments were carried out, there have been two reports on specific issues that follow from the NRA. Sweden plans to initiate further assessments in 2016 to be carried out in 2017.

Criterion 1.4 - The 2013 and 2014 ML and TF national risk assessments are publically available on the websites of the FSA, the Government, and the Riksdag. Other specific risk assessments are generally publically available in accordance with Sweden's policy of public access to official documents, with exceptions for reports of particular sensitivity. Supervisors inform the entities under their remit of these assessments in the course of their supervision.

Criterion 1.5- Sweden developed a national AML/CFT strategy in 2014 based on the 2013/14 NRA, which identified several AML/CFT priority areas and set out measures to be undertaken to enhance the regime. Furthermore, several agencies' own priorities take into account the findings of the NRA and national strategy, and allocate resources to mitigate identified areas of higher risk. Other agencies base their priorities on systematic risk management or on established practices which may not match Sweden's identified ML/TF risks.

Criterion 1.6- Sweden allows specific exemptions from the CDD and ongoing monitoring obligations of the AML/CFT Act for a list of entities and activities, including public authorities, financial institutions within the EEA or other equivalent jurisdictions, companies traded on recognised

exchanges, some life insurance and pensions activity, and electronic money. These exemptions are based on those in Article 11 of the 3rd EU Anti-Money Laundering Directive (Directive 2005/60/EC). These exemptions appear to be based on a presumption of low risk, rather than on a specific risk assessment at either national or EU level. *AML/CFT Act Ch.2 sect.5.*

Criterion 1.7- Sweden requires financial institutions to assess and mitigate their ML/TF risks, and to apply enhanced due diligence in high-risk situations *(AML/CFT Act (2009:62)* Chapter 5, section 1 and *FFFS (2009:1)* Chapter 2).

As identified in the NRAs and in the FSA's risk assessment for 2015, risks such as a lack of understanding and knowledge for ML/TF and risks within specific FIs have been focus areas for the FSA, where additional resources have been allocated to conduct activities aimed to mitigate the identified risks. Sweden's mapping and analyses of identified risk such as currency exchange and cash handling will further develop its supervision and provide further support and guidance for obliged entities.

Sweden's national ML/TF risk assessments have not identified additional sectors, activities, or situations to which AML/CFT measures should be applied in virtue of their risks.

Criterion 1.8- Sweden's AML/CFT Act does not contain provisions for simplified due diligence. Basic CDD measures are required to be applied in all situations subject to the act (noting the exemptions set out under c1.6 above), and enhanced CDD where the ML/TF risks are high.

Criterion 1.9- Financial institutions and DNFBPs are required by the *AML/CFT Act* to assess and mitigate their ML/TF risks, and are subject to supervision for compliance with AML/CFT requirements. Sweden has appointed the FSA as responsible for AML/CFT supervision of FIs The Swedish Gambling Authority (LI) is the AML/CFT supervisor for casinos; other DNFBPs are supervised or monitored for AML/CFT by the CABs, the FMI, SBA, and RN (see Recommendations 26 and 28).

Criterion 1.10- Financial institutions and DNFBPs are required to map and assess their ML/TF risks, document them, and keep their assessments updated. *AML/CFT Act Ch.5 sect.1*.

FIs are required to provide their internal risk assessments to the FSA when applying for a licence. For FIs that are subject to an investigation, the FSA's standard practice is to request for their internal risk assessments and other internal routines.

Real estate agents are required to perform risk assessments in their individual operations, and to deliver the risk assessment information and explain it when FMI conducts market surveillance.

Financial institutions and DNFBPs (including law firms but not lawyers) are also required to ensure that their risk assessments are appropriate to their operations, scope and complexity. *FFFS (2009:1) Ch.2 sect.3, LIFS (2015:3) Ch.2 sect.3, KAMFS (2013:5) Sect.3, CAB Directives Ch.2 sect.3*.

Chapter 5, section 1 of the AML/CFT Act applies to law firms, but not to individual lawyers. In accordance with this regulation, the individual risk assessment of each law firm is to be adapted regularly over time to the specific area of law of the law firm, its mandates under the AML/CFT legislation, its clients, geographical scope of activities, size, etc.

Criterion 1.11- Financial institutions, casinos, and DNFBPs supervised by the County Administrative Boards, are required to establish internal rules for AML/CFT measures, specify who is responsible for procedures, systems, training and guidelines, and implement risk-based measures to mitigate ML/TF risks. *FFFS (2009:1) Ch.3 sect.1, AML/CFT Act Ch.5 sect.1, LIFS (2015:3) Ch.3 sect.1 and Ch.5 sect.2, CAB Directives Ch.3 sect.1 and Ch.10 sect.1*. For public accountants, there are similar requirements in *EtikU 11 sect.7* which is enforceable by way of *RNFS (2001:2) sect.6.*

Real estate agents are required to establish internal rules for AML/CFT measures (*AML/CFT Act (2009:62) Ch. 1 sect. 2 item 8 and Ch. 5 sect. 1*). The responsibility lies with the real estate agent personally and, if he or she is employed, the legal person/employer. Lawyers are required to assess risks of ML and TF in their operations and implement risk-based measures to mitigate those risks (*AML/CFT Act (2009:62) Ch. 1 sect. 2 item 13 and Ch. 5 sect. 1).* There is no requirement that these be approved by senior management.

Criterion 1.12 - Financial institutions and DNFBPs are allowed to not conduct CDD and ongoing monitoring for a list of entities (see c.1.8), except where ML/TF is suspected or where ML/TF risks are assessed to be high. This allows an exemption from CDD and ongoing monitoring, rather than simplified measures, and is not restricted to situations where ML/TF risks are low. It should be noted that FIs and DNFBPs have to monitor transactions pursuant to Ch.3 sect.1 even in situations mentioned in Ch.2 sect.5. AML/CFT Act Ch.2 sect.5.

Weighting and Conclusion:

Sweden is largely compliant with R.1.

Recommendation 2 – National Cooperation and Coordination

Sweden was rated largely compliant with the previous Recommendation 31. The MER recommended that co-ordination at the policy level be enhanced. Recommendation 2 is now more specific about the need for countries to have national AML/CTF policies that encompass identified risks and for coordination to be more formalised.

Criterion 2.1- A national AML/CFT strategy was developed following the national risk assessments in 2013–14, which has formed the basis for the government's ongoing work and dialogue with the authorities as well as the work carried out by authorities themselves. The next update of the strategy is planned to be initiated in 2017. In parallel, Sweden organises round-table discussions where the government and relevant authorities and private sector actors discuss pressing issues, such as on the financing of FTFs in September 2015.

Criterion 2.2- Sweden's national risk assessments for ML in 2013 and for TF in 2014, and its 2014 national AML/CFT strategy, were commissioned by the Swedish Government. But there is no authority or co-ordination mechanism that is responsible for national AML/CFT policies. Instead, there are coordination mechanisms focused on specific risks (e.g. proceeds of crime, organised crime) or types of activity (e.g. supervision). These coordination groups are involved in making

national AML/CFT policies to the extent that they provide input, formally or informally, to the Government's policy process.

Criterion 2.3- There are various bodies and mechanisms for cooperation on an operational level, and for collaboration on activities. For example, there is a Coordination Supervisory Body that coordinates AML/CFT supervision between the relevant authorities and Fipo and Säpo participate in an informal capacity. There are bodies/mechanisms combating organised crime, proceeds of crime, and terrorism that involve the law enforcement, prosecutor, customs and tax agencies; Fipo participates indirectly in these groups as it is a part of the Police Authority. There are in addition bilateral/multilateral co-operation models between Fipo in their own capacity directly with other authorities such as SKV, EBM, Säpo, and the CABs, while relevant agencies are represented or consulted as part of the general procedures for drafting new legislation. However, there appears to be little or no mechanisms for cooperation and coordination on the national policymaking between agencies.

Criterion 2.4- Sweden has formal and informal inter-agency formations that cooperate on non-proliferation related matters. The Reference Group[38] was formed in 1992 for issues related to non-proliferation and chemical, biological, radiological and nuclear defence (CBRN). The last meeting on 19 November 2015 discussed the implications of the Joint Comprehensive Plan of Action (JCPOA) and other financial sanctions issued by the EU.

The Coordinating Council for Non-Proliferation was established to promote more effective cooperation between relevant agencies in countering proliferation of WMD, and consists of ISP's Director-General and representatives from other relevant agencies invited by ISP.

The ISEK is a group of experts from the agencies[39] participating in the coordinating council for non-proliferation. It provides a platform to cooperate and coordinate both on an operative level and through common strategic analyses. When necessary, other relevant agencies, including Fipo and the FSA, take part in ISEK meetings.

On an ad hoc basis, the FSA, the National Board of Trade, the Social Insurance Agency, ISP, and the Ministry for Foreign Affairs meet when necessary to discuss matters related to implementation of sanctions regulations.

Weighting and Conclusion:

Sweden is partially compliant with R.2.

38 The Reference Group consists of Säpo, the Inspectorate of Strategic Products (ISP), Fipo, TV, the Swedish Armed Forces, FRA, the Swedish Defence Research Agency, the Swedish Coast Guard, the Swedish Civil Contingencies Agency, the Swedish Radiation Safety Authority, the Swedish Transport Agency, and the Swedish Ministry for Foreign Affairs (Department for Disarmament and Non-Proliferation).

39 ISP, Säpo, TV, FRA, the Swedish Armed Forces, and Swedish Defence Research Agency

Recommendation 3 – Money Laundering Offence

In its 3rd MER, Sweden was rated largely compliant with the requirement to criminalise money laundering offences. The main technical deficiencies were that criminalisation of money laundering did not cover self-laundering and that the ancillary offences were not sufficiently comprehensive. Since the last evaluation, Sweden has passed a new law on ML criminalisation: the Act on Penalties for Money Laundering Offences (2014:307), which entered into force in July 2014.

Criterion 3.1– ML is criminalised in accordance with the relevant articles of the Vienna Convention and the Palermo Convention. Section 3 of the Act on Penalties for Money Laundering Offences establishes that a person is guilty of a money laundering offence if he or she:

- "transfers, acquires, converts, stores or takes another such measure with the property;
- or supplies, acquires or draws up a document that can provide a seeming explanation for the possession of the property, participates in transactions that are carried out for the sake of appearances, acts as a front or takes another such measure."

A person is also guilty of a money laundering offence if he or she, without the measure having a purpose such as is indicated in above, improperly promotes the possibility of someone converting money or other property deriving from an offence or criminal activities (s.4). A person is guilty of a *money laundering misdemeanour* if he or she did not realise but had reasonable cause to assume that the property derived from an offence or criminal activities. A person who, in the context of business operations or as part of activities that are conducted habitually or otherwise extensively, takes part in a measure that can reasonably be assumed to be taken for ML purposes, is guilty of *commercial money laundering*.

Criterion 3.2– Sweden has an "all crimes" approach which means that all criminal offences which generate proceeds can be predicate offences to ML. The Swedish criminal legislation covers all categories of offences designated in the FATF Glossary. No limitation or threshold is placed on the predicate crime.

Criterion 3.3 **–** This criterion is not applicable in Sweden as there is no threshold approach.

*Criterion 3.4***–** The ML offence covers money and other property derived from an offence or criminal activities, regardless of its value.

Criterion 3.5– When proving that the property is the proceeds of crime, it is not necessary that a person be convicted of the predicate offence. According to section3 of the Act on Penalties for Money Laundering Offences, a person will be found guilty of a money laundering offence provided that "the measure is intended to conceal the fact that money or other property derives from an offence or criminal activities or to promote the possibility of someone appropriating the property or its value." This would not require proof of the exact circumstances of the offence or the criminal activities, such as when it was committed, against whom, etc. This interpretation is supported by the Preparatory Works of the Act on Penalties for Money Laundering Offences and prosecutors' guidelines ("Legal

Memorandum 2015:2").[40] The prerequisite "criminal activities" is also fulfilled even if the prosecutor cannot prove that specific acts have taken place (Government Bill 2013/14:121, p. 109).

Criterion 3.6– The Act on Penalties for Money Laundering Offences is applicable to predicate offenses that occurred in another country. Section 2(2) of the Act states that crimes committed in another country which are equivalent to a Swedish offence may constitute a predicate offence for money laundering.

Criterion 3.7 – The criminalisation of money laundering, as established in the Act on Penalties for Money Laundering Offences, is not restricted to crimes committed by other persons. On that basis, prosecutions for self-laundering are possible under Swedish law. However, the Preparatory Works of the Act on Penalties for Money Laundering Offences and prosecutors' guidelines (Legal Memorandum 2015:2) indicate that a money laundering offence in the form of self-laundering should, as a rule, be consumed by and co-punished with the predicate offence that gave rise to the proceeds. The exception to this rule could be acts of self-laundering by a perpetrator only peripherally associated with the predicate offence. This seems to place a limitation on the criminalisation of self-laundering because a separate act of securing the proceeds of one's own predicate offence may constitute a crime, but would not normally be prosecuted. However, an act of self-laundering could be a circumstance leading to a stricter penalty even when the sentence for the predicate offence consumes the self-laundering charge. In assessing the penal value of the crime, the court should give special consideration to whether the crime was part of a criminal activity which was especially carefully planned or carried out on a large scale and in which the accused had a significant role, such as the money laundering (Chapter 29, Section 2, of the Penal Code). As stated above there are also situations where the offender can be sentenced for both the predicate offence and the money laundering offence.

Criterion 3.8 – It is possible for the intent and knowledge required to prove the ML offence to be inferred from objective factual circumstances. According to the Swedish Code of Judicial Procedure, the court, after evaluating everything that has occurred in accordance with the dictates of its conscience, shall determine what has been proved in the case (1942:740, Chapter 35, section 1)

Criterion 3.9– Natural persons found guilty of ML offences are subject to imprisonment for up to two years (Act on Penalties for Money Laundering Offences, ss.3 and 7).

If the offence is deemed gross, imprisonment for at least six months and at most six years can be imposed (ss.5 and 7). In judging whether the offence is gross, the court shall have regard to all relevant circumstances, particularly: whether the act has concerned objects of "substantial value", whether the criminal measures have been part of criminal activities that have been conducted systematically or extensively, or whether they have otherwise been of a particularly dangerous nature (s.5). The term "substantial value" in terms of an ML offence coincides with corresponding threshold values for crimes against property (e.g. theft, fraud, embezzlement). Hence, when the

[40] A Legal Memorandum is a policy document that is approved by the Chief Prosecutor at the Prosecution Development Centre. The purpose of Legal Memoranda is to provide guidance to prosecutors in different areas of law so that the law is applied uniformly, efficiently and in accordance with the rule of law. The Legal Memoranda are regularly reviewed to ensure that they are in accordance with legislative changes and recent case law.

predicate offence is a crime against property, the same threshold value is applied for the predicate offence as for the subsequent ML offence. As a general rule, a value of five times the price base amount (SEK 221 500, approximately EUR 23 800) would be considered "substantial", and hence the offence would be gross.[41] This principle does not, however, apply in all cases. For example, a drug-related offence can be deemed gross while the subsequent laundering of the proceeds of that crime can be considered normal. Or the opposite: if the predicate offence is a tax crime, the predicate offence can be normal but the subsequent ML offence gross. The Swedish authorities have indicated that approximately 10% of the money laundering offences were considered to be gross in 2015.

If the offence is deemed petty (money laundering misdemeanour), the penalty is a fine expressed in day-fine, and could range from SEK 1 500 to SEK 150 000 (approximately EUR 160 to EUR 16 300) (Penal Code, Ch.25)[42] or imprisonment for at most six months (s.6).

The maximum penalties may appear low in comparison to other countries; however, the penalties applied for money laundering in Sweden are comparable to the penalties for other non-violent offences in Sweden such as theft, fraud, embezzlement and bribery. In that sense, the sanctions applicable to natural persons for ML offences are proportionate and dissuasive.

Criterion 3.10– The sanctions on legal persons, particularly the amount of corporate fines, may not be dissuasive in all cases. Fines can be imposed on a legal person for crimes committed in the course of business activities in cases where the legal person has not done what could reasonably be required to prevent the crime; or if the crime was committed by a person with decision-making powers or with responsibility of supervision (Penal Code Ch.36, s.7). Corporate fines cannot be applied if the crime was committed against the legal entity. Corporate fines range from SEK 5 000 (approximately EUR 540) to SEK 10 million (approximately EUR 1.1 million) (s.8).[43] A conviction of the natural person who committed the crime is not needed to establish corporate liability (Penal code chapter 36, section 7.). Corporate liability does not preclude the possibility of parallel administrative or civil proceedings such as claims for damages against the legal person.

Criterion 3.11– There are appropriate ancillary offences to the ML offence. Chapter 23, section 4 of the Penal Code provides for a punishment of complicity, which covers aiding and abetting, as well as instigation. According to section 8 of the Act on Penalties Money Laundering Offences, attempt, preparation or conspiracy to commit a money laundering offence, a gross money laundering offence or non-petty commercial money laundering is punishable in accordance with Chapter 23 of the Swedish Penal Code.

41 The 2016 price base amount is SEK 44 300 which multiplied by five is SEK 221 500.

42 The day-fine is determined in number to at least 30 and at most 150, depending on the seriousness of the crime. Each day-fine shall than be imposed as a fixed amount from SEK 50 up to and including SEK 1 000, having regard to what is judged to be reasonable with account taken of the income, wealth, obligations to dependants and other economic circumstances of the accused. If special reasons exist, the amount of the day-fine may be adjusted, but the lowest total amount is SEK 750.

43 Sweden indicated that a Committee of Inquiry was tasked to conduct a broad review of corporate fine regulations and propose necessary legislative amendments. One of its main tasks was to consider and propose an increase in the maximum amount for corporate fines. The inquiry report was submitted on 29 November 2016.

Weighting and Conclusion:

Sweden meets most criteria of R.3. Nonetheless, the sanctions against legal persons are not sufficiently dissuasive.

Sweden is largely compliant with R.3.

Recommendation 4 – Confiscation and Provisional Measures

In its 3rd MER, Sweden was rated largely compliant with regard to confiscation and provisional measures. 'e report concluded that confiscation and related provisions needed to be used more effectively, and there should be a greater focus on taking action to seize and confiscate the proceeds of crime - both issues which are now considered as part of the effectiveness assessment.

*Criterion 4.1***–** Sweden has a broad set of legal powers to deprive criminals of their proceeds or instrumentalities. The Act on Penalties for Money Laundering Offences, s. 9-11, contains provisions for confiscation of laundered property, and for property of corresponding value. Proceeds (including income or other benefits derived from such proceeds or of corresponding value) from predicate offences can be confiscated under different laws applicable to that specific offence (e.g. chapter 36, s.1 and 1c of the Penal Code or the Act on Penalties for Narcotics Crimes). Funds linked to the financing of terrorism can also be confiscated using separate provisions in section 7 of the Act on Criminal Responsibility for the Financing of Particularly Serious Crime in Some Cases.

Property will be confiscated unless it is "manifestly unreasonable". According to the preparatory works (Government Bill 2013/14:121, p. 117), an assessment of "manifestly unreasonable" should consider the value of the property in relation to the seriousness of the crime, and the financial situation of the perpetrator. In practice, the exemption is a narrow one, for example to avoid that a perpetrator who do not own or control the proceeds is subjected to a huge confiscation decision which realistically could never be recovered.

For TF, the Swedish authorities have indicated that the presumption is that confiscation should be carried out, but the measure may be waived if there is a strong reason against such a confiscation. *The Act on Criminal Responsibility for the Financing of Particularly Serious Crime in Some Cases* (2002:444) provides that property shall be confiscated unless manifestly unreasonable.

Criterion 4.2– Law enforcement agencies have the authority to take a range of measures to identify, trace and secure property that is necessary to investigate crime or which might become subject to seizing measures, or which is suspected to originate from criminal activity (Chapters 27 and 28 of the Code of Judicial Procedure; Chapter 1, section 11 of the Banking and Financing Business Act; Chapter 3, section 1 of the AML/CFT Act) (see further under Recommendation 31). Chapter 8, sections 8 and 9 of the AML/CFT Act regulate Prohibitions on Disposal of Property (PDPs). The purpose of these measures is to be able to act to prevent the flight or dissipation of assets, prior to a concrete crime having been established or a criminal investigation having begun. PDPs concern a financial institution's or DNFBP's property in the form of funds, debt or other claims, which are suspected to relate to ML/TF and which may not be moved or disposed of.

Criterion 4.3– Laws and other measures in Sweden provide protection for the rights of bona fide third parties. Such protection is consistent with the standards provided in the Palermo Convention. Forfeiture of property may only apply to the persons mentioned in section 11 of the Act on Penalties for Money Laundering Offences , which encompasses a wider circle of persons than Chapter 36, section 5 (a)–(d) of the Penal Code.

Criterion 4.4– Proceeds related to ML and TF are covered by Section 12 of the Act on Penalties for Money Laundering Offences and section 8 of the Act on Criminal Responsibility for the Financing of Particularly Serious Crime in Some Cases. Chapter 27, sections 8 b to 13, of the Code of Judicial Procedure covers how to handle cash and securities seized and how they can be disposed of. Sweden has arrangements for securing physical property seized, including cash and securities, but appears to have no established mechanisms or procedures for managing all seized or confiscated assets, including (potentially) income-generating or perishable assets.

Weighting and Conclusion:

Sweden meets most of the requirements for R.4, except the need for having mechanisms or procedures to manage seized and confiscated property.

Sweden is largely compliant with R.4.

Recommendation 5 – Terrorist Financing Offence

Sweden's 2006 assessment rated it largely compliant with SR.II. The deficiencies identified were that the law did not specifically criminalise the collection or provision of funds in the knowledge that they are to be used (for any purpose) by a terrorist organisation or an individual terrorist; and that the sanctions available were not effective, dissuasive, and proportionate.

Currently the basis for Sweden's TF offence is the Act on Criminal Responsibility for the Financing of Particularly Serious Crime in some cases (2002:444), which entered force in July 2002. In April 2016amendments to the Act entered into force (through Government Bill 2015/16:78) which intended to address the requirements on the financing of a terrorist organisation or an individual terrorist for any purpose.

Criterion 5.1 - The TF offence covers all of the terrorist acts described in article 2(a) and 2(b) of the TF convention. (2002:444, s3)

Criterion 5.2 -The TF offence covers collecting, providing, or receiving funds with the knowledge or intention that they will be used to commit particularly serious crime, such as terrorist offences, or "*by a person or persons forming an association that commit particularly serious crime or are guilty of attempt, preparation, conspiracy to commit or complicity in such crime*". There is no need for a link to a specific planned or executed terrorist act. This brings the offence into line with the requirement to criminalise funding a terrorist organisation or an individual terrorist even in the absence of a link to a terrorist act. (2002:444, s3, second para., letter (b)).

