

National Risk Assessment of Money Laundering and Terrorist Financing in Sweden 2019

A REPORT BY:

The Swedish Companies Registration Office, the Swedish National Council for Crime Prevention, the Swedish Economic Crime Authority, the Swedish Estate Agents Inspectorate, Swedish Financial Supervisory Authority, the Swedish Enforcement Authority, the County Administrative Board of Skåne, the County Administrative Board of Stockholm, the County Administrative Board of Västra Götaland, the Swedish Police Authority, the Swedish Inspectorate of Auditors, the Swedish Tax Agency, the Swedish Gambling Authority, the Swedish Bar Association, the Swedish Security Service, Swedish Customs, and the Swedish Prosecution Authority

Abstract

In this report, the coordination function presents its first common risk assessment of money laundering and the financing of terrorism in Sweden. The risk assessment is the work of sixteen authorities as well as the Swedish Bar Association. The overall assessment is based on a survey of threats, vulnerabilities and risks that the participants in the coordinating function are facing in their work to counter money laundering and the financing of terrorism. The report highlights risks in several areas, including: money mules and misused identities; challenges regarding disseminating, accessing and obtaining information and knowledge within the Swedish system; lack of resources, tools, or adequate legal basis; and large scale money laundering schemes. The forthcoming risk assessment for 2019 focuses on identifying the challenges that the participants in the coordinating function are facing in their work to prevent, detect and prosecute money laundering and the financing of terrorism; and also on highlighting the effect of these challenges on the efficiency of Swedish procedures. In the next risk assessment, various industries and sectors will be examined.

Summary

Introduction

An effective Swedish regime, i.e. Sweden's overall capacity to combat money laundering and terrorist financing, is essential for preventing Sweden from becoming an attractive country for criminals involved in these crimes. According to the evaluation of Sweden made by the FATF (Financial Action Task Force) in 2017, with a follow-up made in 2018, the Swedish regime generally performs well. However, there are risks and vulnerabilities that affect Sweden's ability to prevent and combat money laundering and terrorist financing. An effective regime requires a clear strategy and close cooperation between different stakeholders. It also requires an understanding of the risks and challenges facing the Swedish system.

Purpose and target audience

One of the responsibilities of the coordination function against money laundering and terrorist financing is to make an annual national risk assessment. The objective of the risk assessment for 2019 is to identify the challenges that the members of the coordination function face in their efforts to prevent and tackle money laundering and terrorist financing, and on highlighting how these challenges impact the effectiveness of the Swedish regime. This will also inform the next risk assessment, which will include an analysis of various sectors and industries.

The purpose of the report is to identify the risks of money laundering and terrorist financing in Sweden, and thus help strengthen the Swedish regime against these crimes. The aim is to enable the strategic use of the insights and analyses of the risk assessment in order to help the members of the coordination function take appropriate risk-reducing measures.

The assessment made in this report is based on the knowledge and information available to the coordination function about threat actors, crime schemes and vulnerabilities to money laundering and terrorist financing in Sweden. In order to better depict the current situation, the report is chiefly based on data from 2017–2018. The main target audience is the Government Offices of Sweden and the members of the coordination function.

Overall risk assessment

The report describes, from an official point of view, a number of approaches and developments within money laundering and terrorist financing that negatively impact the Swedish regime (the threats). It also describes the factors negatively impacting the capacity of the Swedish regime to prevent and tackle money laundering and terrorist financing (the vulnerabilities), and the overall assessment of the threats and vulnerabilities affecting the Swedish regime (the risks). This information underpins a number of proposals for strategic measures. The report highlights several areas impacting the Swedish regime against money laundering and terrorist financing. Some of the key themes of the report are discussed below.

One theme is the access to and use of **front men and misused identities** to conceal the origins of proceeds of crime and the identity of the perpetrators. The misuse of identities is problematic for several reasons. It reduces traceability between the proceeds of crime and the criminal operators behind the crimes, thus increasing the complexity of investigations aiming to determine the origin of funds. It also places higher demands on identity checks carried out by public authorities and other actors. The Swedish system currently depends on a high level of trust in basic identification; public authorities and other actors have to rely on the checks carried out by those who issue an identity card or register a company, for example.

Another theme is the need for **increased access to information and knowledge, and a good flow of information**. An efficient flow of information between and within the members of the coordination function is essential when it comes to reaching full potential in combating money laundering and terrorist financing. At present, the Financial Intelligence Section of the Swedish Police Authority is the only entity with the explicit mission of making strategic analyses and providing information and feedback to operators and supervisory authorities.