Criterion 5.3 - The TF offence applies to all funds, whether from a legitimate or illegitimate source. (2002:444, s3)

Criterion 5.4 - The TF offence does not require that the funds were actually used to carry out a terrorist act or are linked to a specific terrorist act. (2002:444, s3)

Criterion 5.5 - As a general principle of Swedish criminal law, the intent and knowledge required to prove the offence can be inferred from objective factual circumstances.

Criterion 5.6 - Natural persons convicted of TF are punishable with imprisonment for up to six years. The scale of punishment is divided into different brackets providing for different penalties depending on the severity of the crime: in petty cases, punishment is not imposed. "Normal" cases are punishable with imprisonment for up to two years, and gross cases (those which are part of an activity carried out on a large scale or are otherwise of a particularly dangerous kind) are punishable with imprisonment for between six months and six years. Internationally, the sanctions available in Sweden are at the bottom of the range available in other FATF and FSRB members. However, sanctions for TF are consistent with the sanctions applied for other comparable crimes in Sweden: the same range of penalties applies for money laundering or for public provocation, recruitment, or training for terrorism. While terrorist acts are punishable with 4 years to life imprisonment, there is a penalty of 2 to 6 years for less serious terrorist acts - the same range as for gross cases of terrorist financing.

Criterion 5.7 - Criminal liability and sanctions can be applied to legal persons, as noted above in the assessment of criterion 3.10. It is not clear whether the level of sanctions which can be applied to a legal person convicted of TF (a maximum of SEK 10 million – approximately EUR 1.1 million) would be proportionate and dissuasive in the absence of parallel criminal, civil, or administrative proceedings. (Penal Code chapter 36 s. 7-10).

Criterion 5.8 -A full range of ancillary offences are available including: attempt (which is explicitly criminalised in the TF offence (2002:444, s4)); and general provisions on complicity (Penal code, chapter 23, s4), which establish criminal responsibility for aiding, abetting, and instigation. Complicity therefore also encompasses the conduct of aiding and abetting an offence; participation in an offence; and contributing to the commission of an offence by a group of persons acting with a common purpose.

Criterion 5.9 - TF offences are predicate offences for ML.

Criterion 5.10 - The TF offence is applicable regardless of whether the person committing the offence is in the same country as the relevant terrorist, terrorist organisation, or terrorist act.

Weighting and Conclusion:

Sweden is largely compliant with R.5.

Recommendation 6 – Targeted Financial Sanctions Related to Terrorism and Terrorist Financing

In its 2006 evaluation, Sweden was rated as Partially Compliant with former SR.III. Issues identified were the lack of a national mechanism to give effect to freezing requests from other countries or to freeze the assets of EU internal terrorists; the lack of guidance to financial institutions and DNFBPs;

lack of clarity about the scope of freezing obligations resulting from the TF offence; and potential mismatch in the definition of funds.

Sweden implements asset freezing obligations through EU regulations, which have direct legal effect in Sweden. The same legal framework remains in place as in 2006: UNSCR 1267/1988 (on Afghanistan) is implemented through EU Regulation 753/2011 and Council Decision 2011/486/CFSP. UNSCR 1267/1989 (on Al Qaida) is implemented through EU Regulation 881/2002 (and successors) and Common Position 2002/402/CFSP. TFS pursuant to UNSCR 1373 are implemented at EU-wide level, through EU Regulation 2580/2001 and Common Positions 2001/930/CFSP and 2001/931/CFSP.

Criterion 6.1 - In relation to designations under UNSCR1267, Sweden has not formalised arrangements for identifying and proposing designations to the UN Sanctions Committees. A Swedish proposal to the UN to designate a person or entity would ultimately be made by the Ministry for Foreign Affairs, following consultation with other relevant ministries and using information from police authorities. This inter-agency consultation would also consider whether the required evidentiary standard (reasonable grounds) was met. Proposals do not appear to be conditional on the existence of criminal proceedings.

In practice, Swedish authorities would consider whether each person or entity should be proposed to the applicable UN Sanctions Committee, or to the EU Working Group responsible for EU designations under CP 931. Swedish authorities indicate that they would follow the procedures and forms of the Sanctions Committees; would provide relevant information; and would specify whether their status as a designating state may be made known. However, it is not possible to verify this, since Sweden has not proposed or co-sponsored any designations since 2002, and does not have either formal procedures or informal mechanisms or practices at national level for considering or proposing designations.

Criterion 6.2 - Sweden implements designations pursuant to UNSCR 1373 through an EU mechanism, based on EU Regulation 2580/2001 and Common Positions 2001/930/CFSP and 2001/931/CFSP. *At national level* the same interagency consultation process noted above would consider potential proposals for designation, which could be made either by the UN or by the EU. *At European level*, the Council of Ministers is the competent authority for making EU designations under UNSCR 1373, based on analysis by the CP931 Working Group, using designation criteria consistent with those in Resolution 1373. The Working Group uses a "reasonable basis" evidentiary standard and designation is not conditional on the existence of criminal proceedings. There are no formal mechanisms for requesting freezing action by other countries either at national or European level, although designations by the EU have direct effect in all 28 EU member states. All designations must include sufficient information to identify the person being designated and exclude those with similar names.

Criterion 6.3 -

(a) At national level, information used in considering designations would principally have been collected by intelligence authorities, including the Security Service. Information collected by law enforcement authorities could be used as a basis for designation, however, their powers to use coercive measures are restricted to the investigation of serious crimes, or where there is significant risk that a person might engage in criminal activity. At EU level, all EU Member

States are required to provide each other with the widest possible range of police and judicial assistance in these matters, inform each other of any measures taken, and cooperate and supply information to the relevant UN Sanctions Committee.

(b) According to EC Regulation 1286/2009 preamble para.5, designations take place without prior notice to the person/entity identified. For asset freezing, the Court of Justice of the EU makes an exception to the general rule that notice must be given before the decision is taken in order not to compromise the effect of the first freezing order. The listed person or entity has the right to appeal against the listing decision in Court, and seek to have the listing annulled.

Criterion 6.4 - In the EU framework, implementation of targeted financial sanctions (TFS), pursuant to UNSCRs 1267/1989 and 1988, does not occur "without delay." Because of the time taken to consult between European Commission departments and translate the designation into all official EU languages, there is often a delay between when the designation and freezing decision is issued by the UN and when it is transposed into EU law under Regulation 881/2002. As regards Resolution 1988, similar issues arise when the Council transposes the decision under Regulation 753/2011. An expedited procedure has been adopted by the Commission for implementation of new listings required by for UNSCR 1989 transposed under EU Regulation 881/2002. This expedited procedure ensures that new listings to come into effect faster and the gap between publication of new designations by the UN and EU transposition has closed to an average of 9 working days from the UN decision. In 2015, transposition times ranged from 4 to 12 days for Resolution 1989 designations, and from 15 days to over four months for Resolution 1988 designations. This is still not consistent with the requirement to implement sanctions without delay. Sweden is considering implementing "bridging measures" at national level to address this issue and has established a committee to prepare legislative proposals by November 2016.

For resolution 1373, TFS are implemented without delay because, once the decision to freeze has been taken, Council Regulation 2580/2001 is immediately applicable to all EU Member States.

Criterion 6.5 -

(a) For UNSCRs 1267/1989 and 1988, EU regulations transposing UNSC decisions are directly applicable in all EU Member States on the day of publication in the EU's Official Journal. There is an obligation on all natural and legal persons to freeze all funds, financial assets, or economic resources of all designated persons and entities (irrespective of their nationality). However, the delays noted above in transposing UN designations into EU Regulations can result in de facto prior notice to the persons or entities in question.

For UNSCR 1373, the obligation for natural and legal persons to freeze the assets of designated persons derives automatically from the entry into force of EU regulation, without any delay and without notice to the designated individuals and entities. Regulation 2580/2001 applies to all persons; however "EU internal terrorists" are not subject to the freezing measures of Common Position 2001/931/CFSP, but only to police and legal co-

operation measures[44]. This leaves a gap in EU implementation of TFS pursuant to UNSCR 1373. The 2007 Treaty of Lisbon (Art.75) provides a legal basis for a possible EU administrative measure to allow for the freezing of funds of persons related to terrorist activities inside the EU; however, legislation to establish such a framework has not yet been initiated.

(b) For UNSCRs 1267/1989 and 1988, the freezing obligation extends to all funds/other assets that belong to, are owned, held or controlled by a designated person/entity. The obligations to freeze the funds or assets of persons and entities to be frozen when acting on behalf of, or at the direction of, designated persons or entities is met by the requirement to freeze funds or assets "controlled by" a designated entity, which extends to persons acting on their behalf in relation to those funds: EU Council Regulation 881/2002 article 2 (2).

For UNSCR 1373, the freezing obligation in EU regulation 2580/2001 art.1(a) and art.2(1)(a) applies to assets belonging to, owned, or held by the designated individual or entity, and does not apply directly to funds or assets controlled by-, or indirectly owned by-, or derived from assets owned by-, or owned by a person acting at the direction of- a designated person or entity. However, EU regulation 2580/2001 also includes provisions empowering the Council to designate any legal person or entity controlled by a designated individual or entity, or a natural person acting on behalf of a designated entity (Art.2(3) (iii) and (iv)). This largely addresses the gaps.

(c) EU nationals and persons within the EU are prohibited from making funds and other assets available to designated persons and entities: EU Council Regulation 881/2002 (article 2 (2)), 1286/2009 (article 1(2)), 753/2011 (article 4) and 754/2011 (article 1).

(d) EU designations are published in the EU Official Journal and website, and included in a consolidated financial sanctions database maintained by the European Commission, with an RSS feed. Since April 2015; the relevant data are produced using a new application called FSD ("Financial Sanctions Database") with new technical features. There are no separate national-level communications mechanisms.

(e) Natural and legal persons (including FIs/DNFBPs) are required to immediately provide any information about accounts and amounts frozen (articles 5.1 of EU Regulation 881/2002, 4 of EU Regulation 2580/2001, 8 of EU Regulation 753/2011).

(f) Articles 6 of EC Regulation 881/2002, 7 of EC Regulation 753/2001, 4 of Regulation 2580/2001 protect the rights of bona fide third parties acting in good faith when undertaking freezing actions.

[44] "EU internal terrorists" are persons or entities within the EU involved in terrorist activities and with no links to international terrorism. This is not the same as EU citizens. Designation of an EU citizen is possible under the existing mechanisms if they linked to terrorist activities posing a threat to international peace and security. The limitation of the existing mechanisms to such forms of terrorism is based on the use of the EU Common Foreign and Security Policy (CSFP) mechanisms as the basis for action under 1373, since action under the CSFP in this domain is mainly directed at preserving international peace and security.

Criterion 6.6-

(a) For designations under UNSCRs 1267/1989 and 1988, Sweden uses the procedures of the UN Sanctions Committees to handle de-listing requests. There are also procedures to seek de-listing through the European Council (for designations under UNSCR 1988) or Commission (for 1989).

(b) For 1373 designations, amendments to Regulation 2580/2001 are immediately effective in all EU Member States. De-listing may occur ad-hoc (if there are no longer grounds for keeping a person or entity in the CP931 list) or as a result of the mandatory six-monthly review of all listings.

(c) A listed individual or entity can write to the Council to have the designation reviewed or can challenge the relevant instrument in Court (based on the Treaty on the Functioning of the European Union (TFEU), article 263 (4)). TFEU Article 275 also allows legal challenges of a relevant CFSP Decision.

(d) (e) Listed individuals and entities are notified about the listing, its reasons and legal consequences, their rights of due process, and the applicable de-listing procedures. These include the availability of the ombudsperson (for designations under UNSCR 1988) and focal point (for designations under UNSCR 1989). Sweden has in the past actively assisted in de-listing procedures, as well as the procedures at EU level for de-listing, unfreezing, and allowing a review of the designation by the European Commission or the Council.

(f) According to the EU Regulations 881/2002 and 2580/2001, upon verification that the person/entity involved is not designated, the funds/assets must be unfrozen.

(g) De-listing and unfreezing decisions taken in accordance with European regulations are published in the Official Journal of the EU and the updated list of designated persons and entities is published on a dedicated site.

Criterion 6.7 - At the EU level, there are mechanisms for authorizing access to frozen funds or other assets which have been determined to be necessary for basic expenses, the payment of certain types of expenses, or for extraordinary expenses, per articles 2a of EU Regulation 881/2002, EU Regulation 753/2011, and 5–6 of EU Regulation 2580/2001.

Weighting and Conclusion:

Sweden is partially compliant with R.6.

Recommendation 7 – Targeted Financial Sanctions Related to Proliferation

This recommendation was added to the standard in 2012. Sweden has therefore not previously been assessed against this recommendation. As a member of the EU, Sweden relies upon the EU framework[45] for implementation of R.7.

Criterion 7.1 - R.7 requires implementation of proliferation-related targeted financial sanctions (TFS) to occur without delay—a term that, in this context, is defined to mean "ideally, within a matter of hours." The EU regulations require all natural and legal persons within the EU to freeze the funds/other assets of designated persons/entities. This obligation is triggered as soon as the regulation is approved and the designation published in the Official Journal of the European Union.

There were initially delays of several months in transposing new UN designations into EU Regulations, following the adoption of UNSCRs 1718 and 1737 in 2007, and subsequent delays in updating the EU list following changes to the UN lists. However with respect to TFS against Iran, on both of the two occasions since 2007 when the list of persons and entities designated by the UN was expanded, the additional persons and entities had previously been designated by the EU. Their designation by the UN had the effect - within the EU regulation - of moving those persons and entities from Annex IX ("the EU Annex") to Annex VIII ("the UN Annex"). For TFS against DPRK, the most recent additions to the UN list of sanctioned persons and entities, made through UNSCR 2270 (2016) were transposed into the applicable decision by the Council of the European Union within two days of their designation by the UN. Delays in transposition have therefore not had any practical effect on either sanctions regime in recent years.

In addition, there is an EU authorisation process imposing comprehensive controls on transfers of funds between the EU and Iran, including prior authorisation (in Art. 30 of Regulation 267/2012, implementing the financial vigilance provisions of UNSCR 1929), and activity-based prohibitions. While these requirements implement different UN obligations and go beyond the scope of R.7, they could potentially also prevent the execution of transactions with designated persons and entities during the period between their UN listing and the EU transposition.

Criterion 7.2 - Responsibilities for implementation of targeted financial sanctions against Iran and DPRK are assigned to independent Government agencies - including the Financial Supervisory Authority, the Social Insurance Agency, and the Inspectorate for Strategic Products, based on their standard competencies. There are arrangements in place for coordination between the different agencies responsible for implementation, as set out under criterion 2.4 above.

(a) European regulations are applicable to all natural persons who are EU citizens and to all legal persons established or formed under the law of a Member State or associated with a commercial transaction carried out in the EU (Regulation 267/2012, Art. 49 and Regulation 329/2007, Art. 16). The freezing obligation is activated upon publication of the Regulations in the Official Journal of the EU. The delays in transposition described above raise the question

[45] UNSCR 1718 on the Democratic People's Republic of Korea (DPRK) is transposed into the EU legal framework through Council Reg. 329/2007, Council Decisions (CD) 2016/319/CFSP, 2013/183/CFSP, and CD 2010/413. UNSCR 1737 on Iran is transposed into the EU legal framework through Council Reg. 267/2012.

of compliance with the obligation to execute freezing measures 'without prior notice', which deprives the EU regulations of any surprise effect, unless entities are previously listed by the EU.

(b) The freezing obligation applies to all types of funds.

(c) The regulations prohibit making available, directly or indirectly, funds or economic resources to designated persons or entities or for their benefit, unless otherwise authorised or notified in compliance with the relevant UN resolutions (Regulation 329/2007 Art. 6.4 and Regulation 267/2012 Art. 23.3).

(d) The lists of designated persons and entities are communicated to financial institutions and DNFBPs through the publication of a consolidated list on the EU site is available and can be downloaded at: http://eeas.europa.eu/cfsp/sanctions/consol-list/index_en.htm. Such publication constitutes a notification to all addresses of the requirements. Guidance to financial institutions and DNFBPs and others who may be holding targeted funds or other assets is publicly available.

(e) Financial institutions and DNFBPs must immediately provide to the competent authorities all information that will facilitate observance of the EU Regulations, including information about the frozen accounts and amounts (Regulation 329/2007, Art. 10 and Regulation 267/2012, Art. 40).

(f) The rights of bona fide third parties are protected by the relevant EU Regulations (Regulation 329/2007, Art. 11 and Regulation 267/2012, Art. 42).

Criterion 7.3 -EU Member States are required to take all necessary measures to ensure that the EU Regulations on this matter are implemented and to determine a system of effective, proportionate and dissuasive sanctions (Regulation 329/2007, Art. 14 and Regulation 267/2012, Art. 47). Sweden's Financial Supervisory Authority, as part of its regular supervision, investigates whether regulated entities have an adequate basis for compliance with the EU Regulations; potentially with support from a specialised section within the Security Service in case of suspected breaches. Breaches of TFS can and have been prosecuted as criminal cases under the Act on Certain International Sanctions (1996:95). In addition, the FSA can apply its range of administrative sanctions (as set out under R.35) in cases of inadequate compliance with the EU Regulations. The FSA has issued instructions, fines, and revoked a company's authorisation in relation to inadequate implementation of EU Regulations.

Criterion 7.4 -The EU Regulations contain procedures for submitting de-listing requests to the UN Security Council for designated persons or entities that, in the view of the EU, no longer meet the criteria for designation. The EU Council of Ministers communicates its designation decisions and the grounds for listing, to designated persons/entities, which have the right to comment on them, and to request a review of the decision by the Council. Such a request can be made regardless of whether a de-listing request is made at the UN level (for example, through the Focal Point mechanism). Where the UN de-lists a person/entity, the EU amends the relevant EU Regulations accordingly. There are specific provisions for authorising access to funds or other assets, where the competent authorities of Member States have determined that the exemption conditions set out in resolutions 1718 and

1737 are met, and in accordance with the procedures set out in those resolutions[46]. There are no specific provisions at Swedish level to unfreeze the funds of "false positives", but informal dialogue with banks has been used to resolve such cases, and is (in principle) supported by a mechanism at the EU Council of Ministers. Sweden has not developed or implemented measures at national level, since no Swedish nationals or Swedish companies have been designated.

Criterion 7.5- The EU Regulations permit the payment to the frozen accounts of interests or other sums due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution, provided that these amounts are also subject to freezing measures (Regulation 329/2007, Art. 9 and Regulation 267/2012, Art. 29). Provisions in the EU Regulations also authorise the payment of sums due under a contract entered into prior to the designation of such person or entity, provided that this payment does not contribute to an activity prohibited by the regulation, and after prior notice is given to the UN Sanctions Committee (Regulation 267/2012, Art. 24 and 25).

Weighting and Conclusion:

Sweden is partially compliant with R.7.

Recommendation 8 – Non-Profit Organisations

Sweden's 2006 evaluation rated it as PC with SR.VIII on NPOs. However, that assessment pre-dated the adoption of the Interpretive Note to SR.VIII, so Sweden has not previously been assessed on the detailed requirements of R.8.

NPOs in Sweden can take several different legal forms, including limited companies, foundations, religious communities, and non-profit associations[47], each of which is subject to separate legal obligations. The NPO sector includes over 148,000 individual NPOs, of which about 80% by number are Non-Profit Associations (NPAs), and about 17% are foundations. However, many NPAs and foundations are used for non-charitable purposes (including to manage common or shared assets, conduct commercial activity, sports associations, trade unions, managing pension obligations etc.) and are not NPOs according to the FATF definition[48]. Because the legal forms used include both charitable and non-charitable entities, it is not possible to give precise figures for the size of the charitable sector in Sweden - though NPAs, foundations, and religious groups all conduct significant charitable fundraising activity.

Criterion 8.1- Sweden conducted a review of the NPO sector in 2008. This included a mapping of the NPO sector (including its size, activities, and other relevant features, an assessment of ML/TF risks and the adequacy of laws, and recommendations for the policy response - several of which have since been acted upon. The risks posed by NPOs were also considered in the 2014 TF national risk

46 EU Regulation 329/2007 articles 7 and 8, and EU Regulation 267/2012 articles 24, 26, and 27.

47 Note that Swedish law provides for a distinct type of legal person named a "Non-Profit Association" - which is distinct from the FATF definition of a non-profit organisation. See R.24 for more information.

48 Swedish authorities estimate that about 24% of foundations are NPOs according to the FATF definition.

assessment, and 'Fundraising for Beneficiaries Abroad' was identified as a high risk area for TF in the national AML/CFT strategy. An exercise is planned for 2016 which will focus on TF risks to the NPO sector.

Criterion 8.2- The Swedish Government's Coordinating Supervisory Body has launched an educational project with the purpose of raising awareness and promoting knowledge of TF in consultation with authorities, financial institutions and DNFBPs. NPOs are also represented on the joint party forum which disseminates information about TF risks, administered by the Swedish Agency for Youth and Civil Society.

Criterion 8.3- Sweden has clear systems to promote transparency, integrity, and public confidence in the administration and management of NPOs. However these systems are self-regulatory in nature and participation by NPOs is voluntary, with only a relatively small number of NPOs choosing take part.

- Swedish Fundraising Control (SIK), a non-profit organisation, provides payment services to NPOs through direct debit accounts beginning with the number "90". SIK approves and supervises all NPOs using such accounts, and applies requirements relating to transparency and integrity. In addition, the Fundraising Council for Volunteering Organisations (FRII) has established a code of good industry practices for its members. Currently SIK has 423 accounts, and FRII has 145 members (out of a total of 100,000+ NPOs).
- Foundations are subject to regulations under the Foundations Act (1994:1220), and to provisions under the Accounting Act (1999:1078).
- The Swedish International Development Agency (SIDA) applies additional requirements to any NPOs which administer aid projects on its behalf or receive funding from it, including transparency about the use of aid.

Criterion 8.4 - Different mechanisms and obligations apply to different types of NPO.

(a) Associations established as limited companies are established through a memorandum of association (which includes information on the purpose, operations, and the identity of their directors), and are required to register with the Swedish Companies Registration Office (SCRO). Foundations are regulated by the Foundations Act (1994:1220), which requires most types of foundations[49] to be registered with and supervised by the relevant County Administrative Board. Registration includes articles of association, a description of the purpose of the foundation, and identity information on directors. Unregistered foundations are not required to have all the information set out in this sub-criterion. Religious Communities are governed by the Religious Communities Act (1998:1593), and the Ordinance on Registration of Religious Communities (1999:731) which requires them to be registered with the Legal, Financial and Administrative Services Agency. Information registered includes the identity information of a representative, and must be signed by all members of the organisation's decision-making body. Finally, Non-Profit Associations are not

[49] Foundations that benefit specific natural persons are exempt, and overall about one third of foundations are estimated to be unregistered.

specifically required to register - although they may be required to seek an organisation number from the Swedish Tax Agency (STA) or (if they engage in trade) to register with the Companies Registration Office.

(b) (c) The Accounting Act requires annual accounts to be submitted by limited companies, economic associations, foundations with more than SEK 1.5 million (EUR 160,000) in assets or which are fundraising or involved in trade; religious communities, and non-profit associations which have legal personality. In the case of limited companies and foundations, these accounts must be audited (with relaxed requirements for smaller foundations and exemptions for small companies). Auditing requirements do not apply to religious communities, and non-profit associations, and for other NPOs, do not necessarily consider whether funds are spent in a manner that is consistent with NPO's purpose and objectives.

(d) As noted under (a) above, most types of NPOs are registered with one or more authorities including the Tax Agency (STA); Companies Registration Office (SCRO); Development Agency (SIDA); Swedish Fundraising Control (SIK); Legal, Financial and Administrative Services Agency; or one of seven County Administrative Boards (CABs).

(e) There is no explicit requirement for NPOs to know their beneficiaries and associated NPOs, but some NPOs do have obligations (e.g. through the SIDA and SIK systems) to actively control the identity, references and reputation among the recipients of fund and their partners.

(f) The Accounting Act (1990:1078) requires retention of accounting information and financial statements for 7 years. There is no obligation to preserve identity information on purpose, objectives, and directors.

Criterion 8.5- There is no single authority responsible for monitoring compliance by NPOs. The relevant registries (noted under 8.4(d)) can monitor compliance with registration and reporting obligations - including the STA monitoring of specific tax regulations and County Administrative Board (CAB) monitoring of the requirements for foundations. The County Administrative Boards act as registering and supervisory authorities for foundations, and have the authority to request information from a foundation or request it to register, to conduct inspections, and to remove directors or impose conditional fines. Swedish Fundraising Control (SIK) and the Swedish Development Agency (SIDA) also monitor NPOs' compliance with their (voluntary) requirements, or which receive their funds. .

Criterion 8.6- The principal authorities involved in the investigation of NPOs are the FIU (Fipo); the Tax Agency (STA), the Economic Crime Authority (EBM), and the Security Service (Säpo). In cases where suspicious activity has been reported through STRs, FIPO analysis has been the basis for extensive supervision by STA and/or criminal investigation initiated by EBM. There appears to be a good basis for cooperation, coordination, and information-sharing between these three authorities; and law enforcement authorities have powers to access information on NPOs. It is not clear that mechanisms exist to identify at-risk NPOs and share information about them. Sweden has 12 registries which hold information on or oversee NPOs, but no coordination mechanism to share information or alerts between them. The FIU (through the STR system) appears to act as the central point for receiving and disseminating information on misuse of NPOs, but this may not be adequate as a basis for preventive action by supervisors or other authorities.

Criterion 8.7- Sweden uses regular international cooperation channels for requests regarding NPOs.

Weighting and Conclusion:

Sweden is largely compliant with R.8.

Recommendation 9 – Financial institution secrecy laws

In its 3rd MER, Sweden was assessed as largely compliant for R.4, as secrecy requirements were reported as negatively affecting the sharing of information by FIs. The *FATF Recommendations* in this area have not changed.

Criterion 9.1- Confidentiality requirements of the financial institution laws allow for information to be provided to competent authorities for domestic criminal investigations or in the case of MLAs. The *AML/CFT Act (2009:62)* gives the Police the right to receive upon request all necessary information to investigate ML/TF. The sharing of such information between Swedish authorities and with foreign authorities is governed by the *Public Access to Information and Secrecy Act (2009:400).*

However, the AML/CFT Act (2009:62), Ch.3, sect.4 stipulates that information from reviews of suspicious transactions cannot be shared with a third-party. It is the FSA's interpretation that this restriction could be overcome if all of an FI's business lines or group entities were to have the same Money Laundering Reporting Officer.

Weighting and Conclusion:

Sweden is largely compliant with R.9.

Recommendation 10 – Customer due diligence

In its 3rd MER, Sweden was rated partially compliant with R.5, due to various deficiencies in the CDD requirements.

Criterion 10.1- Financial institutions are not allowed to provide anonymous accounts or anonymous pass-books. There is an exemption for the activities regulated under the *Certain Consumer Credit-related Operations Act (2014:275), AML/CFT Act (2009:62) Ch.2 sect.14* as while those FIs do not maintain financial accounts for their clients, they have client relationships. However, this is a minor deficiency as this is a small sector, and their clients must have accounts with covered FIs.

*Criterion 10.*2- Financial institutions are obliged to undertake CDD measures in the required situations, but the obligation does not extend to occasional transactions that are wire transfers between €15,000 and €1,000 (below which is not required by the Standards). *AML/CFT Act (2009:62) Ch.2 sect.2.*

Criterion 10.3- Financial institutions are required to identify the customer using ID, register transcripts or via other reliable methods. *AML/CFT Act (2009:62) Ch.2 sect.3.* The FSA's directives

against ML and TF *(FFFS 2009:1 Ch.4 sect. 2-7)* lists identification data required and the methods of verification.

Criterion 10.4- Financial institutions are required to, in the course of identifying and verifying beneficial owners (which applies in cases where one natural person acts on behalf of another), check if persons are authorised to act on behalf of a customer that is a natural person such as through a power of attorney. For customers that are legal persons, that requirement is based on the fact that the register transcripts contain information on the persons that are authorised to sign for the company (or to issue a power of attorney). There is no requirement to verify the identity of the person acting on behalf of the customer. *AML/CFT Act (2009:62) Ch.2 sect.3.*

Criterion 10.5- Financial institutions are required to identify and verify beneficial owners using reliable information. The *Act* defines the beneficial owner as "*a natural person on whose behalf another person acts, or, in cases where the customer is a legal person, a person who exercises decisive influence over the customer*". This is broadly compatible with the FATF definition, and also encompasses cases where a natural person is acting on behalf of another. *AML/CFT Act (2009:62) Ch.2 sect.3, FFFS (2009:1) Ch.4 sect. 8-9.*

Criterion 10.6- Financial institutions are required to collect information about the nature and purpose of the business relationship. *AML/CFT Act (2009:62) Ch.2 sect.3.* The requirement to understand the purpose and intended nature of the business relationship is implied in the requirement in Ch.2 sect.10, according to which the FI, among other things, must control and document that the customers' activities correspond with the knowledge/understanding that the FI has.

Criterion 10.7- Financial institutions are required to conduct ongoing due diligence (which includes ensuring that transactions are consistent with information about the customer, including their business and risk profile, and where necessary, the source of their financial assets), and to keep documents, data, and CDD information up to date. *AML/CFT Act (2009:62) Ch.2 sect.10, FFFS (2009:1) Ch.4 sect. 16 - 17.*

Criterion 10.8- Financial institutions are required to investigate the customer's ownership and control structures when identifying the beneficial owner. However, the definition of beneficial owner only refers to persons and legal persons but not explicitly to legal arrangements (which are not recognised in Sweden, as noted in the analysis of R.25). As a beneficiary of a trust would be considered as a beneficial owner, this would imply that FIs would be required to investigate the ownership and control structures of trusts. *AML/CFT Act (2009:62) Ch.2 sect.3, Ch.1 sect.5*

Criterion 10.9- Customers that are a legal person are identified and verified as part of CDD through the legal person's registration certificate or corresponding sources. This does not explicitly apply to customers that are legal arrangements. Nevertheless, FIs have a general obligation to identify and verify their customers (which would apply even if they are a legal arrangement) using "ID-documentation, register transcripts or other reliable methods". *AML/CFT Act (2009:62) Ch.2 sect.3, Ch. 1 sect.5, FFFS (2009:1) Ch.4 sect. 5.*

Criterion 10.10- Financial institutions are required to identify and verify the beneficial owner. Sweden's definition of beneficial owner includes direct and indirect natural owners if the holding in

the customer amounts to more than 25 per cent, and natural persons who exercise decisive influence over the customer. The preparatory works to the legislation explain "decisive influence" as including "in any other way controls the management of the customer". This broad definition covers the scope of this criterion. *AML/CFT Act (2009:62) Ch.2 sect.3, FFFS (2009:1) Ch.4 sect. 8-9.*

Criterion 10.11- While there are no specific requirements for legal arrangements, FIs are in the course of their normal CDD required to identify and verify beneficial ownership, which in the case of clients that are trustees the FI will identify the beneficiaries. The preparatory works to the AML/CFT Act provide the example of beneficiaries or intended beneficiaries of a trust as the beneficial owners. This will however not result in identifying all trust-relevant parties, such as the settlor and protector (if any).

Criterion 10.12- The identification and verification of a life insurance beneficiary must take place in the context of the first claim payment or when any other right given by the insurance policy is transferred for the first time. But there is no requirement to obtain sufficient information concerning the beneficiary for when beneficiaries are designated by characteristics or by class or by other means. *AML/CFT Act (2009:62) Ch.2 sect.9.*

Criterion 10.13- CDD measures are required to be adapted to ML/TF risks and enhanced CDD measures are necessary if the ML/TF risk is high. In Sweden the beneficiary of a life insurance is determined to be the beneficial owner and will be a relevant risk factor in determining whether enhanced CDD measures are needed. However, there is no requirement that such enhanced measures include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary of life insurance. *AML/CFT Act (2009:62) Ch.2 sect.1 and 6.*

Criterion 10.14- Financial institutions are required to complete CDD before a business relationship is established or occasional transaction is processed, or if necessary to not disrupt the normal conduct of business and if the ML/TF risk is low, to complete CDD without delay after the establishment of the relationship. *AML/CFT Act (2009:62) Ch.2 sect 9.*

Criterion 10.15- Delayed verification is only possible if the ML/TF risk is low, and verification must still be completed in close relation to the establishment of the relationship, otherwise the relationship must be terminated. *AML/CFT Act (2009:62) Ch.2 sect 9 and 11.*

Criterion 10.16- Financial institutions are required to conduct ongoing due diligence on existing customer and business relationships consistent with this criterion. *AML/CFT Act (2009:62) Ch.2 sect.10, FFFS (2009:1) Ch.4 sect. 17.*

Criterion 10.17- Financial institutions are required to conduct enhanced CDD when ML/TF risks are higher. The prescribed enhanced measures include measures to determine the origin of assets; enhanced ongoing supervision of the business relationship, and requiring approval from management. *AML/CFT Act (2009:62) Ch.2 sect.6, FFFS (2009:1) Ch.3 sect. 2.*

Criterion 10.18- The *AML/CFT Act (2009:62) Ch.2 sect.5* lists categories of entities exempt from basic CDD and ongoing monitoring, where the list is not based on an identification of lower risks through an adequate analysis of risks by Sweden or FIs. Where the ML/TF risk is high, or where the customer is a PEP, enhanced CDD has to be applied. This would mean that FIs are required to apply some CDD measures (but not ongoing monitoring) in all cases to identify whether the customer is high risk or a

PEP. *AML/CFT Act (2009:62) Ch.2 sect. 6 and 6a.*Where a customer in a listed category is not high risk or is not a PEP, the exemptions are not required to be commensurate with the level of lower risks.

Criterion 10.19- Financial institutions may not establish or maintain business relationships, or conduct occasional transactions, where CDD cannot be completed. If ML/TF can be suspected, an STR should be filed. *AML/CFT Act (2009:62) Ch.2 sect.11.*

Criterion 10.20- FIs are permitted to execute suspicious transactions (even if CDD cannot be completed) if refraining might hinder further investigations, where they should file an STR immediately. AML/CFT Act (2009:62) Ch. 3, sect. 1.

Weighting and Conclusion:

There are small scope deficiencies in 10.1 and 10.2, as well as other shortcomings with respect to CDD for legal arrangements, in the context of life insurance, and in the exemption of some categories of entities from basic CDD and monitoring.

Sweden is largely compliant with the R.10.

Recommendation 11 – Record-keeping

In its 3rd MER, Sweden was rated as largely compliant with R.10, with the deficiency that there was no law or regulation that customer records be made available on a timely basis.

Criterion 11.1- Financial institutions are required to keep records of all business transactions for 7 years from the date of the transaction. *Accounting Act Ch.4 sect.1, Ch.7 sect.2.*

Criterion 11.2- Financial institutions are required to maintain documents and information on CDD measures for at least 5 years from the date the measures were undertaken, or from the end of the business relationship. This means that every document that the FI has acquired from the customer and other sources as well as all the information that has been documented by the FI during the CDD process has to be kept. This would include the analysis or decisions made by the FI during the on-boarding of the customer. *AML/CFT Act (2009:62) Ch.2 sect.13, Ch.3 sect.1b*

Criterion 11.3- Financial institutions are required to keep detailed information about the business transaction to be kept, including "information regarding documents or other information that constituted the basis for the transaction" which permits reconstruction of transactions. *Accounting Act Ch.5 sect.6 and 7.*

Criterion 11.4- Financial institutions are required to provide any information deemed necessary for an ML/TF investigation without delay upon request from the Police Authority. The FSA and DNFBP supervisors also have access to the FIs' and DNFBPs' CDD information pursuant to the rules governing its supervision powers in the different laws governing the FIs (see R.27) and DNFBPs (see R.28), while the Police Authority's and the prosecutors' right to receive information from the FIs and DNFBPs is described in R.9. AML/CFT Act (2009:62) Ch.3 sect.1, FFFS (2009:1) Ch.4 sect.18.

Weighting and Conclusion:

Sweden is compliant with R.11.

Recommendation 12 – Politically exposed persons

In its 3rd MER, Sweden was rated non-compliant with R.6. Since then, the FATF standards have changed.

Criteria 12.1 and 12.2- Sweden makes no distinction between domestic and foreign PEPs. FIs are required to determine if the customer or beneficial owner can be considered a PEP, and if so, to undertake enhanced CDD measures as well as determine the origin of assets, conduct enhanced ongoing supervision, and obtain senior management approval. Assets are intended to capture both the "source of wealth" and the "source of funds" of the PEP. The term "asset" means "anything of value" in a broad way. When a person ceases to perform functions related to being a PEP, enhanced measures continue to be necessary for at least 18 months and until the person is no longer associated with high ML/TF risks. However, the definition of PEPs does not include senior government officials. *AML/CFT Act (2009:62) Ch.1 sect.5, Ch.2 sect.3, 6a, 7 and 7b.*

Criterion 12.3- The requirements for family members and close associates are met, except when the PEP is not considered to constitute a risk for ML/TF, where the requirements of c.12.1 (b) to (d) are not applied. The list of family member consists of spouses, registered partners, cohabitant partners, children and their spouses, registered spouses or cohabitant partners, or parents of the PEP. *AML/CFT Act (2009:62) Ch.2 sect.7a.*

Criterion 12.4- While there are requirements for the identification and verification of life insurance beneficiaries, who are considered the beneficial owner of the life insurance and would be assessed if they were PEPs, there are no specific requirements in relation to beneficial owners of beneficiaries. AML/CFT Act (2009:62) Ch.2 sect.9.

Weighting and Conclusion:

There is a gap in the definition of PEPs with respect to senior government officials, as well as in the identification of beneficial owners for life insurance.

Sweden is largely compliant with R.12.

Recommendation 13 – Correspondent banking

In its 3rd MER, Sweden was rated non-compliant with R.7.

Criterion 13.1- The requirements of c.13.1 (a) to (d) are necessary for cross-border transactions between Swedish credit institutions and institutions outside the EEA, on the basis that section 6 of the *AML/CFT Act* requires all transactions with non-EEA credit institutions to be treated as high-risk (unless the circumstances of the individual case indicate the contrary). If the circumstances indicate low ML/TF risk, there is no requirement for enhanced CDD. The enhanced CDD requirements also do

not apply to correspondent banking and other similar relationships within the EEA. In those cases normal CDD measures apply. If the FI were to conclude that the risk of ML/TF is high, also if the respondent is an EU FI, it would be obliged to take enhanced CDD measures. *AML/CFT Act (2009:62) Ch.2 sect.6 and 8.*

Criterion 13.2- Financial institutions are required to ascertain that the counterpart conducts CDD and ongoing monitoring on those customers, and is able to provide relevant customer data on request. However, the same issues as c.13.1 apply here. *AML/CFT Act (2009:62) Ch.2 sect.6 and 8.*

Criterion 13.3- Financial institutions are prohibited from establishing or maintaining relations with shell banks or with credit institutions that allow their account to be used by shell banks. AML/CFT Act (2009:62) Ch.3 sect.3.

Weighting and Conclusion:

FIs are allowed to not apply the requirements for cross-border correspondent banking if the ML/TF risk is low. FIs are also not required to apply the specific requirements in 13.1 to correspondent banking and other similar relationships within the EEA, although this is slightly mitigated by the requirement to conduct enhanced CDD in cases of high ML/TF risk.

Sweden is largely compliant with R.13.

Recommendation 14 – Money or value transfer services

In its 3rd MER, Sweden was rated as partially compliant with SR.VI. As an EU country, Sweden's *Payment Services Act* ("PSA") is based on the *EU Payment Services Directive* (2007/64/EC), but differs in that it also includes within its definition of payment service providers ("PSPs") branches of credit institutions from outside the EEA.

A company in Sweden providing payment services outside of Sweden and the EEA and not in an EEA currency is also subject to the PSA. *PSA (2010:751) Ch.3 sect.23*. A PSP may, after receiving a license from the FSA, set up a branch in a country outside the EEA. Applications sent to the FSA must contain a plan for the intended operation with information on the branch organisation and the services it intends to provide, and information on which country the branch will be established in and information on the branch's address and liable management.

Criterion 14.1- PSPs in Sweden (both foreign and domestic) are required to be licensed or registered. Some categories of licenced FIs are able to provide payment services without a separate licence. PSPs licenced in other EEA countries do not require a licence in Sweden, but the home supervisor must first notify the FSA of the PSP. *PSA (2010:751) Ch.2 sect.1, 2 and 3, Ch.3 sect.26 and 27.*

Criterion 14.2- The FSA partners with the Swedish Companies Registration Office to identify legal persons that operate a MVTS without a licence or registration. The Swedish Companies Registration Office notifies companies that in its description of operations stipulate payment services or banking services etc. that a registration or licence is required by the FSA. The FSA also receives related information from Fipo and Säpo, as well as tip-offs from the public. The FSA pays particular attention to currency exchange companies to make sure they do not provide MVTS without the appropriate

licence/registration. If a legal or natural person is conducting business without a licence, the FSA orders the person to cease the operation (*PSA (2010:751) Ch.8, sect.24*). Injunctions with cease and desist orders combined with penalty payments are the available sanctions for unlicensed MVTSs. The FSA has applied such injunctions to MVTSs on 8 occasions (both natural and legal persons) since 2010.

Criterion 14.3- The provision of payment services is subject to the *AML/CFT Act*, and the FSA is the authorised supervisor for PSPs, where the FSA is authorised to also inspect the PSP's branches, agents, and 3rd parties. This includes PSPs licenced in other EEA countries that do not need a licence in Sweden to provide payment services. *AML/CFT Act (2009:62) Ch.1 sect.2, PSA (2010:751) Ch.8 sect.1 and 21.*

Criterion 14.4- All agents for PSPs are required to be registered with the FSA, including those of PSPs licenced in other EEA countries that do not need a licence in Sweden. *PSA (2010:751) Ch.3 sect.17 and 26.*

Criterion 14.5-The registration for agents requires the agent's internal regulations for compliance with the AML/CFT Act. The FSA requires agents to be included in the PSP's AML/CFT and monitoring programmes. PSA (2010:751) Ch.3 sect.17.

Weighting and Conclusion:

Sweden is compliant with R.14.

Recommendation 15 – New technologies

In its 3rd MER, Sweden was rated largely compliant with R.8, owing to the lack of a specific requirement for FIs to have policies in place to deal with the misuse of technological developments. Changes to the *FATF Recommendations* have incorporated the requirements regarding non-face-to-face business in R.10, and refocused R.15 to focus on the identification and mitigation of risks associated with new technologies, with obligations for countries and financial institutions.

Criterion 15.1- When assessing whether the risk is high, FIs are required to direct special attention to ML/TF risks that might arise regarding new products and business methods, as well as the use of new technology (for both new and pre-existing products). Although there are no specific requirements regarding new delivery mechanisms, in doing a risk assessment, FI are required to pay attention to distribution channels in general. *AML/CFT Act (2009:62) Ch.2 sect.6, Ch. 5 Sect 1; FFFS (2009:1) Ch.2 sect 3.*

The risks connected to new products, delivery mechanisms and technology were identified and highlighted as a risk factor in the 2013/2014 NRAs. In the documents, a special focus is put on electronic money, virtual currencies and mobile payments. In addition, the FSA has had several ad hoc meetings during 2014–2015 with both Fipo and EBM regarding bitcoins, and in 2014, the FSA conducted ML/TF inspections on companies that provided virtual currencies.

Criterion 15.2- FIs are required to map and assess risks of ML/TF in their operations and implement risk-based measures to prevent that their organisations are used for ML/TF purposes. The risk

assessment must be documented and kept updated, including before introducing new or significantly altered products, services, markets and other factors relevant for its operations. AML/CFT Act (2009:62) Ch.5 sect.1, FFFS (2009:1) Ch.2 sect.1-4.

Weighting and Conclusion:

Sweden is compliant with R.15.

Recommendation 16 – Wire transfers

In its 3rd MER, Sweden was rated non-compliant for SR.VII. Significant changes were made to the requirements in this area during the revision of the FATF standards. Sweden implements the requirements on wire transfers through the *EU Regulation on Wire Transfers* (1781/2006/EC), which has direct applicability in Sweden. Transfers taking place entirely within the EU and European Economic Area (EEA) are considered domestic transfers for the purposes of R.16, which is consistent with the Recommendation. EU Regulation 1781/2006 does not include all the requirements of R.16 - specifically, it does not include requirements regarding information on the *beneficiary* of a wire transfer, or obligations on the *intermediary financial institutions* involved in a wire transfer, which were added to the FATF standards in 2012. The authorities advise that the new *EU Regulation (2015/847)* that will come into effect on 26 June 2017 will incorporate the new FATF requirements.

Criterion 16.1- FIs are required to ensure that all cross-border wire transfers of €1,000 or more are accompanied by the required and accurate originator information. However, there is no requirement to ensure that such transfers are also accompanied by the required beneficiary information. *EU Regulation 1781/2006 art.4 and 5*.

Criterion 16.2- The requirements regarding batch files are consistent with the FATF requirements regarding originator information. However, there is no requirement to include beneficiary information in the batch file. *EU Regulation 1781/2006 art.7.2.*

Criterion 16.3- Transfers of below €1,000 are required to be accompanied by the originator information. However, there is also no requirement to include the necessary beneficiary information. *EU Regulation 1781/2006 art.5.*

Criterion 16.4- In cases where there is suspicion of ML/TF, verification of the customer (originator) information is required as part of CDD. However, this only applies for wire transfers above €15,000 when CDD is required (see c.10.2). *AML/CFT Act (2009:62) Ch.2 sect.2 and 3.*

Criteria 16.5 & 16.6- Transfers within the EU and EEA are considered to be domestic transfers for the purposes of R.16, and are treated as such within *Regulation 1781/2006*. Domestic transfers may be accompanied only by the account number (or unique identifier) of the originator. The originator's PSP must be able to provide complete information on the originator, if requested by the payee, within three working days which is consistent with the second part of criterion 16.5 and

criterion 16.6. There is also a general obligation to provide information to competent authorities[50]. *EU Regulation 1781/2006 art.6.*

Criterion 16.7- The ordering FI is required to retain complete information on the originator for five years. However, there is also no requirement for beneficiary information. *EU Regulation 1781/2006 art.5*.