The members of the coordination function need to be more involved in drafting and have better access to strategic assessments and analyses of the situation. There is also a need to make greater use of statistics so as to better inform the internal risk assessments and priorities of the public authorities. Compiling knowledge will give the members of the coordination function, both individually and collectively, a better overview of the trends, challenges and needs within the Swedish regime. There is also a need for increased dissemination of information to the operators in order to increase their understanding of and ability to counter the risks of money laundering and terrorist financing. A better understanding of these issues among the operators would also help increase the number and quality of reports to the Financial Intelligence Section of the Swedish Police Authority.

A third point made by the risk assessment is that in certain cases there are **not enough resources, tools and legislation** for the coordination function to take proper action against money laundering and terrorist financing. Some supervisory authorities need more resources to increase their capacity to supervise a large number of operators. Several supervisory bodies also need to update their tools for risk classification. In addition, some of the public authorities in the coordination function currently lack the regulations necessary for effectively combating money laundering and terrorist financing.

Finally, a fourth theme highlighted in the report is the difficulties in detecting and preventing **complex money laundering schemes**. In these schemes, the true identity of the perpetrators and the origin of the funds are concealed through complicated, cross-border structures where money is transferred between different countries and legal persons. Criminal operators also hire enablers who in various ways, because of their skills or their function, plan and execute the schemes. Even if they do not necessarily involve large sums of money, transactions are usually made

through several intermediaries or through the settlement of loans and debts, making it harder to trace the route of the funds. Operators tend not to have the overview required to identify and report cases of this level of complexity. The report indicates that the Swedish regime needs to increase its capability to detect and tackle complex, large-scale money laundering schemes.

- **Front men and misused identities** are used in money laundering schemes. Two risk factors within the Swedish system are trust in basic identification and insufficient opportunities for certain authorities to protect themselves from being used for illicit purposes.
- **Increased access to and dissemination of information and knowledge** is a key condition for an effective Swedish regime against money laundering and terrorist financing. Information must be shared both between authorities and between authorities and operators.
- In certain areas, there are **not enough resources, tools and legislation** for the coordination function to take proper action against money laundering and terrorist financing.
- The Swedish regime needs to increase its capability to detect and tackle **complex, large-scale money laundering schemes**.

1 Introduction

There are no certain estimates regarding money laundering in Sweden, but it is likely that the amount being laundered each year stretches into the billions. The opportunity to make money is the prime motivator behind organised crime. Money laundering enables criminal actors to operate in society behind legitimate facades. This money laundering also contributes to hampering economic growth in Sweden, while at the same time undermining confidence in the financial system. Terrorist financing in turn represents a serious security threat. At present, the threat of terrorism against Sweden is assessed as elevated, which corresponds to a three on a five-point scale. The financing of terrorist organisations, networks and groups, as well as individuals, poses a threat to democracy and undermines security, both within and outside Sweden's borders.

Money laundering and terrorist financing therefore pose difficult challenges for a democratic and law-based society. These criminal activities also constitutes serious challenges to both the Swedish and global economy. An effective Swedish regime, as in the overall ability in Sweden to combat money laundering and terrorist financing, is crucial for preventing Sweden from becoming a country where criminals choose to launder money and finance terrorism. Achieving an effective regime requires a clear strategy and good cooperation between different parts of society. An understanding of the risks and challenges facing the Swedish system is also required. Based on FATF's evaluation of Sweden, it can be concluded that Sweden's system for combatting money laundering and terrorist financing is generally at a good level.

This report constitutes an initial risk assessment from the coordination function against money laundering and terrorist financing. The goal of the report is to create an understanding of the risks involved in the Swedish regime and the ways in which these challenges can be addressed.

1.1 Activities and responsibilities of the coordination function

As of the beginning of 2018, the Swedish Police Authority has the overall responsibility for a coordination function for measures against money laundering and terrorist financing. One of the tasks of the coordination function is to make annual national risk assessments of this issue. The coordination function is made up of the Swedish Bar Association and the following sixteen public authorities:

Swedish Companies Registration Office
Swedish National Council for Crime Prevention
Swedish Economic Crime Authority
Swedish Estate Agents Inspectorate
Swedish Financial Supervisory Authority
Swedish Enforcement Authority
County Administrative Board of Skåne
County Administrative Board of Stockholm

County Administrative Board of Västra Götaland
Swedish Police Authority
Swedish Inspectorate of Auditors
Swedish Tax Agency
Swedish Gambling Authority
Swedish Security Service
Swedish Customs
Swedish Prosecution Authority

1.2 Regulatory frameworks and the Swedish regime

In Sweden, measures to counter and combat money laundering and terrorist financing rely on an administrative law framework and a criminal law framework.