Criterion 16.8- The lack of requirements relating to beneficiary information indirectly affects this criterion. *EU Regulation 1781/2006 art.5*.

Criterion 16.9- Intermediary FIs are required to ensure that all originator information received and accompanying a wire transfer is kept with the transfer. There are no requirements to do the same for beneficiary information. *EU Regulation 1781/2006 art.12*.

Criterion 16.10- Where the intermediary FI uses a payment system with technical limitations, it must make all information on the originator available to the beneficiary financial institution upon request, within three working days, and must keep records of all information received for five years. However, there is also no requirement for beneficiary information. *EU Regulation 1781/2006 art.13*.

Criterion 16.1- Intermediary FIs are not required to take reasonable measures to identify cross-border wire transfers that lack originator information or required beneficiary information.

Criterion 16.12-There are no provisions relating to the role of the intermediary institution in responding to situations where the originator or beneficiary information is missing.

Criterion 16.13- The payee's PSP (beneficiary financial institution) is required to detect whether the required information on the payer is missing. There are no requirements to detect whether the required beneficiary information is missing. *EU Regulation 1781/2006 art.8*.

Criterion 16.14- There are no requirements for the beneficiary institution to verify the identity of the beneficiary under EU Regulation 1781/2006.

Criterion 16.15- When there is incomplete payer information, the payee's PSP is required to either reject the transfer, or ask for the complete payer information. The payee's PSP is required to consider the missing or incomplete payer information as a factor in assessing whether the transfer of funds, or any related transaction, is suspicious, and whether it must be reported to the relevant authorities. There are no requirements relating to cases where the required beneficiary information is missing or incomplete. *EU Regulation 1781/2006 art.9 and 10*.

Criterion 16.16- The requirements apply to all PSPs, which are defined as any natural or legal person whose business includes the provision of transfer of funds services. *EU Regulation 1781/2006 art.2.*

Criterion 16.17- PSPs (as obliged entities) are required to inspect transactions and file an STR where ML/TF is suspected. However, when a PSP controls both the ordering and beneficiary side of a wire transfers, there is no specific obligation to take into account information from both sides in order to

50 The definition of a domestic transfer within the EEA-area in the Regulation (Art.6(1)) is wider than that in R.16, which refers to "*a chain of wire transfers that takes place entirely within the EU*". The Regulation refers to the situation where the PSP of the payer and the PSP of the payee are situated in the EEA-area. Hypothetically, this means that according to the Regulation, a domestic transfer could be routed via an intermediary institution situated outside the EEA-area.

determine whether an STR has to be filed, and to file the STR in any country affected by the suspicious wire transfer. Nevertheless, an obliged entity is required to monitor and analyse the whole business relationship and all transactions without limitation. *AML/CFT Act (2009:62) Ch.3 sect.1.*

Criterion 16.18- Financial institutions conducting wire transfers are subject to the requirements of the EU regulations which give effect to UN resolutions 1267, 1373, and successor resolutions. Act on Certain International Sanctions 1996:95. The gaps identified in R.6 adversely affect the ability of financial institutions to meet their requirements in terms of implementation of targeted financial sanctions.

Weighting and Conclusion:

Sweden is partially compliant with R.16.

Recommendation 17 – Reliance on third parties

In Sweden's 3rd MER, R.9 was judged to be not applicable as FIs only relied on third parties in the context of outsourcing agreements performed under contract. The *AML/CFT Act (2009:62)* has provisions allowing entities to rely on third parties to perform certain CDD measures.

Criterion 17.1- FIs are permitted to rely on third parties to perform CDD checks. The categories of third parties allowed are listed in the *AML/CFT Act*, and they are required to either be licenced or registered in the EEA, or outside the EEA if they apply and are supervised for requirements that correspond to those of the EEA. The *FFFS (2009:1)* specifies which non-EEA jurisdictions are eligible. Because the list of eligible countries is set, FIs do not have to satisfy themselves that the 3rd party is regulated, supervised and monitored for AML/CFT compliance. The requirement that ultimate responsibility for the CDD measures remains with the obliged entity is not in the main body of the law, but is stated in the preparatory works. (*Government Bill 2008/09:70, p. 85–89, 187–188 and Government Bill 2014/15:80, p. 32*). *AML/CFT Act (2009:62) Ch.2 sect.3 and 4.*

Criterion 17.2- The country-level permissions for all EEA states is provided for in the *AML/CFT Act*, and non-EEA states with equivalent regulations are listed in *FFFS (2009:1)*. This approach of using equivalent regulations to determine eligible countries does not take into account country-specific risks and assumes that equivalent regulations in another country would equate to the same level of risks as Sweden.

Criterion 17.3- There are no specific requirements regarding reliance on a third-party that is part of the same financial group.

Weighting and Conclusion:

The list of eligible third countries does not take into account country-specific risks, and there is no requirement that FIs satisfy themselves that the 3rd party is regulated, supervised and monitored for AML/CFT compliance.

Sweden is partially compliant with R.17.

Recommendation 18 – Internal controls and foreign branches and subsidiaries

In its 3rd MER, Sweden was rated largely compliant for R.15 and partially compliant for R.22. Some deficiencies identified included the lack of an obligation to establish screening procedures when hiring employees, enforceability of some requirements for certain FIs, and enforceable requirements for group policies to apply to foreign branches and subsidiaries.

Criterion 18.1- Financial institutions are required to establish internal procedures against ML/TF, based on their operations and risk assessment. This includes compliance management arrangements and employee training. However, there is no requirement for screening procedures when hiring employees. While the authorities present that this is done in practice, this does not meet the requirements of "law or enforceable means". *FFFS (2009:1) Ch.6 sect.1, Ch.7 sect.1. AML/CFT Act (2009:62) Ch.5 sect.1.* While an independent audit function is required by *FFFS (2014:1)*, that Directive does not apply to all FIs[51].

Criterion 18.2- Financial institutions that are the parent entity of a financial group are required to establish common internal AML/CFT rules for the group. The deficiencies in c.18.1 apply here as well. *FFFS (2009:1) Ch.3 sect.4.* The same Directive (*Ch.8 sect.2*) requires procedures for the transmission of internal information within an FI "to the relevant business areas" but not for within the financial group (specifically). While *Ch.8 sect.2.* allows for a ML reporting officer to be responsible for all or several FIs within a group, there is no requirement for customer, account, and transaction information from branches and subsidiaries to be provided to group-level compliance functions.

Criterion 18.3- Financial institutions are required to apply regulations on CDD and record-keeping for their branches and majority-owned subsidiaries outside the EEA, and where that is not possible, to undertake measures to manage the risk and inform the FSA. However, this is limited to CDD and record keeping and does not include all required AML/CFT measures, and also does not apply to branches and subsidiaries within the EEA. AML/CFT Act (2009:62) Ch.2 sect.12. Chap. 3 sect. 3 FFFS 2009:1 requires FIs to communicate to its branches and majority-owned subsidiaries outside the EEA regarding the undertaking's risk assessment and procedures, etc. This requirement also does not apply to branches and subsidiaries within the EEA.

Weighting and Conclusion:

There is no requirement for FIs to have screening procedures when hiring employees, while the requirement for an independent audit function does not apply to all FIs. Some of the requirements for group-wide AML/CFT programmes are missing.

Sweden is partially compliant with R.18.

51 Applies only to banking companies, savings banks, members' banks, credit market companies, and credit market associations.

Recommendation 19 – Higher-risk countries

In its 3rd MER, Sweden was rated partially compliant with R.21, in part as there were no measures that ensured that FIs were advised about concerns of weaknesses in the AML/CFT systems of other countries. The obligations of this recommendation have changed significantly since the 2006 assessment.

Criterion 19.1- Enhanced CDD is required where there is high ML/TF risk, and FIs are required to conduct a risk assessment, including of geographic areas and taking into account other information from organisations, authorities, and other bodies within the area. However, there is no requirement that this be applied to customers and transaction from countries for which it is called for by the FATF. Although FIs may on their own accord assess that a country (who is also named by the FATF) is high risk, that would depend on the risk-assessment conducted by the FI. The FSA examines the FI's risk assessment in its supervision and also publishes the FATF's public statements on their webpage. *AML/CFT Act (2009:62) Ch.2 sect.6, FFFS (2009:1) Ch.2 sect.2 and 3.*

Criterion 19.2- Swedish authorities have limited means to apply countermeasures. The FSA is able to prohibit Swedish FIs from opening branches or subsidiaries in a specific country, or to deny applications from that country's FIs from establishing branches or subsidiaries in Sweden. They could prompt countermeasures indirectly, by naming specific countries as "high risk" in their directives such that FIs apply enhanced CDD (in the same way as the FSA has named specific countries in connection with reliance on third parties in *Ch.9 sect.1 FFFS 2009:1*). The same method could be used to apply countermeasures when called to do so by the FATF, but the FSA has instead opted for the modus described in c.19.1, i.e. to publish the FATF's statements on their website and through that (indirectly) oblige the FIs to take appropriate measures.

Criterion 19.3- The FSA publishes FATF's public statements on its website. Users may subscribe to email alerts, which would notify them of updates to the website, including on AML/CFT.

Weighting and Conclusion:

Sweden has limited means to apply countermeasures, and there is no specific requirement that enhanced CDD is applied to customers and transactions from countries when it is called for by the FATF.

Sweden is largely compliant with R.19.

Recommendation 20 – Reporting of suspicious transaction

In its 3rd MER, Sweden was rated partially compliant for both R.13 and SR.IV. The main technical deficiencies were due to deficiencies in the scope of the STR obligation and TF offence.

Criterion 20.1- FIs are required by law to file STRs promptly with Fipo (the FIU) when there is suspicion of ML/TF. *AML/CFT Act (2009:62) Ch.3 sect.1.*

Criterion 20.2- FIs are required to "inspect transactions" and to then file STRs if there is a suspicion of ML/TF. FIs must refrain from executing transactions that might be suspected, on reasonable

grounds, of being part of an ML or TF scheme. Although the requirement does not explicitly require STR filing for attempted transactions, combined with the reporting duty this would seem implied. AML/CFT Act (2009:62) Ch.3 sect.1. The preparatory works to the law explain that the requirement to file STRs applies even in cases where the transaction is suspended.

Weighting and Conclusion:

Sweden is compliant with R.20.

Recommendation 21 – Tipping-off and confidentiality

In its 3rd MER, Sweden was rated compliant with these requirements.

Criterion 21.1- This criterion is fully met by *AML/CFT Act (2009:62) Ch.3 sect.5.*

Criterion 21.2- This criterion is fully met by AML/CFT Act (2009:62) Ch.3 sect.4.

Weighting and Conclusion:

Sweden is compliant with R.21.

Recommendation 22 – DNFBPs: Customer due diligence

In its 3rd MER, Sweden was rated partially compliant with R.12. The deficiencies related to the scope of DNFBPs subject to the AML Act, the lack of requirements for CDD and monitoring of transactions, and that records of reported suspicious transactions had to be deleted after one year.

Criterion 22.1- DNFBPs are covered by the *AML/CFT Act* along with FIs, and the CDD requirements therein are similarly applicable to DNFBPs (see Recommendation 10). There are additional specific regulations for some types of DNFBPs. There is no threshold for casinos to conduct CDD. Estate agents need to conduct CDD on both their customer (who in most cases is the vendor) and the other party to the property purchasing agreement (in most cases the purchaser). *KAMFS (2013:5) sect.2*. Estate agents and entities regulated by CABs are required to check that representatives are duly authorised. *KAMFS (2013:5) sect.6, CAB Directives Ch.4 sect.3*. While the Guidance for advocates and law firms on the AML/CFT Act elaborates on how the requirements in the Act apply to advocates, associate lawyers and law firms, it is not by itself a "law or enforceable means" under the FATF Standards.

Most of the deficiencies for FIs continue to apply for DNFBPs, except for those relating to life insurance beneficiaries which are not applicable.

Criterion 22.2- DNFBPs are subject to the same requirements as FIs (see Recommendation 11). *Accounting Act (1999:1078) Ch.4 sect.1, Ch.5 sect.6-7, Ch.7 sect.2, AML/CFT Act (2009:62) Ch.2 sect.13, Ch.3 sect.1 and 1b, Regulation 7.12.2 of the SBA Code of Professional Conduct.*

Criterion 22.3- DNFBPs are subject to the same requirements as FIs, and consequently suffer the same deficiencies. However the deficiencies regarding life insurance beneficiaries do not apply to DNFBPs (see Recommendation 12). *AML/CFT Act (2009:62) Ch.1 sect.5, Ch.2 sect.3, 6a, 7, 7a, and 7b.*

Criterion 22.4- DNFBPs are subject to the same requirements as FIs under the *AML/CFT Act* (see Recommendation 15). *AML/CFT Act (2009:62) Ch.2 sect.6, Ch.5 sect.1, EtikU 11 Ch.7*.

Criterion 22.5- DNFBPs are subject to the same requirements as FIs, and consequently suffer the same deficiencies (see Recommendation 17). AML/CFT Act (2009:62) Ch.2 sect.3 and 4.

Weighting and Conclusion:

Similar deficiencies as identified in R.10, R.12 and R.17 are applicable for DNFBPs.

Sweden is largely compliant with R.22.

Recommendation 23 – DNFBPs: Other measures

In its 3rd MER, Sweden was rated partially compliant with R.16. The deficiencies included the scope of DNFBPs subject to the AML Act, since CFT obligations did not apply to DNFBPs, as well as concerns about STR reporting and tipping-off.

Criterion 23.1- DNFBPs are subject to the same requirements as FIs (see Recommendation 20). *AML/CFT Act (2009:62) Ch.3 sect.1.*

Criterion 23.2- DNFBPs are required to provide training programmes to employees. *AML/CFT Act (2009:62) Ch.5 sect.1*. Casinos, estate agents[52], public accountants, and entities regulated by CABs need to have compliance management arrangements. *LIFS (2015:3) Ch.5, KAMFS (2013:5) sect.4, EtikU 11 Ch.7, CAB Directives Ch.10 sect.1.* Casinos and entities regulated by CABs are required to also have independent audit functions. *LIFS (2015:3) Ch.3 sect.1 and Ch.8 sect.1, CAB Directives Ch.3 sect.1.* There are no requirements for DNFBPs to have screening procedures when hiring employees.

Criterion 23.3- DNFBPs are subject to the same requirements as FIs, and consequently have similar deficiencies (see Recommendation 19). *AML/CFT Act (2009:62) Ch.2 sect.3 and 4*. Estate agents are required to take into account information from international bodies when conducting their risk assessments. *KAMFS (2013:5) sect.3.*

Criterion 23.4- DNFBPs are subject to the same requirements as FIs (see Recommendation 21). AML/CFT Act (2009:62) Ch.3 sect.4 and 5.

Weighting and Conclusion:

Similar deficiencies as identified in R.18 and R.19 are applicable for DNFBPs.

Sweden is largely compliant with R.23.

52 Pursuant to the AML/CFT Act, the responsibility lies with the real estate agent personally and, if he or she is employed, the legal person/employer.

Recommendation 24 – Transparency and beneficial ownership of legal persons

In its 2006 report, Sweden was rated partially compliant with former R.33, due to deficiencies in the requirements on beneficial ownership information to be collected and made available, as well as concerns about the majority of foundations needing to be registered. Since then, the FATF standard has substantially changed.

Criterion 24.1-

Companies, Partnerships, Economic Associations, Sole Traders: The Swedish Company Registration Office (SCRO) maintains websites (www.bolagsverket.se and www.verksamt.se) which provide basic information on types and features, and procedures for creation, for sole traders, limited companies, partnerships, and economic associations. The website includes information about where basic ownership (but not beneficial ownership) in limited companies and partnerships are kept, and that they can be accessed on request.

Foundations and Non-Profit Associations (NPAs)[53]**:** Basic information on foundations can be obtained at the Foundations Database (web05.lansstyrelsen.se/stift/StiftWeb/SSearch.aspx). Basic information on foundations and NPAs, and on registering them, are found at the STA's website (www.skatteverket.se/foretagorganisationer/foreningar/stiftelser). Information filed by registered foundations held by an authority is generally accessible to the public on request in Sweden, except where there are valid reasons to deny access. There is also information about NPAs on the SCRO's website.

Criterion 24.2- The use of companies in ML predicates was considered in Brå's 2015 ML NRA (*2015:22*). EBM also assesses the risks related to legal persons created in Sweden being used for economic crimes in its intelligence reports. However, there is no ML/TF risk assessment of all types of legal persons created in Sweden.

Criterion 24.3-

Companies: The SCRO maintains the company register. Companies must register in order to acquire legal personality, and provide inter alia the articles of association in addition to information on the registered address of the company, the share capital, the directors and deputy directors, and the persons who sign for the company. *Companies Act Ch.27 sect.1*, Companies *Ordinance Ch.1 sect.3 and 4.*

*Partnerships***:** The SCRO maintains the trade register, where partnerships must register to acquire legal personality. The trade register contains information about the partnership's activity as well as the identity of its partners, including names, social security numbers or equivalent, and addresses. *Partnership and Non-registered Partnership Act Ch.1 sect.1*, *Trade Register Act (1974:157) sect. 4*.

53 NPAs are a distinct type of legal entity defined in Swedish law. These do not correspond exactly to the definition of an NPO in the FATF Standards, which is based on the function and objectives of the organisation, not its legal type. This means that several different types of (Swedish) legal persons, including NPAs, foundations, religious organisations, and others, can be considered NPOs for the purposes of FATF Recommendation 8.

Foundations: All but one type of foundation must be registered at the County Administrative Board, where a foundation register is maintained. The information in the register includes the foundation's postal address and telephone number, and the identity and contact details of members of the board or managers. *Foundations Act (1994:1220) Ch.10 sect.1 and 2*. However, a specific type of foundation – foundations that use their assets for the benefit of identified persons, typically family foundations – is not required to be registered with the County Administrative Board, although tax registration is required if the foundation carries out business activities. *Foundations Act (1994:1220) Ch.1 sect.7, Tax Procedure Act Ch.7 sect.1.*

Economic Associations: The SCRO approves applications to form economic associations, which include the association's statutes and the board of directors. The information submitted to SCRO is largely the same as for limited companies, with the exception that annual reports for small size associations are handed in to the SCRO on request. Information held by the SCRO is generally publically available. *Annual Reports Act Ch.8 sect. 3 item 2, Freedom of the Press Act Ch.2 sect. 1 and 2.*

NPAs: There is no general requirement that NPAs be registered. NPAs that engage in trade or intend to do so may be registered in the trade register, and if they are required to produce an annual report, they must register (*Trade Register Act sect. 2*). Any NPAs which must submit any form of tax report to the tax authority must register with the Tax Agency (STA), which some banks require in order to open a bank account. For the registration, associations need to provide information to the SCRO about the name and the nature of the operations of the association, its statutes, representatives, as well as information on the board directors and board deputies (*Trade Register Act sect. 4, Trade Register Ordinance 1974:188 sect. 8*).

Criterion 24.4-

Companies: Companies are required to maintain share registers, containing among other details information regarding each share's number, the shareholders' names and personal ID numbers, company numbers or other identification numbers as well as postal address, the class to which each share belongs and whether share certificates have been issued. *Companies Act Ch.5 sect.1 and 5.* The board of directors is responsible for ensuring that the share register is maintained, stored, and made available for all persons who wish to review it. *Companies Act Ch.5 sect.7.* For companies whose share registers are maintained by CSDs, the information available to the public is limited to shareholders holding more than 500 shares. *Companies Act Ch.5 sect.19.*

Partnerships: While there is no legal requirement for a partnership to maintain identity information of its partners, such information is held in the trade registry. *Partnership and Non-registered Partnership Act Ch.2 sect.2*.

Foundations: Information about the founder(s) of the foundation is contained in the foundation instrument which has to be signed by the founder(s). *Foundations Act (1994:1220) Ch.1 sect.3.* Information on beneficiaries of a foundation is based on a statement of purpose of the foundation. However, identification of individual beneficiaries may not be possible in cases where the beneficiaries are defined as a class of persons or the foundation works for the benefit of a cause.

Economic Associations: The register of members is maintained by the Board of each association, and contains information of each member's name and postal address, as well as the amount of membership fees paid and to be paid.

NPAs: NPAs are not required to keep a register of members. In practice they will need to have some information on their members in order to hold the annual meetings, which law enforcement agencies can obtain pursuant to the rules in the Code of Judicial Procedure.

Criterion 24.5-

Companies: Exercise of shareholders' rights is conditional on the information contained in the share register, and the share register is required to be immediately updated when information on changes to shareholdings is presented to the company. *Companies Act Ch.5 sect.1 and 9.* Where the share registry is maintained by a CSD, the same requirements for information and updates apply.

Partnerships: Partnerships are required to update changes to the information held in the trade register without any delay. *Trade Register Act (1974:157) sect.13.*

Foundations: Foundations are required to update changes to the information held in the foundation register immediately. *Foundations Act (1994:1220) Ch.10 sect.3.*

Economic Associations: The board is responsible for submitting any changes to any aspect to the registered information, e.g. the composition of the association to the SCRO, or new address. *Economic Associations Act Ch.6 sect 15*. There is an implicit requirement for board to ensure that the information on members is updated on a timely basis[54], and the Economic Association's accountant should as a part of the control of the board's governance of the association verify if the member register has been kept correctly.

NPAs: For NPAs registered in the trade register, any change in the information registered must be notified to the SCRO.

Criterion 24.6- Sweden does not require companies or company registries to obtain and hold beneficial ownership information, and instead relies on a combination of existing mechanisms to obtain beneficial ownership information. In the specific case of listed companies, there are disclosure requirements for direct and indirect shareholdings (including by relatives and proxies) at several levels of ownership percentages. *Act on Trade in Financial Instruments (1991:980) Ch.5 sect.5*. For companies or associations where up to four owners own shares corresponding to more than half of the votes, these companies or associations may opt to provide information to identify the owners and persons with close interest to them in order to get an "F-skatt" so that preliminary taxes are not withheld from it (*Tax Procedure Act Ch.3 sect 1*). This may in some cases allow beneficial ownership to be identified. In cases where the legal owner (or beneficiary in the case of foundations) is also the beneficial owner, the information held by the SCRO (or CABs for foundations) would be relevant, but this would not apply to foundations and NPAs that are not registered (see criterion 24.3 above).Sweden also relies on beneficial ownership information collected by FIs and DNFBPs in the

54 Amendment to the Economic Associations Act entered into force on 1 July 2016 (after the dates of the on-site and hence not assessed), where the obligation that the board must keep the information updated is expressly stated in the law.

course of the CDD process (see Recommendations 10 and 22), although this will not include entities that were not formed through a lawyer or CSP and do not have relationships with FIs and DNFBPs in Sweden.

Criterion 24.7- The same deficiencies as in c.24.6 apply here. There is a general obligation that FIs and DNFBPs conduct ongoing due diligence, and keep documents, data, and CDD information up to date (see Recommendations 10 and 22). *AML/CFT Act (2009:62) Ch.2 sect.10*.

Criterion 24.8-

Companies, Economic Associations and Foundations: Companies, economic associations and foundations are required to either have an authorised representative (a natural person) resident in Sweden, or must otherwise designate someone to fill this role. Any document received by the representative from courts and authorities is considered as served. The representative is not however required to be accountable to competent authorities for providing information or for giving assistance. *Companies Act (2005:551) Ch.8 sect.40, Economic Associations Act Ch._6 sect 11, Foundations Act Ch._2 sect 16a.* While board members are responsible for questions concerning the ownership of the company, economic association or foundation, and for providing such information to competent authorities, under EU law board members may reside outside of Sweden. There are no other significant requirements ensuring that companies cooperate with competent authorities to the fullest extent possible in determining the beneficial owner(s). The relevant sector legislation requires the obliged entities to inform the competent authorities of the beneficial ownership of their customers upon request.

NPAs: There are no requirements that NPAs have representatives or designate a DNFBP, or have comparable measures, to be accountable to competent authorities for the purposes of this criterion.

Criterion 24.9- Information provided to government authorities are kept indefinitely unless they are assessed to not hold value. *Archives Act (1990:782) sect.3*. For companies, the shareholder register must be preserved for 10 years after the company's termination. *Companies Act (2005:551) Ch.5 sect.3*. For economic associations, the member register is required to be preserved for 7 years after the dissolution. *Economic Associations Act Ch.3 sect 8*. There are no requirements for partnerships and foundations to maintain information and records from the partnership or foundation after dissolution. However, information concerning partners is registered and thus available and also concerning foundations the statutes and annual reports are filed.

FIs and DNFBPs are required to maintain documents and information on CDD measures for at least 5 years from the date the measures were undertaken, or from the end of the business relationship (see Recommendation 11 and 22). *AML/CFT Act (2009:62) Ch.2 sect.13, Ch.3 sect.1b*

Criterion 24.10- The Police Authority has the power to obtain information held by banks. *BFBA (2004:297) Ch.1 sect.11.* This is similarly the case for other FIs and DNFBPs who must upon request from the Police Authority provide all the information necessary for an investigation related to ML or TF without delay (see Recommendation 11 and 22). *AML/CFT Act (2009:62) Ch.3 sect.1.* The STA can request information from the banks, e.g. bank account statements, a proxy or other documents that enable the STA to determine who uses the bank accounts of legal persons (Tax Procedure Act Ch.9 sect.9). FI and DNFBP supervisors have the power to request information needed to perform

supervision (see Recommendations 27 and 28). The SCRO can obtain information from limited companies if an obligation to hand it in has not been met (Companies Act Ch. 30 sect. 3).

Criterion 24.11-

Companies: Swedish law does not allow for the issuance of bearer shares or bearer share warrants.

Criterion 24.12-

Companies: Nominee shareholders are allowed for companies whose share registers are maintained by CSDs. Only clearing organisations, banks and brokers can operate as a nominee in Sweden, and nominees are required to provide the CSD with information on the shareholders whose shares he/she is managing, such as names and personal identity numbers, corporate/organisation identity numbers or other identification numbers and postal addresses, as well as the number of different kinds of share owned by each shareholder. Companies Act Ch.5 sect.14, Financial Instruments Accounts Act (1998:1479) Ch.3 sect.7 and 12. The CSD is required to make available to the public the list of shareholders that have more than 500 nominee-registered shares in the company. Companies Act Ch.3 sect.13.

Criterion 24.13-

Companies: The SCRO may dissolve companies that fail to file the names of the board of directors or managing director. Companies Act Ch.25 sect.11. Fines[55] or terms of imprisonment not exceeding one year will be imposed on any person who intentionally or through negligence fails to maintain a share register or fails to make such share register available. Companies Act Ch.30 sect.1. The SCRO may impose conditional fees[56] on board members or a CEO in order to force the company to comply with an obligation to register information. Companies Act Ch.30 sect.3.

Partnerships: A party which issues incomplete, incorrect, or misleading information is subject to a fine, depending on the severity of the infringement. The range varies from a minimum of SEK 200 (EUR 22) to a maximum of SEK 4,000 (EUR 440). Trade Register Act sect.22.

Foundations: CABs may request documents or information from the foundations that are under its supervision, participate in meetings with the board, in special cases conduct an inspection on-site, or may dismiss members of the board (*Foundations Act Chapter 9, sections 1, 4, 5 and 6*). The CABs may impose conditional fees to force the foundation to comply (Ch. 10 sect. 11).

Economic Associations: Failure of the board to meet obligations to keep a member register or to make it available may lead to fines (*Chapter 16, section 1 of the Economic Associations Act)*. The SCRO may impose conditional fees on board members or a CEO in order to force the economic association to comply with an obligation to register information (*Chapter 16, section 2 of the Economic Associations Act*).

55 The size of the amount is guided by the Default Fines Act (1985:206), and is related to the economic situation of the defendant; effectively, there is no set maximum amount.

56 Ibid.

NPAs: Providing incomplete or incorrect information can be a criminal offense.[57] The sentence would be fine or imprisonment up to 6 months or in serious cases imprisonment for 2 years (*Code of Judicial Procedure, Ch.15, sect. 12*).

Criterion 24.14- The STA provides information about taxation on request (EOIR) from other countries. When a request is received, the STA consults available systems and/or investigates on behalf of the requesting authority. Fipo assists foreign counterparts' requests by sharing the information available to Fipo, such as issues relating to beneficial owners. The SPA's three International Public Prosecution Offices handle incoming requests for assistance, which may relate to basic and beneficial ownership information. Refer to R.37 on limitations to the use of investigative techniques in some cases where the money laundering offence would not be considered gross.

Criterion 24.15- There is no formalised process for monitoring the quality of assistance received from other countries, but Sweden reports that individual authorities such as the STA and SPA provide feedback on the assistance received to their foreign counterparts on request and proactively.

Weighting and Conclusion:

There is no ML/TF risk assessment of all types of legal persons created in Sweden. Not all foundations are required to register, while there is no requirement for NPAs to register. There are gaps in ensuring that companies co-operate with competent authorities to the fullest extent possible in determining the beneficial owner.

Sweden is partially compliant with R.24.

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

In its 3rd MER, these requirements were considered to be not applicable, as Sweden does not recognise the legal concept of common law trusts. The *FATF Recommendations* have since been revised such that some elements of R.25 apply to all countries. Sweden is not a party to the Hague Convention on the Law Applicable to Trusts and on their Recognition and does not recognise the concept of a trust formed under foreign law. Therefore, a trust cannot hold or acquire any obligations or rights in Sweden. That being said, there are no restrictions for a resident of Sweden to act as trustee, protector or administrator of a trust formed under foreign law. The provision of trust-related services has been regulated under the *AML/CFT Act (2009:62)*.

Criterion 25.1- Sub-criteria (a) and (b) are not applicable as Sweden does not recognise common law trusts. Regarding (c), professional trust service providers are within the scope of the *AML/CFT Act (2009:62) Ch.1 sect.2* and are therefore required to conduct CDD on their customers and the customers' beneficial owner, and to maintain the information for at least five years (*Ch.2 sect.13*). But there are no requirements relating to trust-relevant parties that are neither the customer nor the customer's beneficial owner. The deficiencies regarding customers that are legal arrangements in R.10 and R.22 on beneficial ownership CDD requirements for legal arrangements are relevant here. The deficiencies are to an extent mitigated by Swedish tax law, which requires Swedish trustees of

[57] If the offence is of a serious nature and there is *mens rea*.

foreign trusts to keep information identifying the settlor and beneficiaries of the trust and provide them to STA to determine the tax liability of the trust's asset and income. *Tax Procedure Act Sect. 37(6), 39(3).*

Criterion 25.2- The CDD information collected by professional TCSPs is required to be up-to-date (see R.22). This however does not apply to the information that is not collected as part of CDD.

Criterion 25.3- FIs and DNFBPs are required to determine beneficial ownership of their customers, but the deficiencies regarding customers that are legal arrangements in R.10 are relevant here. There is no requirement for trustees themselves (professional or otherwise) to disclose their status.

Criterion 25.4- There are no restrictions in law on trustees providing competent authorities with any information relating to trusts.

Criterion 25.5- Law enforcement is able to obtain information held by Swedish trustees (such as the information required by the tax law) in the course of their investigations through investigative measures, e.g. searching of people's premises and seizing evidence. *Code of Judicial Procedure Ch.27-28*. The authorities' supervisory powers enable them to obtain information from FIs and DNFBPs, including TSPs (see R.27 and R.28).

Criterion 25.6- The STA provides information through e.g. Tax Information Exchange Agreements (EOIR) on trusts and other legal arrangements. When a request is received, the STA consults available systems and/or investigates on behalf of the requesting competent authority.

Criterion 25.7- In cases where trustees are FIs or TSPs, they would be liable for failure to comply with AML/CFT requirements (see R.27 and R.28). Failure by trustees to comply with the requirements to keep the tax-related information relating to the trust is an offence and subject to a fine. *Tax Procedure Act Sect. 44(2).*

Criterion 25.8- FIs and DNFBPs can be sanctioned for failing to provide the information requested by supervisors (see R.27, R.28, and R.35).

Weighting and Conclusion:

Requirements on professional trust service providers to conduct CDD does not extend to trust-relevant parties that are neither the customer nor the customer's' beneficial owner. This limitation impacts several other criteria.

Sweden is partially compliant with R.25.

Recommendation 26 – Regulation and supervision of financial institutions

In its 3rd MER, Sweden was rated partially compliant with R.23, due to scope issues with the AML Act, the lack of fit and proper tests for senior management, and limitations to the ability to ensure compliance of money exchange and money remittance services with AML/CFT requirements.

Criterion 26.1- The FSA is responsible for the supervision of FIs, including for AML/CFT requirements. *FSA Ordinance (2009:93) sect.1*.

Criterion 26.2- Core principles institutions are required to be licensed. Other types of FIs are required to be licensed or registered. *BFBA (2004:297) Ch.2 sect.1, IBA (2010:2043) Ch.1 sect.1, SMA (2007:528) Ch.2 sect.1, CFOA (1996:1006) sect.1, DTOA (2004:299) sect.7, IMA (2005:405) Ch.2 sect.1, EMA (2011:755) Ch.2 sect.1, IFA (2004:46) Ch.1 sect.4, PSA (2010:751) Ch.2 sect.1 and 4, AIFMA (2013:561) Ch.2 sect.3 and Ch.3 sect.1, CCOA (2014:275) sect.4.*

Criterion 26.3- At the licence or registration stage, there are fit and proper requirements for legal owners (i.e. persons with "qualified holdings")[58] of all categories of FIs, except insurance mediators where such requirements do not apply to owners of legal persons. There are fit and proper requirements for the board, the MD and their alternates (but not for all senior management positions) for most types of FIs. These requirements do not apply to beneficial owners of FIs (where the legal owner(s) or person(s) with qualified holdings is not the beneficial owner).

On an on-going basis, changes to significant levels of legal ownership of some FIs require the FSA's approval at which fit and proper checks are applied, and the FSA may deny approval. Where the FSA has determined that a significant legal owner is no longer qualified, the FSA may for most types of FIs order the person to divest ownership. The FSA is able to order the removal or replacement of a board member or the MD if the person is no longer qualified, and to revoke the FI's licence/registration if the order is not complied with, but this does not apply to all senior management positions.

Criterion 26.4 –

(a) Sweden last underwent an IMF FSAP assessment in 2011[59], and was assessed to be largely in line with the Core Principles. However, the FSAP noted concerns on the lack of power to assess fitness and propriety of all members of senior management and the ability to remove senior management from their positions, insufficient on-site inspection across systemic and non-systemic institutions, and the lack of obligations to implement screening procedures to ensure high ethical and professional standards when hiring staff. The level of supervisory resources was also indicated as an issue. Since then, the FSA has undertaken extensive work to address the concerns identified.

(b) Non-Core Principle FIs are supervised or monitored by the FSA for AML/CFT compliance. FSA Ordinance (2009:93) sect.1.

Criterion 26.5- The FSA has a risk-based framework for the supervision of AML/CFT, which is determined by risk assessments and risk classifications. Risk assessments are conducted annually "to identify and rank risks that affect the stability and functionality of the financial system and the interests of consumers".

---

58 Fit and proper requirements are applied to "qualified holdings" for banks, defined as direct or indirect ownership representing 10 percent or more of the equity capital or of voting rights or other holdings which renders it possible to exercise a significant influence over the management of the undertaking. *BFBA (2004:297) Ch.1 sect.5, IBA (2010:2043) Ch.1 sect.15, SMA (2007:528) Ch.1 sect.5, CFOA (1996:1006) sect.3, DTOA (2004:299) sect.6, EMA (2011:755) Ch.1 sect.2, IFA (2004:46) Ch.1 sect.1, PSA (2010:751) Ch.1 sect.4, AIFM (2013:561) Ch.1 sect.11, CCOA (2014:275) sect.6*. For insurance mediators, the requirements only apply to physical person and not owners of legal persons.

59 The IMF's 2016 FSAP assessment of Sweden was completed after the onsite.

The FSA has, as a result of the risks identified in the 2013–2014 NRAs and the national strategy, enhanced its focus on the identified risk areas, such as currency exchangers and MVTS. Furthermore, the FSA has conducted several presentations for the private sector and produced guidance documents for currency exchangers with the purpose to help them implement the AML/CFT regulations.

The FSA's risk classification tool determines the classification of the ML/TF risk of supervised entities. The current risk classification tool consists of 4 factors: (1) the amount of turnover, (2)whether the entities handle cash or not, (3) whether entities offer cross border transactions to their customers, and (4) number of STRs filed by the entity. However, the framework is not yet complete as the assessment of mitigating measures is not yet in place, while inherent vulnerability is based on only two factors: cash transactions and cross-border transactions. The policies, internal controls and procedures of the entity or group are not considered in the risk classification tool beyond the dimensions listed above.

The FSA's risk classification tool is under development to become more diverse and to consist of more risk factors. Currently the FSA uses the information from the above risk-classification tool combined with other factors and information about the FIs to determine which institutions should be subject to supervisory activity. These factors depend on the scope and focus of the planned investigation, and can include turnover, geographical position, balance sheets, offered products and services, STRs filed, specific information from Fipo and other divisions within the FSA, previous inspections, supervisory colleges and contact with other countries' supervisors, as well as FIs' responses to AML/CFT questionnaires from the FSA.

Criterion 26.6- The FSA regularly reviews the risk of specific financial institutions when they are subject to supervisory activities by the FSA and when the risk classification is updated with new information. The authorities report that STR information from Fipo is received quarterly and that it inputs into the risk classification of FIs. When the FSA receives specific information about a financial institution the risk profile of that institution is evaluated.

The FSA closely monitors the four largest banks with regards to major events or developments in the management and operations, both within the financial institution and on a group level. For cross-border banking groups, the competent authorities work closely with oversight in the Group's college of supervisors. These banks are required to notify the FSA in case of a major event or IT incident. These notifications are to be followed by a written report to the FSA. The FSA's Anti-Money Laundering Division is able to conduct event-driven supervision, and has done so e.g. in relation to the "Panama Papers".

Weighting and Conclusion:

Fit and proper requirements do not apply to all senior management positions, nor to the beneficial owners in all situations. There is no ability to force persons who are no longer suitable to divest ownership for some types of FIs. The risk classification tool for the ML/TF risk of supervised entities is not yet complete and is still under development (at the time of the onsite), as the assessment of mitigating measures is not yet in place, while inherent vulnerability is based on only two factors.

Sweden is partially compliant with R.26.

Recommendation 27 – Powers of supervisors

In its 3rd MER, Sweden was rated largely compliant with R.29, due to scope issues as well as limitations to the powers of supervisors on some financial institutions.

Criteria 27.1, 27.2, and 27.3- The FSA has powers under the respective FI legislation to supervise or monitor for compliance with AML/CFT requirements, including the ability to conduct inspections and compel the production of information. *FSA Ordinance (2009:93) sect.1, BFBA (2004:297) Ch.13 sect.2-4, IBA (2010:2043) Ch.14 sect.2, 3 and 6, SMA (2007:528) Ch.23 sect.1, 2 and 4, CFOA (1996:1006) sect.7 and 7a, DTOA (2004:299) sect.10, IMA (2005:405) ch.7 sect.4, EMA (2011:755) Ch.5 sect.1-3, IFA (2004:46) Ch.10 sect.1, 2 and 4, PSA (2010:751) Ch.8 sect.1-3, AIFMA (2013:561) Ch.13 sect.1, 5-7 and 9, CCOA (2014:275) sect.16 and 17.*

Criterion 27.4- As the supervisor and licensing/registration authority the FSA is able to impose a range of administrative sanctions on FIs that fail to comply with AML/CFT requirements, such as the ability to give warnings, impose injunctions/prohibitions, issue fines, and revoke licenses. However, the ability to issue fines is limited to some FIs, and within that subset, some only allow conditional fines, which means the full range of measures are not available for those institutions (see Recommendation 35). The FSA considers that revoking a license of an FI is more dissuasive than imposing an administrative fine.

Weighting and Conclusion:

The ability to issue fines is limited to some types of FIs, as some only allow conditional fines.

Sweden is largely compliant with R.27.

Recommendation 28 – Regulation and supervision of DNFBPs

In its 3rd MER, Sweden was rated non-compliant for R.24. The deficiencies included supervisory bodies not having responsibility for AML/CFT, lack of administrative sanctions, as well as issues of coverage of DPMS, TCSPs, lawyers and accountants.

Criterion 28.1- Casinos in Sweden are required to be licensed, operated by a state-owned company (AB Svenska Spel), and are supervised for compliance with the *AML/CFT Act* by LI. *Casinos Act (1999:355) sect.1, sect.11, and sect.14*. Fit and proper tests are applied to the board and senior management of AB Svenska Spel.

Criterion 28.2 and 28.3- Other DNFBPs are supervised or monitored for AML/CFT by the CABs, the FMI, SBA, and RN. *Estate Agents Act (2011:666) sect.28, AML/CFT Act (2009:62) Ch.6, Code of Judicial Procedure (1942:740) Ch.8 sect.6, Public Accountants Act (2001:883) sect.3, RN Ordinance (2007:1077) sect.1.*

Criterion 28.4–

(a) The DNFBP supervisors/SRBs are able to obtain information from their supervised entities and conduct inspections. Estate Agents Act (2011:666) sect.28, AML/CFT Act (2009:62) Ch.6 sect.6 and *sect.7, Code of Judicial Procedure (1942:740) Ch.8 sect.6, Public Accountants Act (2001:883) sect.28, Casinos Act (1999:355) sect.14a.*

(b) Fit and proper requirements are in place in the licensing/registration of DNFBPs. Estate Agents Act (2011:666) sect.6, AML/CFT Act (2009:62) Ch.6 sect.5, Code of Judicial Procedure (1942:740) Ch.8 sect.2, Public Accountants Act (2001:883) sect.4. These requirements do not apply to corporate real estate agencies and law firms, although they apply to individual estate agents and lawyers. Beneficial owners of the DNFBPs are not screened.

(c) Supervisors/SRBs have a range of sanctions available including the revoking of licences, rectification orders, and warnings. Some categories of DNFBPs may be given fines, but others do not have such an option. Casinos Act sect.14b and sect.14c, Estate Agents Act (2011:666) sect.29, AML/CFT Act (2009:62) Ch.6 sect.7a and sect.9, Code of Judicial Procedure (1942:740) Ch.8 sect.7, Public Accountants Act (2001:883) sect.32-35.

Criterion 28.5- The CABs adapt their supervision based on their conduct of external risk analyses and their understanding of the risk profiles of their supervised industries. The CABs request information via a digital questionnaire from the supervised entities about their awareness of AML/CFT obligations and risks. The data is then used for the CABs' risk classification system which leads to the supervision focusing on higher-risk entities.

In addition to the work with the risk classification system, a representative from each CAB also participates in their corresponding RUC, which helps the CABs to identify high-risk entities to be supervised. Besides the intelligence information from the RUCs, the CABs also obtain information about modus operandi and current trends of organised crime in the region and nationally.

Estate agents are at least inspected on 5-year intervals regarding potential convictions of crime and level of debts. Supervisors may conduct inspections with AML/CFT components based on reports filed on specific estate agents and on market surveillance, as well as on a thematic basis (*FMI Strategy for AML Supervision).* FMI's understanding of ML/TF risks is principally based on the frequency and substance of the decisions on disciplinary sanctions against estate agents in AML/CFT matters.

Weighting and Conclusion:

Sweden is largely compliant with R.28.

Recommendation 29 – Financial Intelligence Units

Sweden was rated as largely compliant in its 2006 Evaluation, with technical deficiencies relating to the time limit on data retention, and the lack of guidance to reporting entities.

Criterion 29.1– Sweden's FIU (the "Financial police" – Fipo) is established as a branch of law enforcement, within the Police Authority (Ordinance containing Instructions for the Police Authority (2014:1102), Ch.35). Fipo is an agency of the National Operations Department (NOA). By law, obliged entities must report to the Police Authority suspicious transaction reports on ML and TF (AML/CFT Law, Ch.3, s.1).

Fipo's duties and function within the Police Authority are defined in broad terms in the authority's internal guidelines, which are binding policy documents. According to the Rules of Procedure for the Police Authority, NOA has responsibility for the intelligence activity related to money laundering and terrorist financing (Ch.3, s.19). Section 2.6.2 of the Administrative Procedures for the National Operations Department establishes that Fipo has functional responsibility for the intelligence activities of the Police Authority as regards money laundering and terrorism financing. Fipo has also responsibility for work to counter money forgery and for issuing restraint orders to the effect that property cannot be moved or disposed until further notice (Prohibitions on Disposal of Property, PDP). The specific duties of Fipo are not formally regulated in details. Nonetheless, the Swedish authorities have indicated that the main duty of Fipo is to conduct operational analysis, and communicate the results of their analysis to relevant investigative units within the Police Authority, the Security Service (Säpo) and other law enforcement authorities to ensure that law enforcement measures can be undertaken.

Criterion 29.2– Fipo acts as the national centre for the receipt of STRs and other related reports. Reporting entities must file STRs with the Police Authority (AML/CFT Law, Ch.3, s.1). Supervisory authorities must immediately inform the Police Authority if they, in their inspections or otherwise, discover circumstances that might relate to ML or TF (*AML/CFT Law, Ch.3, s.6*). Sweden has indicated that entities are obliged to report to the Police Authority (Fipo) information on cash withdrawals, transfers, currency exchange and payment services. Fipo weekly receives cash reports from Customs.