The administrative law framework, of which the Swedish Money Laundering Act is a central part, aims to prevent and detect cases of financial activities and other business activities being used for money laundering and terrorist financing. A number of operators, including lawyers, banks, real estate agents and accountants, are covered by the Swedish Money Laundering Act. They are required to take measures to prevent their activities from being used for money laundering and terrorist financing. The operators are under the supervision of the Swedish Financial Supervisory Authority, the Swedish Estate Agents Inspectorate, the Swedish Inspectorate of Auditors, the Swedish Gambling Authority, the Country Administrative Boards of Skåne, Stockholm and Västra Götaland, and the Swedish Bar Association. Both the operators and the supervisory authorities (not including the Swedish Bar Association) are required under the Swedish Money Laundering Act to report any suspicion of money laundering or terrorist financing to the Swedish Police Authority.

The criminal law framework aims to prosecute individuals guilty of money laundering and terrorist financing and to forfeit proceeds of crime. This framework mainly consists of the Swedish Act on Penalties for Money Laundering (2014:307) and the Swedish Act on Criminal Responsibility for the Financing of Particularly Serious Crime in Some Cases (2002:444). The public authorities within the coordination function that are responsible for tasks related to the criminal law framework are the Swedish Police Authority, the Swedish Economic Crime Authority, the Swedish Security Service, the Swedish Prosecution Authority, the Swedish Tax Agency and Swedish Customs.

Together, the Swedish Money Laundering Act, the Swedish Act on Penalties for Money Laundering and the Swedish Act on Criminal Responsibility for the Financing of Particularly Serious Crime in Some Cases form the legal basis for Sweden's capacity to combat money laundering and terrorist financing. The Swedish regime against money laundering and terrorist financing includes all stakeholders concerned by this legislation. These stakeholders include supervisory authorities, law enforcement authorities and operators. The Swedish regime must also have a good understanding of money laundering and terrorist financing and raise awareness of these issues within the regime in an effective and efficient way.

1.3 Risk assessment for 2019 – a special focus on the members of the coordination function

Under the fourth Anti-Money Laundering Directive, all EU member states must make national risk assessments. States can draw up their own national risk assessment as they see fit, as long as they adopt a risk-based approach.

The risk assessment for 2019 focuses on identifying the challenges that the members of the coordination function face in their work to prevent, detect and prosecute money laundering and terrorist financing, and on highlighting how these challenges impact the effectiveness of the Swedish regime. Consequently, this report does not contain any risk assessment for different industries and sectors. This is partly due to the need to highlight the current systemic risks before analysing various industries and sectors in more detail.

The risk assessment is thus an overview and should be viewed as input for future national risk assessments in which risks within different industries and sectors will be identified. The process of carrying out an analysis by sector will be initiated in 2019.

1.4 Purpose and recipients

The purpose of this national risk assessment is to identify the risks of money laundering and terrorist financing in Sweden so as to contribute to the strengthening of the Swedish regime in this area. The knowledge yielded by the risk assessment can be used strategically in assisting the members of the coordination function to take appropriate risk reduction measures.

The primary recipients of the risk assessment are the Government Offices of Sweden and the actors that comprise the coordination function. The risk assessment is also relevant for other authorities and operators concerned with money laundering and terrorist financing.

1.5 Methodology for threat, vulnerability and risk assessment

This is the first time that a risk assessment is being performed by the new coordination function, and the methodology has been developed and adapted to Swedish conditions during the course of the work.

In implementing the national risk assessment presented in this report, the coordination function has chosen to design a work process to assess threats, vulnerabilities and risks. The section on threats describes a number of approaches and phenomena relating to money laundering and terrorist financing that negatively impact the Swedish regime based on a government authority perspective. The section on vulnerabilities then describes the factors that have a negative impact on the Swedish regime's ability to prevent, obstruct and manage money laundering and terrorist financing.

The section on risks then addresses the overall assessment of the threats and vulnerabilities that have implications for the Swedish regime. The risks section forms the basis for the strategic action proposals presented in section 8.

In order to centre on current phenomena, the data for the analysis has primarily been limited to the period 2017 and 2018. The focus has been on establishing an inventory of knowledge and information available within the coordination function. The strategic measures in section 8 can be considered to be a basis for decisions and highlight areas in need of continued attention in the work to combat money laundering and terrorist financing. The threats, vulnerabilities and risk ultimately presented in this risk assessment are the result of the overall risk assessment of the coordination function.

2 Threats – money laundering

This section presents an overall assessment of the threats affecting the Swedish anti-money laundering regime from a government authority perspective. The following points are considered to be the main system threats in Sweden:

- The use of frontmen and stolen identities
- Criminal operators exploiting new financial payment solutions
- Complex money laundering schemes that cut through multiple sectors and jurisdictions
- Operators doing business without a licence or registration

2.1 The use of frontmen and stolen identities

In recent years there has been an increase in criminal environments regarding the use of other people's identities in criminal enterprise. Examples of this include borrowed, stolen or false identities. A prerequisite in a criminal enterprise is to be able to move money between different accounts without this activity being traced back to the original offence or the criminal operator or operators behind it.