Criterion 29.3–

(a) All reporting entities are required by law to provide any information deemed necessary for an ML/TF investigation without delay upon request from the Police Authority (AML/CFT Act, Ch.3, s.1). This applies to all reporting entities (i.e. is not limited to those which previously filed a related STR). The threshold for Fipo to request additional information from reporting entities is that there must be an indication (of any kind) of a possible ML/TF crime and that the information thus could be necessary for a ML/TF FIU case. The information gathered could then be forwarded to other units or authorities in order to initiate a criminal investigation, thus enabling the use of all coercive measures available to a criminal investigation. The Swedish authorities have indicated that the threshold for starting a criminal investigation within the Police Authority is very low as, according to the Code of Judicial Procedure, a criminal investigation should be initiated as soon as there is reason, because of a report or because of something else, to believe that a crime has been committed (Ch.23, s.1). Regardless of whether a criminal investigation has been initiated or not, Fipo has the power to obtain and use additional information from reporting entities as part of the intelligence gathering it performs to build up a case (operative analysis).

(b). Fipo has access to information in the Police Authority's database as well as the criminal records register (criminal convictions), suspicion register (actively suspected crime), the general surveillance register (intelligence information) and the central investigation register (operative register for modus operandi). Fipo also has direct access to information that is held by other authorities, such as census information, tax data, registries of property ownership, vehicle ownership, family relations and company information. Fipo can also obtain information from the intelligence databases that Säpo shares with the intelligence services of the Police Authority. On request, Fipo can obtain information from Swedish Social Insurance Agency, the Swedish Prison and Probation Service, the Swedish Enforcement Authority, the SPA, the Swedish Migration Agency, the Swedish Employment Agency and the Swedish Coast Guard.

Fipo manages an ML register, pursuant to the Police Data Act (2010:361), where STRs, persons related to the STRs and information of note for the analysis and administration of STRs is stored. Personal data in the ML register should be kept for a maximum of five years, counting from the latest update related to the data in question (s.20).

Criterion 29.4- Fipo carries out operational analysis on the basis of information received from reporting entities. To conduct operational analysis, Fipo uses the ANACAPA method, supported by tools such as iBase, Analyst Notebook, Surfa and Excel.

Fipo's activity with regard to strategic analysis is not established by law or in procedures. The Swedish authorities have indicated that the Police Authority has put greater focus on strategic analysis and pointed to some examples of strategic analysis conducted by Fipo, such as the report *Money Laundering within serious organised crime*, Fipo's yearly reports, and information brochures. The efforts made by Fipo in conducting strategic analysis are not sufficient to meet the requirements of C.29.4.

Criterion 29.5- Fipo disseminates the results of its analysis to the relevant authorities either as an operational report (if the information provides cause to believe that a crime giving rise to proceeds has been committed), or as an intelligence document in cases which do not meet this threshold but where there are nevertheless reasons to disseminate the information. An operative report describes the predicate offence or the criminal activity giving rise to proceeds as well as the suspicion of the ensuing ML offence. Operative reports and intelligence documents can be disseminated to law enforcement units within the Police Authority and external authorities such as EBM, Säpo, SKV and TV, among others. Intelligence documents can be disseminated to authorities involved in law enforcement intelligence, including foreign FIUs. Fipo uses secure and protected channels for dissemination.

Incoming requests pass by the request desk (and are rerouted via the desk if an officer is contacted directly) so that all requests pass by the same channel. A coordinating officer makes a first assessment and then distributes the request to the person best suited to answering it. Answers to requests are forwarded to law enforcement or investigative authorities in the form of intelligence documents.

Criterion 29.6- Fipo is part of the NOA and is subject to security requirements that are established in the Security Protection Act (1996:627), internal service regulations, etc. Fipo's operative information

is subject to the requirements in Chapter 18 of the Public Access to Information and Secrecy Act (2009:400), which means that all intelligence information is confidential.

All Fipo employees undergo security screenings that establish if the person is suitable for work of importance for the security of the nation and of significant anti-terrorism importance. The person cannot commence work in such sectors until the screening is complete. Security screenings are subsequently performed repeatedly. New employees undergo special security training that covers methods for secure information management, legislation regulating how to store information and which information may be stored, access to registers, management and sharing information, etc. Fipo has facilities in the same building as NOA, but has its own shell protection where only Fipo employees with security clearance have access to the facilities. Visitors are accompanied, and access to the ML register is limited to Fipo employees.

Criterion 29.7- Fipo is a law enforcement FIU, established as an independent section within the National Operations Department (NOA) of the Police Authority. The Police Authority is itself operationally independent of the Swedish Government (*Instrument of Government 1974:152*), and has its operational autonomy established in law and administrative practice. The Police itself meets elements (a), (b), and (d) of this criterion. Fipo has sufficient operational independence and autonomy from the rest of the Police Authority. Fipo relies on the IT tools provided by the Police Authority (which are not fully adequate for an FIU) and at the time of the onsite visit was not able to change them despite having noted the need to improve them.

NOA has responsibility for intelligence activity related to money laundering and terrorist financing (Rules of Procedures for the Police Authority, Ch.3, s.19), while Fipo has functional responsibility for the intelligence activities of the Police Authority as regards money laundering and terrorism financing (Administrative Procedures for NOA, s.2.6.2). Fipo is headed by a Head of Section, and Chapter 5, Section 8 of the Rules of Procedure sets forth that each Head is mandated to make decisions in accordance with his/her area of responsibility, unless otherwise stated in any other policy document or statute. The FIU has the authority to make autonomously a decision to analyse; and to request and disseminate specific information.

As regards the ability to make arrangements or engage independently with other domestic authorities, Fipo may interact and exchange information on an ad hoc basis through the desk unit. Fipo can engage with foreign counterparts autonomously to exchange information. Fipo can do this with FIUs within the EU and Egmont without a formal agreement. When there is a need for formal agreements or bilateral agreements with other states, Fipo can engage with these after receiving a mandate from the Government Offices.

The Head of an organisational unit is responsible for deciding on financial matters in accordance with the allocated budget. The budget is allocated every year to the Police Authority, which then develops its own activity plan and follow-up on the basis of the Government's directions. At the time of the onsite visit, Fipo had obtained sufficient funding for the development of adequate IT tools, but not yet started up the project.

Fipo's staff is dedicated only to the FIU, not shared with other police units, and all of Fipo's functions are kept separate from other activities within the Police Authority. Fipo can make arrangements or

engage independently with other domestic competent authorities; or engage directly with foreign counterparts.

Criterion 29.8- Fipo has been a member of the Egmont Group since 1995.

Weighting and Conclusion:

Most criteria are met. The way Fipo currently conducts strategic analysis is not sufficient to meet the requirements of C.29.4.

Sweden is largely compliant with R.29.

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

In its 3rd MER, Sweden was rated largely compliant with regard to the responsibilities of law enforcement authorities. The deficiency related to resource issues and effectiveness, which is not assessed in this section under the 2013 Methodology. The new Recommendation 30 contains much more detailed requirements.

Criterion 30.1 – Sweden has a broad range of authorities responsible for investigating and prosecuting ML offences. The law enforcement authorities that have responsibility to investigate money laundering, associated predicate offences and terrorist financing are: the Police Authority, the Swedish Prosecution Authority, the Swedish Economic Crime Authority, and the Security Service. The Tax Agency and Customs have investigative duties and may also be involved in certain ML cases.

- Decisions to initiate a preliminary investigation are made by the *Swedish Police Authority*, the *Swedish Security Service (Säpo)* or the prosecutor (Code of Judicial Procedure Ch.23). If the investigation has been initiated by the Swedish Police Authority or the Swedish Security Service and the matter is not of a simple nature, the prosecutor assumes responsibility for conducting the investigation as soon as someone is reasonably suspected of the offence. The prosecutor also takes over the conduct of the investigation if special reasons so require.
- Prosecutors within the *Swedish Prosecution Authority (SPA)* lead criminal investigations related to serious crime (which includes ML cases) and make decisions about prosecutions and coercive measures. All individual prosecutors should be competent to manage ML cases. Investigations that require international cooperation, special methods as well as cases relating to serious ML that might require special methods and/or comprehensive international cooperation should be led by the International Public Prosecution Offices.
- ML cases that relate to financial crimes (such as including accounting offences, tax crimes, crimes related to bankruptcy, crimes on the financial market and EU fraud) are dealt with by the *Swedish Economic Crime Authority (EBM)*.
- ML investigations are then conducted by the *Police Authority* under the leadership of the prosecutor. The Police Authority is organised, since 1 January 2015, with seven

police regions and the National Operations Department (NOA). Each of the seven police regions, as well as the NOA, has responsibility for investigating money laundering cases within their region, with NOA focusing on aggravated organised crimes. Within the NOA, dedicated intelligence units carry out the investigations, intelligence and surveillance. At the request of the prosecutor, civil investigators (economists and analysts in EBM for example) and the Tax Fraud Investigation Unit of the Tax Agency may also participate in the investigation.

- Suspected acts of terrorism or TF are processed by prosecutors at the *National Security Unit*, where they are assisted by the *Security Service*. The Security Service (Säpo), an independent authority since 1 January 2015, is responsible for fighting terrorism, including conducting CFT investigations.
- The *Tax Fraud Investigation Unit within the Swedish Tax Agency* conducts criminal investigation on request of the prosecutor in cases of tax and accounting crimes, but also related crimes such as ML and bribing. Swedish Customs investigates crimes pursuant to the Act on Penalties for Smuggling and receives reports on travellers who bring more than EUR 10 000 in cash into or out of the EU.

Criterion 30.2 – Law enforcement investigators are obliged to pursue investigation of any related ML/TF offences. This obligation stems from the Code of Judicial Procedure, which requires the police, prosecutors or the Security Service to initiate a criminal investigation as soon as there are reasons to believe that a crime subject to prosecution (which includes ML/TF) has been committed (Code of Judicial Procedure, Ch.23, s.1 and 3).

Criterion 30.3 – The law enforcement bodies noted above have the authority to identify, trace, and initiate the freezing and seizing of property. Sweden practices asset-focused law enforcement, which considers issues of asset tracing and confiscation at an early stage of each investigation. This is supported by two dedicated asset recovery offices, located within the Police Authority (NOA) and the Swedish Economic Crime Authority (EBM), consisting of staff specialised in asset recovery.

Criterion 30.4 –In Sweden, all financial investigations of predicate offences are conducted by law enforcement authorities or those authorities with investigative powers (including tax and customs authorities).

Criterion 30.5 – All corruption offences and any associated money laundering offences are investigated by the National Anti-Corruption Unit - a specialised prosecution unit within the Swedish Prosecution Authority. Sweden also has a National Anti-Corruption Group within the Police Authority, responsible for the investigation of corruption offences. These units have the same investigative powers as their non-specialised counterparts. Cases of TF arising from corruption are investigated by Säpo.

Weighting and Conclusion:

Sweden is compliant with R.30.

Recommendation 31 – Powers of law enforcement and investigative authorities

In its 3rd MER, Sweden was rated compliant for old Recommendation 28. The new Recommendation 31 contains much more detailed requirements in the area of law enforcement and investigative powers.

Criterion 31.1- Law enforcement and other investigative authorities responsible for investigating ML, predicate offences, and TF are able to obtain access to all necessary documents and information for use in investigations and preliminary investigations that have advanced so far that a person is reasonably suspected of the offence, and have a range of tools available to ensure this, including:

- *Production orders* – Any person who possesses a piece of written documentation that might constitute evidence is obliged to present it to the law enforcement authority, under penalty of a fine (Code of Judicial Procedure, Ch.38, ss.2 and 4). The suspect or any related person is not obliged to disclose such information. If not presented voluntarily, the court can nonetheless subpoena the document and obtain it through search of premises and seizure (see below). Under the AML/CFT legislation, the FIU can obtain upon request any information deemed necessary for an ML/TF investigation from reporting entities or whoever operates a gambling venture (AML/CFT Act, Chapter 3, s.1). These entities should provide the requested information without delay, under penalty of a fine (AML/CFT Act, Chapter 7).
- *Search of persons and premises* - The investigative authorities have the powers to conduct search of persons and premises in case of offences punishable by imprisonment (Code of Judicial Procedure, Ch.28). These powers generally apply to the suspected person and his/her premises, but can be extended to other persons/premises in certain circumstances (if there is extraordinary reason to assume that an object subject to seizure or custody will be discovered, if it is of importance for investigation of the offence, the offence was committed in those other premises or the suspect was apprehended there). The decision to use those powers is made by the leader of the investigation, the prosecutor or the court. The police may decide to conduct a body search or the search of the premises in case delays would lead to an increased risk.
- *Taking witness statements* -The competent authorities have the powers to question persons, even before the preliminary investigation (Code of Judicial Procedure, Ch.23, s.3). They can also request witness statements when there are reasons of particular importance (s.9). A person, who refuses to provide information with regard to circumstances of importance for the investigation and is instructed to act as a witness in court, may be interviewed by the leader of the investigation in court (s.13). A witness who refuses to take an oath, testify or respond to a question may be subject to a conditional fine or imprisonment up to three months (Ch.36, s.21).
- *Seizure and obtaining evidence* - Competent authorities have the power to seize any object, including written documents, that can be reasonably presumed important to a criminal investigation, or that may be the proceeds from a crime or subject to criminal

forfeiture (Code of Judicial Procedure, Ch.27, s.1). A written document may not be seized if the document is in possession of a person who has a duty of confidentiality (S.2). The decision on seizure is made by the leader of the investigation, prosecutor or court. Police officers may make this decision if a delay is associated with risk. In such case, a report should be immediately filed to the prosecutor or leader of the investigation who will decide whether to uphold the seizure.

With regard to lawyers and other qualified legal practitioners, the duty of confidentiality covers confidential information received in the course of the exercise of his or her profession (Statutes (Charter) of the Swedish Bar Association, Ch.34). According to Swedish case law it is prohibited to do search and seizure of written documents in the possession of an advocate at a law firm (NJA 1977 p. 403, NJA 1990 p. 537, NJA 2010 p. 122 and of the Supreme Administrative Court; in the Annual Reporter of the Supreme Administrative Court, RÅ 2001 ref. 67 I and II, and the judgment from 28 February 2012, case number. 7066-10).

Criterion 31.2 – Competent authorities conducting investigations of gross ML offences and TF offences have access to a wide range of investigative techniques, including: secret interception of electronic communication (Code of Judicial Procedure, Ch.27, s.18), secret surveillance of electronic communication (s.19) secret camera surveillance (s.20a), secret room interception (bugging) (s.25a), and interception of post (s.9). The material that derives from these types of investigative techniques during the preliminary investigation may be used fully as evidence in the trial for the crime for which the measure was taken (an ongoing preliminary investigation is as a main rule a criteria for the use of secret surveillance). When secret investigative techniques are used while investigating more serious offences, information from such investigative techniques often can be used when investigating a money-laundering offence or a terrorist financing offence (Code of Judicial Procedure Ch.27, s.23).

The decision to use these techniques must be made by a court, on request by the prosecutor. If the delay in obtaining permission would harm the investigation, the prosecutor may grant permission, and he/she should report the fact to the court for confirmation (s.21). All enforcement tools are subject to the principles of purpose, need and proportionality, and their use is limited to specific circumstances, defined by the maximum sentence applicable to the crime being investigated: interception of communications and camera surveillance can be used only in the investigation of crimes punishable with not less than two years of imprisonment, while bugging can be used only in the investigation of crimes punishable with not less than four years of imprisonment. Since money laundering offences carry a penalty of up to two years of imprisonment, it appears that these techniques cannot be used in the investigation of ML, unless the ML offence is presumed to be gross.

There are separate provisions which allow the use of the techniques above for intelligence purposes to prevent particular serious offences, including terrorist offences (Act on Measures to Prevent Certain Particularly Serious Crimes). The permission to use these techniques is issued by the Stockholm District Court on request by the prosecutor. If the delay in obtaining the permission would significantly limit the ability to prevent the offence, the prosecutor may grant the permission pending the court's decision. The police, customs, and secret services can collect information for

intelligence purposes under certain circumstances from any person with an electronic communication network or device (Act on Collecting Information about Electronic Communications in the Law Enforcements Agencies' Intelligence Activities). Other techniques that can be used in ML/TF investigations are the ability to secure electronic information that is stored in computers and similar devices (mirroring), infiltration, provocative measures and technical surveillance methods. The Swedish authorities indicated that investigative authorities can use "controlled delivery". A request for a controlled delivery in Sweden is dealt with/decided by a prosecutor.

Criterion 31.3 – Competent authorities can obtain banking information directly from credit institutions during the course of an investigation or in a matter regarding legal assistance in a criminal case (Banking and Financing Business Act, Ch.1, s.11). The Swedish authorities have indicated that on average it takes one week to obtain the required information from credit institutions, and that in an urgent case it is often possible to receive an answer earlier than that. It should be noted that there is no centralised register of bank accounts in Swedish banks. If in possession of the account number, the investigative authorities can retrieve the name of the bank and the branch. In case only the name of the person is available, it would be difficult to identify in a timely manner whether the person holds a bank account.

The authorities can request the credit institution not to disclose to the customer or third-party that information was provided, or that an investigation or a matter regarding legal assistance is pending (s.12). Such a prohibition may be issued if it is necessary to avoid compromising a criminal investigation or to fulfil an international agreement.

The Tax Agency can also collect information from various sources, including from credit institutions, for the purposes of clarifying tax issues (Tax Procedure Act, Ch.40). Investigative authorities can request the Tax Agency to obtain information from the tax database in accordance with the Public Access to Information and Secrecy Act.

Criterion 31.4 – The FIU is an integral part of the Police Authority, and all competent authorities investigating ML, TF, and associated predicate offences are able to ask for all information collected and held by the FIU. The Tax Agency and the Economic Crime Authority have each designated a liaison officer in the FIU to work on intelligence and investigatory operations.

Weighting and Conclusion:

Law enforcement authorities have many compulsory powers to obtain all necessary documents and information for money laundering investigations. However, some investigative techniques can be used only for serious offences. The absence of a centralised register of bank accounts in Sweden, or of other mechanism, makes it difficult for the authorities to identify assets in a timely manner.

Sweden is largely compliant with R.31.

Recommendation 32 – Cash Couriers

In the third MER, Sweden was rated Non-compliant on Special Recommendation IX due to the lack of an obligation to declare or disclose cash or bearer negotiable instruments while entering or leaving

Swedish territory. The fourth follow-up report of Sweden considered the progress made by Sweden with the introduction at EU level of the *EU Regulation (EC) No 1889/2005 on controls of cash entering or leaving the community* which entered into force on 15 July 2007 and the amendments made to the Customs Act. Recommendation 32 contains new requirements that were not assessed under the 2004 Methodology, but which are assessed under criteria 32.2 and 32.10 of the 2013 Methodology.

Criterion 32.1 – Sweden has implemented a declaration system for incoming and outgoing transportation of cash and bearer negotiable instruments (BNI) by physical persons leaving and entering the EU. The *EU Regulation (EC) No 1889/2005 on controls of cash entering or leaving the community* (EC Regulation) obliges natural persons leaving or entering the EU to declare cash (including bearer negotiable instruments) of a value of EUR 10 000 or more. The EU Regulation is further regulated by Chapter 7a of the Customs Act, the Customs Ordinance and the Guidelines for Customs Activities. Sweden has however not implemented a system to require declaration or disclosure for physical transportation of cash and BNI through mail and cargo.

Sweden has no mechanism to declare or disclose incoming and outgoing cross-border transportation of cash and BNI within the EU.

Criterion 32.2 – Sweden has implemented a written declaration system for all travellers carrying amounts above a threshold (EUR 10 000). The declaration must be made in writing on a specified Cash Declaration Form. As of 11 March 2016, the declaration form is also available electronically via an application for mobile telephones.

Criterion 32.3 – Sweden does not implement a disclosure system

Criterion 32.4 – In order to check compliance with the obligation to declare, Customs may examine means of transport and baggage (Customs Act, Ch.7a, s.3). If there is reason to assume that an individual has not fulfilled their obligation to declare, the individual may be subjected to a body search to determine whether they are carrying any cash (s.4). Customs does not have the powers to obtain information from the carrier with regard to the origins of the cash or BNI and their intended use; nonetheless the Police can obtain this information. If necessary, Customs would request the Police to intervene and would hold the individual until the Police's arrival.

Criterion 32.5 – Failure to comply with the customs legislation or the obligation to declare cash and BNIs is a customs offence punishable by a fine (Customs Act, Ch.10, s.1). Fines are applied on the basis of a day fine system ranging from 30 to 150 day fines (see c.3.9 above for an explanation of the day fine system). The Swedish authorities have indicated that the penalty for failure to declare is usually 50 day fines. The amount is determined by a combination of the seriousness of the crime and the financial situation of the person liable.

Criterion 32.6 – The Swedish authorities have indicated that Customs reports every week all information from declarations of cash transportations across the border to the FIU. This is done through an excel sheet that is maintained by Customs and transmitted to the FIU via encrypted email. An initial assessment is made by Customs and is included in the excel sheet. If anything irregular or noteworthy is detected, Customs informs the FIU immediately.

Criterion 32.7 – Customs and Police collaborate when, for example, to obtain additional information on the cash or when cash should be seized. Customs collaborates with Fipo via a weekly excel sheet, as described above. At the moment, the mechanism only allows for information exchange with Fipo.

Criterion 32.8 – Customs has the power to retain cash if the person fails to comply with the obligation to make a declaration (EC Regulation, art.4) and also when necessary to carry out a control (Customs Act, ch.7a, s.5). If the control identifies a false declaration, the sanction is a fine and cash cannot be restrained. Nevertheless, if a ML/TF or a predicate offence is suspected, Customs can contact the Police who can act on suspicion of crime and seize the cash. The Police can retain cash after decision from a prosecutor or a police inquiry leader (Act on Criminal Responsibility for the Financing of Particularly Serious Crime in some Cases (2002:444) sections 8–9). The decision is usually taken during a phone call. The Police can also decide to retain cash on immediate danger when there is no time to do a phone call or there is a risk that the money or the suspect may leave. This is frequently used by the Police when they e.g. find large amounts of cash in cars, and the suspect cannot give good explanation why the cash is in their custody.

Criterion 32.9 – Within the EU, Customs can exchange information on declarations and cases of non-fulfilment with other customs via a number of EU mechanisms (Council Act 98/C 24/01 of 18 December 1997, the Convention on mutual assistance and cooperation between customs administration OJ C 24, 23.1.1998, and the Council Regulation (EC) No 515/97 of 13 March 1997). Outside the EU, the FIU receives information from Customs and can exchange it with its foreign counterparts.

All information from Cash Declaration Forms is maintained for three years, which includes the amount of currency or BNIs declared and the identification data of the carrier (Regulation 1889/2005 Art. 6 and 7).