In order to control the accounts used for the purpose of moving money, a network of multiple individuals or identities is needed. Criminal operators therefore exploit others by "borrowing" or stealing a real identity belonging to another individual. This is done either against their will, without their knowledge, or in exchange for compensation. The identity can, for example, be commandeered by accessing the e-identification linked to the account. It is common for the principal to control a large number of digital identities as it is possible to have multiple individuals' e-identifications linked to the same device. Aside from bank accounts, e-identification also gives access to, for example, the login function for government agency services.

False identities are also used for money laundering schemes. In these cases, a criminal operator uses a false or manipulated identity documents in order to make the primary identification more difficult.

2.2 Criminal operators exploiting new financial payment solutions

As new payment methods have emerged for legal purposes, the criminal world has been quick to adapt to developments. In recent years, new companies have been formed that offer financial payment solutions, so-called fintech companies. This is a sector under heavy development in Sweden. The emergence brings with it several challenges. In particular, the Swedish system is assessed as being exposed to threats based on the fact that these new financial payment solutions increase the possibilities for anonymisation and layering. Furthermore, there are several services for transferring money in real time between private individuals, companies and

associations with the need to provide a bank account or credit card number to the counterparty. Law enforcement authorities have shown how, for example, mobile payment services are used in criminal activities. Mobile payment services have characteristics that are deemed to constitute a high risk of money laundering, for example, through the possibility of conducting real-time transactions of relatively high amounts.

All in all, these capabilities are sought after in criminal activity. Cryptocurrency trading can also be conducted today in a fairly uncomplicated manner by individuals with relatively low technical knowledge. A well-known cryptocurrency is bitcoin, which can be stored in virtual wallets or “hardware wallets” provided by companies. As large sums can be handled anonymously, operators can store and transfer criminal proceeds with a low risk of detection.

2.3 Complex money laundering schemes that cut through multiple sectors and jurisdictions

The distinguishing element of international and more advanced money laundering schemes is that they cut through multiple sectors, multiple supervisory areas, and multiple jurisdictions. International criminal groupings are often specialists in identifying and exploiting weaknesses in national regulations. A characteristic trait of this type of criminality is that there may be an ability to exploit weaknesses in the Swedish welfare system through advanced criminal schemes that involve the use of companies and stolen identities.

There are some indications that cross-border money laundering schemes in many cases involve companies engaged in imports and exports. Money can be laundered through stating incorrect information on the price, quantity or quality of imported or exported goods. The scheme is facilitated by the complexity associated with foreign exchange transactions and various trade-financed arrangements, which enables a mixing of legitimate and illicit funds. In addition, large volumes of trade flows hamper the detection of individual suspicious transactions. The use of so-called facilitators is a recurring feature in more advanced money laundering schemes.

Facilitators refers to those actors who, by virtue of their competence or function, enable criminal operators to commit crime. For example, the interagency status report on organised crime 2018–2019 states that it has become easier for criminal operators to acquire broader capabilities through experts and facilitators. One explanation for this is that the market for criminal services, referred to “crime as a service”, has increased in recent years. This means that criminals buy or rent services required for a particular criminal scheme. This also includes money laundering.

The key competencies and positions of the facilitators can be used in several ways, including for advice on the formal requirements imposed on registering and running companies, on purchases and sales, on financial transactions, and on how criminal proceeds can be inserted into the legal economy either in Sweden or abroad. Facilitators can also provide criminal operators with Swedish or foreign

companies, frontmen or identities. The facilitator may also personally hold a key position and make decisions or approve a transaction as part of a money laundering scheme. Facilitators are found within all types of crime and are not unique to money laundering. The most qualified players are characterised by them often acting with the support of some form of business. The service or competence provided by facilitators is either done deliberately as part of a criminal scheme or through a company being infiltrated by individuals linked to criminal operators. It can happen that facilitators are forced to assist as a result of threats or pressure from the criminals.

2.4 Operators doing business without a licence or registration

As banks have reduced their cash handling in Sweden, criminal operators have moved the handling of cash to other services such as currency exchangers and money transferors to withdraw, deposit or exchange cash. In this sector, there are also several operators conducting business without a licence or registration, or acting outside the boundaries of their licence.