Criterion 32.10 – Customs has in place measures to ensure the confidentiality of the information collected through the declaration system (Public Access to Information and Secrecy Act (2009:400), Chapter 27, sections 2–3).

Criterion 32.11 – A person who does not fulfil his/her obligation to declare cash or who submit incorrect information commits a customs offence and can be fined from 30 to 150 day fines (Customs Act, ch.10,s.1). Cash cannot be seized or confiscated because of mere failure to fulfil the obligation to declare cash. If there is a suspicion of ML/TF or a predicate offence, Customs can contact the Police who can seize the cash in order to perform further investigation. A person who is carrying out a physical cross-border transportation of currency or BNIs that are related to ML/TF or predicate offence may be subject to criminal sanctions (under the AML/CFT Act or other provisions of the Penal Code).

Weighting and Conclusion:

The legislation does not cover cash couriers within the EU borders, which is a significant issue considering the risks of cross-border money laundering with some EU countries.

Sweden is partially compliant with R.32.

Recommendation 33 – Statistics

In its 3rd MER, Sweden was rated partially compliant with R.32.

Criterion 33.1-

(a) Sweden has comprehensive statistics on STRs received and disseminated, with breakdown of categories and sub-categories over the past 7 years.

(b) Statistics for reported ML/TF, investigations, prosecutions and convictions are collected and maintained. [60]

(c) Statistics are available for the number of seizure decisions for the last three years, and number and amounts for claimed amounts (hereunder confiscation). However there are very limited breakdowns of the values, and in several instances they do not cover the past five years.

(d) The statistics for FIU cooperation is broken down by countries, over 3 years for outgoing requests and 5 years for incoming requests. The breakdown of MLA is not by country and is limited by year, while international Cooperation through the Central Authority is not broken down to ML and TF, or country, which makes it of very limited use.

Weighting and Conclusion:

Sweden is largely compliant with R.33.

Recommendation 34 – Guidance and feedback

In its 3rd MER, Sweden was rated largely compliant with R.25, noting as a deficiency that there is a lack of AML guidelines for all the sectors.

Criterion 34.1- The authorities have undertaken several outreach programmes to FIs and DNFBPs. These include conferences and seminars by LI, EBM, FSA, FMI, SBA, and CABs, industry meetings by the STA and FMI, training by Säpo, and other activities by Fipo and the FSA to raise awareness of AML/CFT among their supervised entities. Information on AML/CFT can also be found on the websites of the Swedish Government and the FSA.

The FSA, FMI, LI, and RN provide feedback on AML/CFT deficiencies to supervised entities in the course of their supervision, and where sanctions are involved, publishes them to serve as guidance for other FIs. For example, the FSA publishes all decisions that results in a sanction on its website, which serves as "case law" for financial institutions in their implementation of AML/CFT requirements.

FMI and the CABs (but not all supervisors) also provide a broad range of outreach and guidance about the application of AML/CFT measures to entities that they supervise.

60 Note however that there are challenges of comparing statistics because of new legislation introduced in 2014. Also, the old provision of "handling stolen goods" covers acts where most cases are not indeed money laundering, which means the numbers are of limited use in this assessment.

Fipo publishes an annual report containing statistics and information on current topics such as new legislation, organisational changes and typologies. Fipo has also developed a simpler brochure for the obliged entities. In addition, the authorities provide public information on the development of criminality in several ways, e.g. reports published by the Police Authority and Brå.

Fipo conducts regular visits to obliged entities to provide feedback on submitted STRs and to exchange experiences of trends and modes in ML, and with Säpo for TF. Fipo has designated contact officers for obliged entities so as to create and maintain long-term relationships. The FSA has since 2015 included a qualitative review of STRs in its inspections with the purpose to examine if the STRs that are filed with Fipo are of acceptable quality and are filed within a reasonable time frame.

Weighting and Conclusion:

Sweden is largely compliant with R.34.

Recommendation 35 – Sanctions

In its 3rd MER, Sweden was rated largely compliant with R.17 due to limitations in the range of administrative sanctions available for FIs, directors, and senior management.

Criterion 35.1-

R.6 – Breaches of obligations and prohibitions in EU Regulations on economic sanctions, leads to sanctions ranging from a fine to up to two years in prison for "normal degree" breaches committed with intent to up to four years for "gross" cases. If the breach was committed with gross negligence, the penalty ranges from a fine to imprisonment for up to six months. *Act on Certain International Sanctions (1996:95) S.8*. For FIs, the FSA is able to impose a range of administrative sanctions on FIs that do not comply with EU Sanctions Regulations, including in relation to the obligation to report freezing actions (See sub-section on R.9 to R.19 below).

R.8 – There is no designated authority for administering sanctions with regard to R.8, although different authorities (such as the STA, Swedish Fundraising Control, SIDA, and the CABs) monitor compliance with obligations regulated in applicable laws, such as submitting information, annual reports etc. and are vested with the power to apply limited sanctions (injunctions, delay fees).

R.9 to 19 – As the supervisor and licensing/registration authority the FSA is able to impose a range of administrative sanctions on FIs that fail to comply with AML/CFT requirements, such as the ability to give warnings, impose injunctions/prohibitions, and revoke licenses. However, the ability to issue fines is limited to some FIs, and within that subset, some only allow conditional fines. *BFBA (2004:297) Ch.15 sect.1 and 8, IBA (2014:982) Ch.16 sect.2, SMA (2007:528) Ch.25 sect.1 and 9, CFOA (1996:1006) sect.8-11, DTOA (2004:299) sect.15, 18 and 19, IMA (2005:405) Ch.8 sect.1, EMA (2011:755) Ch.5 sect.8 and 25, IFA (2004:46) Ch.12 sect.1 and 8, PSA (2010:751) Ch.8 sect.8 and 15, AIFMA (2013:561) Ch.14 sect.1 and 24, CCOA (2014:275) sect.20 and 32.*

R.20 to 21 – FIs and DNFBPs may be fined for failure to comply with the requirements for STR filing and tipping-off. The applicable range of fines/sanctions depends on the nature of the business and are the same as for any other violation of the AML/CFT Act. *AML/CFT Act (2009:62) Ch.7 sect.1.*

R.22 to 23 – The supervisors and SRBs of the DNFBPs are able to impose sanctions ranging from the revoking of licenses to warnings, and in some cases the giving of fines. The range of sanctions available differs between DNFBP-types:

- Casinos: LI may issue injunctions and prohibitions, with fines[61], needed for compliance with the Casino Act and its directives, or the AML/CFT Act (2009:62). The casinos' permits may be revoked or amended if the conditions or regulations are not complied with or there are other reasons for doing so. *Casino Act (1999:355) sect.14b, 14c, 15*
- Real estate agents: FMI may issue warnings or reminders to estate agents, and revoke the licences. *Estate Agents Act (2011:666) sect.29*.
- DPMS/Legal professionals/Tax advisers/TCSPs: CABs may issue injunction or termination orders with conditional fines guided by the Default Fines Act (1985:206) which provides for a fine proportional to the economic circumstances of the defendant. *AML/CFT Act (2009:62) Ch.6 sect.7a and sect.*9
- Lawyers: SBA is able to issue warnings, reprimands, or statements, or disbar lawyers. Warnings may be combined with a fine of SEK 1 000 – 50 000 (EUR 110 – 5 500). *Code of Judicial Procedure (1942:740) Ch.8 sect.7*
- Public accountants: For public accountants, RN may revoke their licence, or issue warnings or rectification orders[62]. *Public Accountants Act (2001:883) sect.32 and sect.35*

Criterion 35.2- The board, MD, and their alternates, of banks and securities companies can be liable to sanctions when the FI is found to be guilty of a serious violation of the *AML/CFT Act (2009:62). BFBA (2004:297) Ch.15 sect.1a, SMA (2007:528) Ch.25 sect.1a*. There are no equivalent sanctions for senior management of other FIs.

Sanctions can apply to lawyers who are directors or senior management of law firms for not complying with the AML/CFT Act, who can be sanctioned by the SBA's Disciplinary Committee. For public accounting firms, RN may sanction public accountants in management positions. Senior management in other DNFBPs do not appear to bear personal liability, unless they are themselves personally licenced (e.g. as real estate agents).

Weighting and Conclusion:

Sweden is largely compliant with R.35.

61 The size of the amount is guided by the Default Fines Act (1985:206), and is related to the economic situation of the defendant; effectively, there is no set maximum amount

62 From 17 June 2016 (after the dates of the on-site), the law was updated where RN may sanction public accountants with a maximum fine of SEK 1 million (approximately EUR 105 000), or for registered audit firms, 2% of the annual turnover.

Recommendation 36 – International Instruments

In its 2006 Mutual Evaluation, Sweden was rated LC. The FATF found that the Palermo Convention was not implemented in as far as self-laundering was concerned; the Terrorist Financing Convention was not fully implemented with regard to identification of customers in whose interests accounts are opened, and the lack of adequate measures to ascertain the identity of beneficial owners according to old R.5 (now R.10). These deficiencies have been largely addressed (see C.3.7 and C.10.5).

Criterion 36.1- Sweden is a party to the international instruments covered by this Recommendation: Vienna Convention (ratified on 22 July 1991), the Palermo Convention (ratified on 30 April 2004), the Terrorist Financing Convention (ratified on 6 July 2002) and the Merida Convention (ratified on 25 September 2007).

Criterion 36.2 - Sweden has implemented the relevant articles of these Conventions.[63]

Weighting and Conclusion:

Sweden is compliant with R.36.

Recommendation 37 – Mutual Legal Assistance

In the third MER, Sweden was rated LC for former R.36 and SR.V. The report noted that it was unclear whether Sweden could execute coercive measures relating to requests involving conspiracy to commit basic money laundering, and collecting/providing funds/assets to be used by a terrorist organisation or individual terrorist.

Criterion 37.1- Sweden can provide mutual legal assistance on the basis of the International Legal Assistance in Criminal Matters Act (2000:562) and the Act on International Cooperation in the Enforcement of Criminal Judgements (1972:260). In addition, Sweden performs MLA co-operation within the EU through e.g. the European Judicial Network and Eurojust. Bilateral MLA treaties are in place with Australia (1998), Canada (2000), and the United States (2001).

Dual criminality is generally not required, except for coercive measures (e.g. seizure, search of premises and others) and some investigative techniques (interception and surveillance of telecommunications, secret camera surveillance, bugging, and forensic medical examination of the body of a deceased person). Dual criminality concerning coercive measures is not required in case of MLA with EU members, Iceland and Norway, provided that imprisonment may be imposed by the requesting state.

Criterion 37.2- Sweden has established a central authority that serves as a contact point for MLA in all cases where direct contact between national authorities is not allowed. The central authority is a

63 While Sweden has implemented all the other elements of the conventions, an element of the Merida Convention, (Article 29) which obligates countries to provide for the suspension of the statute of limitations where the alleged offender has evaded the administration of justice, is yet to be implemented by Sweden.

sub-division of the Ministry of Justice's Division for Criminal Cases and International Judicial Co-operation.

When a request is received, this division will conduct some formal examination and then pass the request on to a local prosecutor, the Prosecutor-General's Office or to the competent court. In most cases, however, the requests can be sent directly from the requesting authority to the competent prosecutor or court, for example requests from Norway, Iceland, a European Union country, or a country with which Sweden has an agreement providing for clearance for direct contacts. Chapter 2, section 10 of the International Legal Assistance in Criminal Matters Act requires that requests for legal assistance shall be dealt with promptly. The internal directive of the SPA (ÅFS 2007:12) recommends that assistance should be provided within two months.

There are separate case management systems. In-bound and out-bound requests for MLA which are received by the central authority are recorded on a digital case management system, which is maintained by the Division for Criminal Cases and International Judicial Co-operation. MLA requests which are handled through direct contacts between competent authorities and are recorded by the authorities on their digital case management systems. These systems feature registration of all incoming and outgoing documents of any significance and allows for searches by e.g. case classifications and countries. It is possible to monitor the progress of a specific request.

Criterion 37.3- Section 14 of the International Legal Assistance in Criminal Matters Act establishes the grounds for refusals of a request for legal assistance and these do not pose unreasonable or unduly restrictive conditions. One ground for refusal is quite broad ("circumstances are otherwise such that the request should not be granted"), however, the Swedish authorities have indicated that this provision is used only when the other grounds for rejection are not applicable but the request should nevertheless not be approved in view of the circumstances of the case. The Swedish authorities have also indicated that the provision is to be applied restrictively and is used very rarely in practice (only once between 2000 and 2014). If an international agreement conflicts with the legal grounds for refusal established in the Act, the international treaty will prevail. If a prosecutor or a court considers that a request should be refused on any of the grounds mentioned in the Act, the request will be handed over to the Government for a final decision.

Criterion 37.4- Requests for legal assistance cannot be rejected on the sole ground that the offence is considered to involve fiscal affairs, or on the ground of confidentiality attaching to FIs. The International Legal Assistance in Criminal Matters Act specifically makes reference to a number of Swedish statutes that oblige FIs to provide information (Ch.5, s.10).

The general provisions of the International Legal Assistance in Criminal Matters Act are applicable when it comes to MLA requests concerning DNFBPs; therefore, requests cannot be rejected on the sole ground that the offence is considered to involve fiscal matters or on the ground of confidentiality, except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies in accordance with national law.

Criterion 37.5- Sweden's legislation protects the confidentiality of MLA requests. The Public Access to Information and Secrecy Act (2009:400) establishes that secrecy applies to information that concerns international requests for legal assistance if it can be assumed that the request was made on the condition that the information would not be disclosed (Ch.18, s.17).

Criterion 37.6- According to the International Legal Assistance in Criminal Matters Act dual criminality is not a requirement when the request does not involve coercive actions (Ch.2, s.2).

Criterion 37.7- Dual criminality is required for coercive measures. Under Swedish law, dual criminality is satisfied if the act to which the request relates corresponds to an offence in Sweden. It is not required that the offence should be placed within the same category of offences or that the offence should be denominated by the same category. It is sufficient if an underlying conduct corresponds to an offence under Swedish law.

Criterion 37.8- The underlying principle of the law on MLA in Sweden is to equate a foreign criminal investigation or proceeding with a national case. A request from a foreign country is handled in the same way as an investigation being carried out domestically. The Swedish authorities are also able to provide for mutual legal assistance in the form of other powers and investigative techniques other than those mentioned under R.31 (that some investigative techniques can be used only for gross ML cases).

Weighting and Conclusion:

Sweden meets most criteria of R.37, however there are some limitations to the use of investigative techniques in some cases where the money laundering offence would not be considered gross.

Sweden is largely compliant with R.37.

Recommendation 38 – Mutual Legal Assistance: Freezing and Confiscation

In the third MER, Sweden was rated LC with former R.38 and SR.V. The main deficiencies were the failure to establish an asset forfeiture fund, and, since dual criminality was required, uncertainty as to how effectively Sweden could execute coercive measures relating to requests involving collecting/providing funds/assets (for any purpose) to be used by a terrorist organisation or individual terrorist.

Criterion 38.1 – The International Legal Assistance in Criminal Matters Act (2000:562), chapter 4 is applicable to provisional attachment, seizure and search of premises.

Chapter 1, Section 2 of the International Legal Assistance in Criminal Matters Act is generally applicable with regard to investigative measures. According to Chapter 4, Section 19, property may be seized and transferred to a requesting state if it can be reasonably assumed that the property is of importance for the investigation of an act; if the property can be reasonably assumed to have been expropriated from someone by a criminal offence; or if property ought to be confiscated by reason of a criminal offence and the property could have been forfeited under Swedish law in a trial in Sweden and there are special reasons to transfer the property to the requesting state.

With respect to enforcement of foreign decisions on confiscation, the Act on International Cooperation in the Enforcement of Criminal Judgements (1972:260) is applicable. Pursuant to Section 1, sanctions involving confiscation may be enforced in Sweden insofar as required by an agreement which Sweden has entered into with another state. Within the EU, the Act on the Recognition and Enforcement of Confiscation Orders within the EU (2011:423) is applicable. The law

implements the Council Framework Decision 2006/783/JHA on the application of the principle of mutual recognition to confiscation orders. Furthermore, Section 1 of the Act (1963:193) on cooperation with Denmark, Finland, Iceland and Norway on the enforcement of sentences allows for enforcement of Nordic sentences including confiscation. Requests for confiscation from foreign countries can be given effect according to the provisions of these laws.

Under section 18 of the Act on International Cooperation in the Enforcement of Criminal Judgments, if a request for the enforcement of a European criminal judgment has been made, property that has been declared forfeited through the judgment may be confiscated if such confiscation would have been possible under Swedish law in proceedings in Sweden.

As regards freezing, under chapter 3, sections 8–9 of the AML/CFT Act (2009:62), Fipo may, after a request from its foreign counterpart, make an interim decision to freeze property in the form of money, claim or any other right subject to ML or TF that is held by an obliged entity. Such a decision will thereafter be subjected to final assessment by a public prosecutor.

Also, within the European Union, the Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence applies. Pursuant to the Act on Recognition and Execution of European Union Freezing Decisions (2005:500) a request for executing a freezing order from an EU member state can be sent directly to a Swedish prosecutor

Criterion 38.2– The main rule is that confiscation is related to a criminal conviction or a decision by a public prosecutor within a pre-trial investigation. The Swedish authorities have indicated that Chapter 36, sections 1–6 and 14 of the Penal Code (1962:700) in conjunction with section 3 of the Act on Confiscation in Certain Cases (1986:1009) provide the means for confiscation without a criminal conviction or decision by a public prosecutor in the particular situation when lawful prosecution or conviction cannot be undertaken, due to e.g. the statute of limitations or the death of the perpetrator, provided that a summons was served within five years from the time when the crime was committed. While a non-conviction based confiscation order made within the context of a criminal proceeding in a third country may be enforced in Sweden, a foreign non-conviction based confiscation order made within the context of a civil or an administrative procedure cannot be enforced in Sweden.

In accordance with the Act on the Procedure on Forfeiture in Certain Cases etc. (1986:1009) confiscation is also feasible when no conviction is possible where perpetrators are unknown. Swedish authorities also indicated that in addition to existing provisions on non-conviction based confiscation in the Penal Code, the Government proposes certain legislative amendments in order to transpose the provisions on non-conviction based confiscation in the Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union into national law.

Criterion 38.3– Sweden refers to Eurojust and Europol with respect to arrangements enabling co-ordination of seizure and confiscation actions with other EU countries. The administration of frozen or seized property is handled by the police or by the Swedish Enforcement Agency (Chapter 27, section 10 of the Code of Judicial Procedure). However, as mentioned in R.4, property can be disposed of, but no management mechanism exists as such, for example when it is necessary to run affairs or administer the property more actively.

Criterion 38.4– Under Chapter 5, section 11 of the International Legal Assistance in Criminal Matters Act, the Government may decide that property or its value that is forfeited by a Swedish order that has become final and non-appealable shall completely or partially be transferred to another state that has provided Sweden with such legal assistance as is referred to in that Act during a preliminary investigation or trial or that in another way has provided information or assistance that has been of significance for investigating the offence. Section 36 of the Act on International Cooperation in the Enforcement of Criminal Judgments (1972:260) includes provisions on the transfer to another state of property forfeited by a foreign order.

Within the EU the following also applies: under Section 18 Act on the Recognition and Enforcement of Confiscation Orders within the European Union (2011:423), funds recovered accrue to the Swedish State if the amount is less than EUR 10 000. In other cases, funds recovered are divided equally between the Swedish State and the other EU member state. Following an agreement with the other member state, the Government may decide on a distribution other than that given in the first paragraph.

Weighting and Conclusion:

Sweden fulfils most of the obligations for R.38, however, a foreign non-conviction based confiscation order made within the context of a civil or an administrative procedure cannot be enforced in Sweden. There is no systemic way to manage all confiscated property (see R.4).

Sweden is largely compliant with R.38.

Recommendation 39 – Extradition

In the third MER, Sweden was rated compliant with former R.39 and largely compliant with former SR.V. The main deficiency was that the application of dual criminality might create an obstacle to extradition in cases involving FT activities that were not specifically criminalised in Sweden (collecting/providing funds/assets to be used (for any purpose) by a terrorist organisation or individual terrorist). The underlying gap in the TF offence has since been addressed (c.f. C5.2).

Criterion 39.1- ML and TF are extraditable offences (Extradition for Criminal Offences Act, s.4). Requests for extradition received by the Ministry of Justice are monitored through the case management system used for MLA requests (see R.37 above). The Prosecution Authority and the courts have individual case management systems in relation to their part of the handling of the requests for extradition. The decision on extradition is eventually made by a court, on proposal of the prosecutor who decides to implement the international arrest warrant. The prosecutor communicates to the court the request for extradition and the court must without delay summon the parties to a hearing and decide whether the coercive measures should be sustained or revoked.

The conditions related to extradition depend on whether the requesting state is i) a state from outside the Nordics and the European Union, ii) a state within the Nordics or iii) a member state of the European Union. Sweden does not place unreasonable or unduly restrictive conditions on the execution of requests (Extradition for Criminal Offences Act; Nordic Arrest Warrants are regulated in

the Act on Surrender from Sweden pursuant to a Nordic Arrest Warrant; European Arrest Warrants are regulated in the Act on Surrender from Sweden pursuant to a European Arrest Warrant).

Criterion 39.2– As a general rule, the law prohibits Swedish nationals from being extradited (Extradition for Criminal Offences Act (1957:668)). This prohibition can be overridden with respect to Nordic states, EU member states (Extradition for Criminal Offences Act (1957:668), s.1), International Tribunals for Violations of International Humanitarian Law and the International Criminal Court (Act on Surrender from Sweden pursuant to a Nordic Arrest Warrant, Act on Surrender from Sweden pursuant to a European Arrest Warrant, Act on Co-operation between Sweden and the International Tribunals for Violations of International Humanitarian Law (1994:569), Act on Co-operation with the International Criminal Court (2002:329)). In cases where Sweden does not extradite its own nationals, it will at the request of the country seeking extradition submit the case without undue delay to its competent authorities for the purpose of prosecution of the offences set forth in the request. This principle was recently applied in a case concerning a Chilean request for extradition of a Swedish national (ref JuBC2015/00344/BIRS).

Criterion 39.3– Dual criminality is generally required for extradition to non-Nordic states. Extradition may be granted only if the act for which it is requested corresponds to an offence for which imprisonment for one year or more is prescribed by Swedish law (Extradition for Criminal Offences Act (1957:668), s.4). The Swedish authorities have confirmed that it is the act/conduct that constitutes the criminal offence not the categorisation or denomination of the offence which determines whether or not the requirement concerning dual criminality is satisfied. Within the EU, dual criminality is required but a considerable exemption to this requirement are the so called "list crimes," included in a list of serious offences punishable by deprivation of liberty of at least three years. In these cases, extradition will take place regardless of the absence of dual criminality and with no consideration to the denomination of the offence, or other assessment of the offence. Examples of serious offences subject to the European Arrest Warrant list are participation in a criminal organisation, laundering of the proceeds of crime and terrorism.

*Criterion 39.4***–** When a person sought consents to extradition there is a simplified extradition mechanism in the sense that the procedure is shortened. Simplified extradition mechanisms are also in place in the context of the European Arrest Warrant and the Nordic Arrest Warrant.

Weighting and Conclusion:

Sweden is compliant with R.39.

Recommendation 40 – Other Forms of International Cooperation

In the third MER, Sweden was rated compliant for R. 40, provisions of R.40 relating to former SR.V were considered sufficient, and former R.32 was rated partially compliant.

*Criterion 40.1***–** The competent authorities that can provide international cooperation include the Police Authority (via contact points in the unit for international police cooperation – IPO), Fipo, Säpo, Prosecution Authority, EBM, and the STA (in general, the STA investigates cases under the leadership

of a prosecutor; as such they are able to obtain international police cooperation through the Swedish SPOC). All these authorities have frameworks for a lawful basis and a number of well implemented systems that allow them to exchange information on all levels of law enforcement, from intelligence to investigations. This applies to exchanges of information without prior requests, but also management of incoming and outgoing information requests.

Criterion 40.2 –

(a) The Police Authority, Fipo, Säpo, the Prosecution Authority and EBM have lawful basis for providing international cooperation. The Swedish authorities have explained that given the mandate of the Police Authority and Fipo, it is implicit that some tasks will require international cooperation. So, an express legal provision allowing international cooperation is generally not required and there are legal possibilities for cooperating internationally in operative matters, i.e. sharing personal data. There are a number of legal provisions explicitly allowing the mentioned authorities to share information with international partners, for example the Police Data Act, and provisions overriding secrecy in the Public Access to Information and Secrecy Act.

The EBM has a firm legal basis for the exchange of information with its foreign counterparts (Penal Code (1962:700) Ch.2).

With respect to Säpo, the authority's Ordinance with Instructions (2014:1103), section 16, provides that Säpo should cooperate with foreign authorities or agencies and multilateral organisations to the extent needed and to be further specified by the government. Section 17 provides that Säpo may enter into international agreements about cooperation with foreign law enforcement, intelligence or security agencies, or other corresponding organs in EU member states.

(b) EBM and the SPA are authorities under the Government and are obliged to streamline not only the work inside the authority but also to make the co-operation between authorities more efficient.

(c) The international cooperation channels' communications systems, i.e. SIENA (Europol) and I 24/7 (Interpol) meet industry standards for information and operation security. Europol is currently (as of 2015) undertaking measures to raise the security classification for SIENA from RESTRICTED to SECRET. This increased security classification will give authorities the possibility to exchange (send and receive) information that requires higher protection and will not affect the use of SIENA for information sharing of documents with a "lower" classification. Communication between prosecutors and the police takes place using electronic communication over encrypted networks. Normally, requests for legal assistance to or from Eurojust are transferred via encrypted networks.

(d) The IPO has procedures for prioritising cases. The main rule is that all incoming requests to IPO should be investigated and prioritised within an hour of receipt. A prioritisation level from 1–3 is applied uniformly over all channels of cooperation. As regards the other competent authorities, a general assessment is that Swedish law enforcement authorities give high priority to international cooperation. This will normally depend on the nature of the

cases as well as many other parameters that feed into the prioritisations of the independent authorities.

(e) All incoming information to IPO is managed in a case management system, which is only accessible to a limited number of civil servants. The system is regulated by the Police Data Act (2010:361). The police part of EBM may use the same channels for international police cooperation as the Police Authority. The same regulations (Police Data Act etc.) apply in these instances. The Tax Agency, in accordance with the Archive Act (1990:782) and Security Protection Act (1996:627) and the SPA have internal procedures and processes for safeguarding the information received including by restricting access of information to a limited number of staff and using encrypted systems.

Criterion 40.3– Sweden can provide international co-operation on the basis of its domestic legislation. Sweden has also entered into treaties to provide cooperation with 20 states.[64] The bilateral agreements further enhance mutual cooperation. The Police Authority has also entered into agreements with foreign law enforcement authorities in EU member states and states that are member of the Schengen area. Outside the EU, the Police Authority can enter into bilateral and multilateral agreements on police cooperation with other Police Authorities after receiving a mandate from the Government Offices.

Criterion 40.4– The Swedish authorities have indicated that feedback is provided upon request from the other authority or in particular circumstances. There is no regular feedback in all matters. No partner complained about the feedback received from Sweden.

Criterion 40.5– There are generally no unreasonable or unduly restrictive conditions on the provision of exchange of information and assistance. Information related to crime-fighting can normally be shared with all authorities that can (or that should) take action on the basis of the information. Fipo shares information with counterparts regardless of the status or nature of the counterpart FIU. Sharing information with authorities with duties other than fighting crime for other purposes could be more difficult unless the exchange is regulated by law.

Criterion 40.6– The Act on International Police Cooperation (2000:343) contains a general regulation in section 3 which stipulates that Swedish authorities should comply with conditions that regulate the use of information or evidence that has been received from another state, irrespective of provisions in other acts or regulations. Thus, safeguards and controls will apply if the requested authority stipulates that the information should only be used for the specific purpose for which it was sought. Furthermore, all work by the Police Authority is controlled and safeguarded by a system of internal and external processes and institutions (i.e. the Chancellor of Justice, the Commission on Security and Integrity Protection, the Data Protection Authority, etc.).

Criterion 40.7– Section 3 of the Public Access to Information and Secrecy Act (2009:400), provides that items of information subject to secrecy under that Act shall not be disclosed to a foreign authority or international organisation, unless: disclosure is made in accordance with a special rule contained in an act or ordinance; or it would be permitted, in a corresponding case, to communicate

64 Bosnia and Herzegovina, Cambodia, Croatia, Denmark, Finland, France, Hungary, Iceland, Kosovo, Malta, Norway, Poland, Romania, Russia, Slovenia, Spain, Thailand, Ukraine, the United States and Vietnam.

the item of information to a Swedish authority and if it is manifestly evident, according to the disclosing authority's examination, that disclosing the item of information to the foreign authority or the international organisation is compatible with Swedish interests.

Competent authorities may refuse to provide information if the requesting competent authority cannot protect the information effectively except where a court decision, a decision by the Government or a legal provision obliges the authority to provide the other authority with the information concerned.

Criterion 40.8– There are legal possibilities to exchange information with foreign counterparts. The applicable provisions are the Police Data Act (2010:361), the Police Data Ordinance (2010:1155) and the Public Access to Information and Secrecy Act (2009:400). Information held by authorities is as a main rule public in Sweden. Information held by Fipo is nonetheless often protected by secrecy. Swedish legislation does provide possibilities to share secret information (Police Data Act, the Police Data Ordinance and the Public Access to Information and Secrecy Act). Section 13 of the Police Data Ordinance establishes that certain information can be shared with a foreign authority responsible for the combatting of money laundering or the financing of particularly serious crime, if it is needed in order for the foreign authority to be able to anticipate, prevent, detect, investigate or prosecute crimes. When there is no applicable rule for exchanging confidential information in these regulations, rules overriding secrecy in the Public Access to Information and Secrecy Act are applicable. The rules that override secrecy are applicable when it comes to for instance requests for banking issues within the framework of cooperation between FIUs.

*Criterion 40.9***–** Fipo (Sweden's FIU) is a Section of the Intelligence Unit of the NOA, part of the Police Authority. Any legal competence given to the Police Authority with regard to international cooperation also applies to Fipo (Police Act (1984:387)

Criterion 40.10– The FIU provides feedback upon request from the other authority or if the circumstances in the particular case provide sufficient reasons therefor. There is no regular feedback, but the stated intention is that this should occur frequently.

Criterion 40.11– Fipo can share all information that arises from analysis with other FIUs. If the information contains personal data, the provisions in section 13 of the Police Data Ordinance (2010:1155) and Chapter 2, section 15 of the Police Data Act (2010:361) permit its disclosure.

Fipo employs the principle of reciprocity for any information that Fipo has access to. However, its ability to obtain additional information to be exchanged is limited to FIU cases where an AML or CFT investigation by the FIU in Sweden is ongoing (see c.29.3 above). Until 2016, Fipo interpreted the requirement to have an investigation in Sweden as a basis to reject the foreign requests to obtain additional information. Since 2016, Fipo changed this interpretation so that it will obtain the information through an "initiative case" (e.g. a case initiated by the FIU on the basis of information available and not in response to a specific STR) if a foreign FIU demonstrates that there is ground for suspicion of a crime. At the time of the onsite visit, this new interpretation was not tested in practice.

*Criterion 40.12***–** As mentioned in c.26.1, the FSA is responsible for the supervision of FIs, which includes for AML/CFT requirements. Within the EU and EEA, the FSA should provide any and all

information that a competent authority in another state within the EEA requires for its supervision (Banking and Financing Business Act (2004:297), Chapter 13, sections 6a and 8).

As regards information sharing outside the EU and EEA, bilateral agreements or MoUs are needed to enable an effective exchange of information. However, it should be mentioned that a bilateral cooperation agreement is not a precondition to exchanging information with an authority of another country. The FSA may, on request, disclose information to an authority if the Public Access to Information and Secrecy Act (2009:400) does not hinder a disclosure. However, a bilateral agreement may in more detail regulate the exchange of information between the authorities, and it may specify how information may be exchanged on a regular basis.

Criterion 40.13– As mentioned in c.40.12, the FSA can exchange information pursuant to the Banking and Financing Business Act and/or bilateral arrangements.

Criterion 40.14 **–** Within the EU, the FSA can exchange any and all information that a competent authority in another state within the EEA requires for its supervision, which means that regulatory, prudential, and AML/CFT information can be provided (Banking and Financing Business Act, Ch.13 and 15).

Criterion 40.15– The Banking and Financing Business Act, Chapter 13, sections 6a–8 oblige the FSA to cooperate and exchange information with foreign competent authorities *to the extent which follows from Sweden's membership in the European Union.* Furthermore, these provisions state that the FSA should disclose such information that a competent foreign authority (within the EEA) needs for its supervision of a foreign credit institution, a foreign financial institute or subsidiary which operates in Sweden.

The Payment Services Act, Chapter 8, section 4 and the Electronic Money Act, Chapter 5, section 4 provide that the FSA should in its supervisory activities cooperate with and exchange information with competent authorities within the EEA[65] including the European Central Bank, national central banks and other competent authorities appointed in accordance with EU law applicable to providers of payment services and issuers of electronic money respectively. The FSA may grant investigative cooperation to foreign counterparts outside the EU on the basis of Article 116 of Directive 2013/36/EU which stipulates that supervisory colleges should include authorities from third countries where appropriate.

Criterion 40.16– Whether information received by the FSA is subject to confidentiality is determined by the provider of the information, i.e. the requested financial supervisor. Where the information is subject to confidentiality, the information will not be used for any purpose other than for that which it was requested. Pursuant to Chapter 30, section 7 of the Public Access to Information and Secrecy Act (2009:400), secrecy applies for information the FSA has received in accordance with an agreement with a foreign state where the agreement is approved by the Riksdag. It is possible to determine in advance if information received by the FSA will be subject to confidentiality. However, if the requested state has not subjected the information to any confidentiality requirements, the

65 Similar provisions are contained in the Swedish Capital Adequacy and Large Exposures Act (2006:1371), Chapter 10, section 9; the Special Supervision of Financial Conglomerates Act, Chapter 6, section; and the Capital Requirements Directive (CRD) 2006/49/EC. Chapter 10, section 10.

information may be used for other purposes, in which case, information received could be used for risk classification purposes by the FSA or within the planning stage of a supervisory activity.

Criterion 40.17– Within the EU, Sweden implemented the Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union. Outside the EU, the legal grounds for disclosing information depends on which type of information is concerned in each individual case. Information may be shared spontaneously or upon request. The provisions in the Police Data Act (2010:361) and regulations in the Public Access to Information and Secrecy Act (2009:400) apply.

Criterion 40.18– There are no legal impediments to the Police Authority's assisting another state upon request with investigations using non-coercive measures. Regulations with regard to international police cooperation can be found in the Act on International Police Cooperation (2000:343) and the Ordinance on International Police Cooperation (2010:705). If a request by a foreign authority involves coercive measures, MLA is needed to collect and exchange the information. If the information in question is obtainable without coercive measures, exchange can normally be granted to the foreign counterpart. The exchange of FIU intelligence is described in other sections of this report.

Criterion 40.19– Within the EU, joint investigations can be conducted on the basis of the Act on Joint Investigation Teams for Criminal Investigations (2003:1174). In addition, the Swedish authorities have indicated that there is an informal and unregulated cooperation, where police and prosecutors interact with representatives of corresponding authorities in other countries, including with non-EU countries.

Criterion 40.20– The Swedish authorities have indicated that Fipo can typically act as intermediary and help competent authorities to reach relevant counterparts in other countries in ML/TF cases, using the "normal" networks for cooperation between FIUs. The basic approach is that if the information has been received from other law enforcement authorities, their permission is necessary before the information is forwarded to external parties. This information is often complemented with information about its origin and any limitations to its use from the original 'owner' of the information. Any information that is received from other FIUs indirectly is managed similarly. It is only forwarded to other authorities with permission from the external partner.

Weighting and Conclusion:

Sweden is compliant with R.40.

Summary of Technical Compliance – Key Deficiencies

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
1. Assessing risks & applying a risk-based approach	LC	• There is no standing authority or mechanism to co-ordinate actions to assess risks. • Some exemptions from the CDD and ongoing monitoring obligations are based on a presumption of low risk, rather than on a specific risk assessment.
2. National cooperation and coordination	PC	• There is no authority or co-ordination mechanism that is responsible for national AML/CFT policies, or for cooperation and coordination on national policymaking between agencies.
3. Money laundering offence	LC	• The sanctions on legal persons, particularly the amount of corporate fines, may not be dissuasive in all cases.
4. Confiscation and provisional measures	LC	• Sweden has no established mechanisms or procedures for managing all seized or confiscated assets, including (potentially) income-generating or perishable assets.
5. Terrorist financing offence	LC	• The maximum level of sanctions which can be applied to a legal person convicted of TF is not proportionate and dissuasive.
6. Targeted financial sanctions related to terrorism & TF	PC	• Sweden does not have either formal procedures or informal mechanisms or practices at national level for considering or proposing designations; • Implementation of targeted financial sanctions (TFS), pursuant to UNSCRs 1267/1989 and 1988 does not occur "without delay." • "EU internal terrorists" are not subject to freezing measures pursuant to UNSCR 1373
7. Targeted financial sanctions related to proliferation	PC	• New TFS related to proliferation cannot be implemented without delay;
8. Non-profit organisations	LC	• Non-Profit Associations and some foundations are not required to register; • There is no explicit requirement for NPOs to know their beneficiaries and associated NPOs • There is no coordination mechanism between the 12 bodies which register or oversee NPOs to identify at-risk NPOs and share information about them.
9. Financial institution secrecy laws	LC	• The restriction on the sharing of information from reviews of suspicious transactions with third parties affects FI's abilities to share such information between business lines or group entities.
10. Customer due diligence	LC	• The requirements for identification of customers that are legal entities do not cover all trust-relevant parties. • The list of categories of entities exempt from basic CDD and ongoing monitoring is not based on an identification of lower risks.
11. Record keeping	C	The recommendation is fully met.
12. Politically exposed persons	LC	• The definition of PEPs does not include senior government officials • The requirement for life insurance covers beneficiaries but does not extend to beneficial owners.
13. Correspondent banking	LC	• The measures set out in R.13 apply to the correspondent banks in the EEA area only subject to their assessment as high risk, which is more restrictive than the FATF Standard.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
14. Money or value transfer services	C	The recommendation is fully met.
15. New technologies	C	The recommendation is fully met.
16. Wire transfers	PC	• The EU regulation in force does not yet cover beneficiary information and contains limited requirements for intermediate financial institutions, which affects almost all the criteria in this Recommendation.
17. Reliance on third parties	PC	• There is no requirement for FIs to satisfy themselves that the 3rd party is regulated, supervised and monitored for AML/CFT compliance. • Reliance on members of the EU is not based on the level of country ML/TF risks but rather the presumption that all EEA Members states implement harmonized AML/CFT provisions
18. Internal controls and foreign branches and subsidiaries	PC	• There is no requirement to ensure high standards when hiring employees. • Some of the requirements for group-wide AML/CFT programmes are missing.
19. Higher-risk countries	LC	• There are limited means to apply countermeasures.
20. Reporting of suspicious transaction	C	The recommendation is fully met.
21. Tipping-off and confidentiality	C	The recommendation is fully met.
22. DNFBPs: Customer due diligence	LC	• Similar deficiencies as identified in R.10, R.12 and R.17 are applicable for DNFBPs.
23. DNFBPs: Other measures	LC	• Similar deficiencies as identified in R.18 and R.19 are applicable for DNFBPs.
24. Transparency and beneficial ownership of legal persons	PC	• There is no ML/TF risk assessment of all types of legal persons created in Sweden. • Not all foundations are required to register, while there is no requirement for NPAs to register. • There are gaps in ensuring that companies co-operate with competent authorities to the fullest extent possible in determining the beneficial owner
25. Transparency and beneficial ownership of legal arrangements	PC	• Requirements on TSPs to conduct CDD do not extend to trust-relevant parties that are neither the customer nor the customer's' beneficial owner.
26. Regulation and supervision of financial institutions	PC	• Fit and proper requirements do not apply to all senior management positions, nor to the beneficial owners in all situations. • There is no ability to force persons who are no longer suitable to divest ownership for some types of FIs. • The risk classification tool for the ML/TF risk of supervised entities was still being developed (at the time of the onsite).
27. Powers of supervisors	LC	• The ability to issue fines is limited to some types of FIs, as some only allow conditional fines.
28. Regulation and supervision of DNFBPs	LC	• Some categories of DNFBPs may be given fines, but others do not have such an option. • Some DNFBP are not supervised on a risk-sensitive basis in the manner required by this Recommendation.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
29. Financial intelligence units	LC	• The efforts made by Fipo in conducting strategic analysis are not sufficient.
30. Responsibilities of law enforcement and investigative authorities	C	The recommendation is fully met.
31. Powers of law enforcement and investigative authorities	LC	• Some investigative techniques cannot be used in the investigation of ML, unless the ML offence is presumed to be gross. • There is no mechanism to identify in a timely manner whether natural and legal persons hold or control bank accounts.
32. Cash couriers	PC	• Sweden has not implemented a system to require declaration or disclosure for physical transportation of cash and BNI through mail and cargo. • Sweden has no mechanism to declare or disclose incoming and outgoing cross-border transportation of cash and BNI within the EU. • There is a formal mechanism to exchange information on issues related R.32 only between Customs and Fipo.
33. Statistics	LC	• The statistics related to seizures and confiscations are very limited in terms of breakdown of values, and in the period covered.
34. Guidance and feedback	LC	• Not all supervisors provide outreach and guidance about the application of AML/CFT measures to entities that they supervise.
35. Sanctions	LC	• The powers to apply sanctions with regard to the requirements under R.8 are limited. • For preventive measures, the ability to issue fines is limited to some FIs and DNFBPs, and within that subset, some only allow conditional fines.
36. International instruments	C	The recommendation is fully met.
37. Mutual legal assistance	LC	• There are some limitations to the use of investigative techniques in some cases where the money laundering offence would not be considered gross
38. Mutual legal assistance: freezing and confiscation	LC	• A foreign non-conviction based confiscation order made within the context of a civil or an administrative procedure cannot be enforced in Sweden. • There is no systemic way to manage all confiscated property.
39. Extradition	C	The recommendation is fully met.
40. Other forms of international cooperation	C	The recommendation is fully met.

GLOSSARY OF ACRONYMS

Abbreviation	Full name in Swedish	Full name in English
Brå	Brottsförebyggande rådet	Swedish National Council for Crime Prevention
CAB	Länsstyrelse	County Administrative Board
CATS	Centrum för asymmetriska hot- och terrorismstudier (Försvarshögskolan)	Centre for Asymmetric Threat Studies (at the Swedish Defence University)
EBM	Ekobrottsmyndigheten	Swedish Economic Crime Authority
FAR	Branschorganisationen för redovisningskonsulter, revisorer och rådgivare	Professional Institute for Authorised Public Accountants, Approved Public Accountants and Other Highly Qualified Accountancy Professionals
Fipo	Finanspolisen	Finance Police (FIU)
FMI	Fastighetsmäklarinspektionen	Swedish Estate Agents Inspectorate
FOI	Totalförsvarets forskningsinstitut	Swedish Defence Research Agency
FRA	Försvarets radioanstalt	National Defence Radio Establishment
FRII	Frivilligorganisationernas insamlingsråd	Fundraising Council for Volunteering Organisations
FSA	Finansinspektionen	Swedish Financial Supervisory Authority
GOB	Grov organiserad brottslighet	Aggravated organised crime
IPO	Enheten för internationellt polissamarbete	Unit for International Police Cooperation
ISP	Inspektionen för strategiska produkter	Inspectorate of Strategic Products
KFM	Kronofogdemyndigheten	Swedish Enforcement Agency
LI	Lotteriinspektionen	Swedish Gambling Authority
MUCF	Myndigheten för ungdoms- och civilsamhällesfrågor	Swedish Agency for Youth and Civil Society
Must	Militära underrättelse- och säkerhetstjänsten	Swedish Military Intelligence and Security Service
NÅA	Nationella åklagaravdelningen	National Public Prosecution Department
NOA	Nationella operativa avdelningen	National Operations Department (of the Swedish Police Authority)
NSU	Riksenheten för säkerhetsmål	National Security Unit (at NÅA)
RN	Revisorsnämnden	Swedish Supervisory Board of Public Accountants
RUC	Regionalt underrättelsecentrum	Regional Intelligence Centre
Säpo	Säkerhetspolisen	Swedish Security Service
SBA	Sveriges advokatsamfund	Swedish Bar Association
SCB	Statistiska centralbyrån	Statistics Sweden
SCRO	Bolagsverket	Swedish Companies Registration Office
Sida	Styrelsen för internationellt utvecklingssamarbete	Swedish International Development Cooperation Agency
SIK	Svensk insamlingskontroll	Swedish Fundraising Control
STA	Skatteverket	Swedish Tax Agency
SPA	Åklagarmyndigheten	Swedish Prosecution Authority
TV	Tullverket	Swedish Customs

www.fatf-gafi.org

April 2017

Anti-money laundering and counter-terrorist financing measures - Sweden

Fourth Round Mutual Evaluation Report

In this report: a summary of the anti-money laundering (AML) / counter-terrorist financing (CTF) measures in place in Sweden as at the time of the on-site visit on 26 May - 10 June 2016.

The report analyses the level of effectiveness of Sweden's AML/CTF system, the level of compliance with the FATF 40 Recommendations and provides recommendations on how their AML/CFT system could be strengthened.