3 Vulnerabilities – money laundering

This section presents an overall assessment of the vulnerabilities affecting the Swedish anti-money laundering regime from a government authority perspective. The Swedish anti-money laundering regime serves as a safeguard and reduces the opportunities for criminal operators to implement money laundering schemes without detection. FATF's latest assessment of Sweden showed that the Swedish system is working well on many levels. Nevertheless, a number of vulnerabilities have been identified in the work with this risk assessment. The primary vulnerabilities are found to fall within the following areas:

- Inadequate identity verification
- Uneven reporting to the Financial Intelligence Unit and too few actors with reporting obligations
- Government agency operations or practices are exploited by criminals
- The limited exchange of information at the strategic level
- Weak control signals to government agencies regarding anti-money laundering efforts
- Limited resources within the Financial Intelligence Unit
- Limitations of supervisory bodies

3.1 Inadequate identity verification

Government agencies and other actors usually rely on the checks carried out by the actor issuing, for example, an identity card, coordination number or e-identification, and thereby assume that they are correct. This assumption applies to both physical and digital IDs. In its own inquiry from 2017, the Swedish Tax Agency states regarding coordination numbers that: “companies and individuals, but also government agencies, have the wrong picture that the Tax Agency through assigning a coordination number has at the same time ensured that all information linked to the person is correct and that no further checks are needed from their side”.

Supervisory authorities and law enforcement agencies retrieve information from sources such as the registers of the Swedish Companies Registration Office to use it as a basis when supervising and combatting crime. However, the Swedish Companies Registration Office does not have the possibility of assuring the quality of the information in its registers, nor is it able to tip off other agencies to suspicious persons. The sole task of the Office is to register submitted material. This trust in the primary identification represents a vulnerability as documents issued or used on false premises can be utilised in contact with government agencies and companies and thereby facilitate money laundering and other criminal schemes.

3.2 Uneven reporting to the Financial Intelligence Unit and too few actors with reporting obligations

3.2.1 Uneven reporting to the Financial Intelligence Unit by business operators

The anti-money laundering regulations are based on the premise that business operators report suspected money laundering and terrorist financing to the Financial Intelligence Unit at the Swedish Police Authority's Department of National Operations. The task of the FIU is then to process the information and then forward this to other sections within the judiciary. The FIU is also tasked with communicating trends to business operators, supervisory authorities and the Swedish Bar Association, information which can then form the basis of their risk analysis.

In 2017, a total of 16,551 reports were submitted to the Financial Intelligence Unit by 228 business operators, of which 96 were banks. The number of reports concerning suspected money laundering and terrorist financing increased to just over 19,300 in 2018, and overall the number of unique contributors increased to 356. This represents just a small proportion of all actors in Sweden with an obligation to report to the Financial Intelligence Unit. There are very few business operators in the non-financial sector that report suspicions of money laundering or terrorist financing. The degree of reporting is low, for example, among real estate agents, and business operators that provide tax advice, company formation, and accounting and auditing services, as well as businesses engaged in commercial trade for cash payment.

In parallel with the relatively low level of reporting, there is a need to improve the quality of the reports. Insufficient reporting means that money laundering may be under way which is not brought to the attention of the law enforcement authorities. The consequences will also be that it will be difficult to get a picture of how money laundering looks in different industries, which impairs the feedback to business operators and supervisory authorities.

3.2.2 More operators need to be obligated to report

According to the Anti-Money Laundering Act, all supervisory authorities (but not the Swedish Bar Association) and government agencies handling cash must report suspected money laundering to the Financial Intelligence Unit. An agency that is neither a supervisory authority nor dealing with cash is however instructed to provide information to the police in the form of tips or a report of criminal activity. Businesses not covered by the anti-money laundering legislation are not obligated to report suspected money laundering. There are such businesses that have access to information which allows them to identify an overarching pattern at the product level and therefore should be able to detect suspicious transactions. The fact that these operators are not obligated to report in this respect can be viewed as a vulnerability in the Swedish system. This concerns, among other things, issuers of e-identification, credit bureaus and third party providers that enable payment intermediation or the transfer of funds.

3.3 Government agency operations or practices are exploited by criminals

Swedish government agencies can be exploited in money laundering schemes. This entails a vulnerability for the Swedish regime, especially if the agencies lack sufficient

opportunities to counteract this exploitation. One example of this is the Swedish Companies Registration Office's limited ability to prevent their registers from being used to register companies with frontmen on the board, register incorrect ultimate beneficial owners, or switch out an annual report.

The Swedish Tax Agency's services can also be used to create false identities or create a fictitious income. One particularly problematic area is the issuance of coordination numbers, which are assigned by the Tax Agency upon request from government agencies and educational institutions. Unlike the assignment of civic registration numbers, personal presence is not required. A coordination number can then be used in money laundering schemes to acquire bank accounts and bank security tokens (not bank-ID), to be a board member or beneficial owner on a company's board of directors, or to produce fake invoices, employment agreements, income statements or loan documents. Furthermore, the Swedish Enforcement Authority has limited opportunities to counteract money laundering. The Enforcement Authority can be exploited, for example, through the construction of a debt relationship or through cash deriving from crime being earmarked for seizure with the goal of being injected into the financial system.

3.4 The limited exchange of information at the strategic level

An effective flow of information between and within the members of the coordination function is a prerequisite for achieving full potential in combating money laundering. There is a need for members of the coordination function to review strategic assessments or situation reports concerning money laundering. This is to enable them to form the basis for the authorities' internal risk assessments and priorities. At present, the Financial Intelligence Unit is the sole actor with the explicit assignment to conduct strategic analyses and provide information and feedback to business operators and supervisory authorities.

An increased flow of compiled information at an aggregated level from several agencies within the coordination function would create better conditions for an efficient flow of information. Similarly, the law enforcement authorities would be more equipped to compile crime statistics that could serve as a basis for such a strategic analysis. If specific information, such as at the operational level, is to be shared between government agencies with the goal of crime prevention, there may be a need to establish confidentiality regulations to keep this information secret.

Some supervisory authorities, such as the county administrative boards, do not currently have a sufficient ability to classify information. Other agencies within the regime, such as the Swedish Companies Registration Office, are also in need of additional confidentiality regulations to be able to carry out effective work to combat money laundering. An increased amount of strategic assessments and compiled information at an aggregated level, as well as increased exchange of information, would contribute to the ability to prevent and combat money laundering. For example, it would provide better conditions for prioritisation and give supervisory authorities increased data to conduct risk-based oversight.

3.5 Weak control signals to government agencies regarding anti-money laundering efforts

At present, the coordination function's agencies are governed by the Ministry of Enterprise and Innovation, Ministry of Justice and Ministry of Finance. This places demands on coordination between both ministries and agencies. Conflicts in terms of objectives can sometimes arise when the need to counteract money laundering and terrorist financing is set against other priorities such as regulatory simplification, incentives to start companies and the demand for increased digitisation. There is a need for clearer joint control signals from the assigner indicating that the work with combatting money laundering and terrorist financing is to be prioritised.

In addition, the fact that not all agencies within the coordination function have a crime prevention brief can complicate the efforts. The Swedish Tax Agency, the Swedish Companies Registration Office, Swedish Customs and the Swedish Enforcement Authority currently have no remit in terms of working to prevent money laundering and terrorist financing. Money laundering and terrorist financing is not included in Swedish Customs' area of responsibility if it cannot be linked to customs offences. Swedish Customs can therefore not prioritise other suspected money laundering or work with detecting and reporting suspicions to another agency (if not reported to the Financial Intelligence Unit or addressed within the context of the targeted initiative against organised crime).

The Enforcement Authority and the Swedish Companies Registration Office do not have any specific obligations to report suspected money laundering aside from in the case of cash handling. The Swedish Companies Registration Office also has limited possibilities to analyse register content, incidents and connections to identify behaviour that may entail financial crime such as money laundering. With regard to the Tax Agency, the agency currently has access to a wealth of information about natural persons, companies, associations and foundations.

This gives the Agency a good opportunity to detect and report suspected money laundering. As the Agency has no legal obligation to report suspected money laundering, its ability to combat money laundering is not being used to its full extent. As it stands, the tax crime units have the possibility of investigating money laundering offences on behalf of prosecutors. As and from 1 July 2019 however, money laundering is included in the crime directory of the tax crime units.

3.6 Limited resources within the Financial Intelligence Unit

The Fourth Anti-Money Laundering Directive stipulates that Member States are to provide their Financial Intelligence Unit (FIU) with sufficient financial, technical and human resources to be able to fulfil their duties. The Financial Intelligence Unit at the Swedish Police Authority's Department of National Operations is Sweden's FIU and the actor within the Swedish regime that is responsible for receiving reports of

suspected money laundering and terrorist financing. At the same time, they must also be able to exercise their responsibility for police intelligence operations in the area. At present, the FIU's financial resources are limited and heavily strained by the subsequent difficulties in meeting the requirements imposed on the FIU.

3.7 Limitations of supervisory bodies

There is currently a major focus within the Swedish regime regarding how the law enforcement authorities are intervening against money laundering and terrorist financing. At the same time, it is clear from a vulnerability perspective that the supervisory bodies have limited resources to effectively implement their work to prevent money laundering and terrorist financing. It is often the case that the supervisory bodies must prioritise their duties. In many cases, this can lead to a deprioritising of supervisory measures in relation to other assignments and tasks within the organisation. There may therefore be a need for resource reinforcements.

Staff resources for carrying out supervision vary between the supervisory bodies. Swedish Financial Supervisory Authority and the county administrative boards have special administrators who conduct supervision in accordance with the Anti-Money Laundering Act, while the Swedish Estate Agents Inspectorate, the Swedish Inspectorate of Auditors and the Swedish Bar Association can work to detect money laundering and terrorist financing within the framework of their general oversight. Furthermore, several supervisory authorities have an extensive range of entities to supervise. The county administrative boards at present have 7.5 full-time equivalents responsible for the supervision of more than 11,500 registered entities. In 2018, the boards carried out 123 desk reviews and 7 site inspections. The Swedish Estate Agents Inspectorate has over 7,000 entities to supervise, with a total of 10 FTEs working with all forms of supervision. This creates clear vulnerabilities in the Swedish regime. In addition to this system vulnerability, there are also specific challenges facing the respective regulatory bodies. For example, Swedish Financial Supervisory Authority has oversight responsibilities throughout the financial sector with significant economic values and high volumes of financial transactions.

Furthermore, it is noted that, in addition to resource challenges, there are also other distinct vulnerabilities among the supervisory authorities. The Fourth Anti-Money Laundering Directive stipulates that EU Member States shall apply a risk-based supervisory approach based on the risks of money laundering and terrorist financing prevalent in their Member State. The development of risk-based supervisory methods is underway, but there are no finished tools for risk classification at some of the authorities. In order to be able to carry out effective supervision, it is important to have good knowledge of those areas of activity within which the entities operate. The entities under the supervision of the county administrative boards operate within different types of industries and sectors. This means that the supervisory measures must be adapted to the entity's specific area of activity, which is demanding in terms of time and knowledge. Given the diverse areas of activity of the entities being supervised, it is difficult to perform a risk assessment for these. The county administrative boards need to develop methods for risk-assessing the entities. A

partial explanation for the weaknesses in the supervisory authorities' risk assessment of business operators is, to some extent, an inadequate exchange of knowledge and experience between supervisory bodies and law enforcement authorities (also refer to section 2.4). Another vulnerability concerns the constraints on supervisory bodies' ability to impose sanctions. It is important that the supervisory authorities have a mandate to sanction on undesirable behaviour. There are examples indicating that the sanction possibilities may be far too limited.

Finally, a vulnerability has been identified regarding the notification requirement. The challenge is that business operators covered by the Anti-Money Laundering Act and the supervision of the county administrative boards must provide notification of the registration of their business to the Swedish Companies Registration Office's Beneficial Ownership Register, aimed at preventing money laundering. Notification to this register is, according to the Anti-Money Laundering Act, a requirement for conducting the business activity covered by this obligation.

One problem for the county administrative boards is that there are business operators conducting business activity subject to the notification requirement but which are not fulfilling this obligation. This may be due to the business operator not being aware of the requirement, or that despite this knowledge they still neglect to submit notification of their business for various reasons. The consequence of this is that there is probably a significant pool of business operator subject to the notification requirement that the county administrative boards are unaware of. The county administrative boards do not have the authority to impose penalties on operators that, despite the requirements of the Anti-money Laundering Act, do not register in the Beneficial Ownership Register.

4 Risks – money laundering

This section presents an overall assessment of the risks affecting the Swedish anti-money laundering regime from a government authority perspective.

- Inadequate identity verification
- Efficiency of the administrative system
- Complex money laundering schemes – difficult to detect
- No coherent overview
- Inefficient supervision of currency exchangers and unregistered money transferors

4.1 Inadequate identity verification

The Swedish system relies on a high level of trust in primary identification. Primary identification is also a central requirement for preventing the use of false or stolen identities for the purpose of money laundering. As mentioned in the chapters on threats and vulnerabilities, borrowed, stolen and false identities have become increasingly important in money laundering schemes in Sweden. One risk is that government agencies and private operators trust in the verification having been done at some other point. This may include companies being registered by the Swedish Companies Registration Office based on incorrect basic information, or that a bank accepts an e-identification issued by another bank as adequate identification. As previously mentioned in the vulnerabilities chapter, the Swedish Companies Registration Office and the Swedish Tax Agency are particularly vulnerable, which exposes the system to a risk in this respect. There are probably also additional agencies whose operations can be exploited to create legitimacy on false grounds.

4.2 Efficiency of the administrative system

One objective of the administrative anti-money laundering regulations is for different sectors of society, both business operators and government agencies, to work to reduce the risks of money laundering and terrorist financing. In the threat and vulnerability analysis, various problems that may limit the efficiency of the administrative system have been identified.

4.2.1 Business operators

Relatively few business operators report to the Financial Intelligence Unit. The reporting rate from the non-financial operators is particularly low. This is probably largely due to ignorance regarding their obligations and what suspected money laundering comprises. The consequences of this can be that certain money laundering transactions are not detected, stopped or investigated of law enforcement authorities. As has emerged in the vulnerability chapter, there are now also business operators that could detect money laundering but which are currently not subject to the reporting obligation under the Anti-Money Laundering Act (e.g. issuers of e-

identification). An increased reporting obligation for these operators would likely increase the efficiency of the Swedish regime.

4.2.2 Oversight and supervisory bodies

The Fourth Anti-Money Laundering Directive stipulates that the Member States shall apply a risk-based supervisory approach based on the risks of money laundering and terrorist financing prevalent in their Member State. The development of risk-based supervisory methods is underway, but there are no finished tools for risk classification within several supervisory bodies. This poses a risk with the consequence that the supervision is not effective enough. The absence of a good system for risk-based selection can lead to the supervisory authorities not supervising those operators that run the greatest risk of being exploited for money laundering or terrorist financing. An effective supervisory operation also requires the authorities to have sufficient resources to carry out this oversight.

Furthermore, as indicated in section three, there are business operators that do not register their business. These fall outside of state supervision in practice. This poses a particular risk, in particular where there is reason to assume that the unregistered operators are also those that do not otherwise comply with the anti-money laundering regulations.

4.2.3 Feedback

In order to be able to apply a risk-based approach, both supervisory bodies and business operators are in need of information and feedback. The supervisory authorities require specific information on different possible money laundering schemes in order to strengthen the authorities' risk assessment of different operators. Operators also often require feedback on submitted reports as well as increased knowledge of warning signals. Only the Financial Intelligence Unit has an explicit mandate to produce strategic analyses and provide information and feedback to business operators and supervisory authorities. The feedback currently taking place does not cover the need for such as expressed by both supervisory authorities and business operators. The consequences of inadequate feedback are that the potential for effective oversight and reporting from operators becomes lower.

4.3 Complex money laundering schemes – difficult to detect

The section on threats identifies and describes how advanced money laundering schemes extend across Sweden's borders. The overall assessment is that advanced, large-scale money laundering schemes are at present relatively difficult to detect, prevent and investigate within the Swedish regime. The reasons for this are many:

The more complex international money laundering schemes are difficult to identify and are therefore not discovered by business operators. Instead, what is reported primarily consists of individual transactions. Another reason is that it is the nature of these cases to stretch across the areas of responsibility of several government agencies and across the borders of several nations. This requires well-resourced investigative capacity and the effective and smooth exchange of information between Swedish

authorities and the equivalent authorities in other countries. Finally, it can be noted that this sort of investigation is extensive and resource-intensive, which often works against the demand to solve multiple crimes. Altogether, these create a risk that criminal operators can exploit the Swedish system and that the complex schemes can be perpetuated.

4.4 No coherent overview

An effective flow of information between and within the members of the coordination function is a prerequisite for achieving full potential in combating money laundering. As indicated in the vulnerabilities chapter, there is in many cases no overall, and operationally well-founded, strategic assessments or situation reports. There is also an absence of compiled statistics in several areas, which reduces the possibilities of a coherent overview of the scope and form of money laundering in Sweden. There is a clear need for members of the coordination function to review strategic assessments or situation reports concerning money laundering to a greater extent. This would increase the chances of a risk-based approach within the regime and could serve as a basis for prioritising initiatives to combat money laundering. The opportunities to provide feedback to business operators would also be likely to increase. This also requires the coordination functions members to implement these assessments and situation reports in their operations.

4.5 Inefficient supervision of currency exchangers and unregistered money transferors

Currency exchangers and payment service companies are identified by the EU as an industry with a high risk of money laundering and terrorist financing. FATF also describes both traditional and alternative money transferors as key components in certain money laundering schemes. The same is indicated by the threat and vulnerability analyses. Currency exchange, money transfer and money remittance are assessed as constituting that part of the financial market where most operators run businesses without registration or the licences required, or which operate outside the boundaries of the licence. The ability to carry out effective supervision is thereby impaired.

5 Threats – terrorist financing

This section presents an overall assessment of the threats relating to terrorist financing that affect the Swedish regime from a government authority perspective.

- The threat from terrorists
- Fundraising activities with legitimate funds or with seemingly legitimate purposes
- Criminal proceeds to finance terrorism
- Low sums and non-complex financing schemes
- The hawala money transfer method
- Cross-border flows and flows within Sweden
- Self-financing

5.1 The threat from terrorists

At present, Islamic-motivated terrorism poses the most serious terrorist threat to Sweden. In Sweden, there are more violent Islamists than ever before, although the large increase in the number of people who sympathise with violent Islamism has probably dropped off in recent years. Furthermore, the white power environment and the autonomous environment also have the ability to commit violent crimes with ideological overtones, even if the terrorist threat from these actors is assessed as low. One trend which has become increasingly evident in Europe in recent years is the lone, self-radicalised actors who, without cooperation with other networks or terrorist organisations, plan and implement attacks on their own initiative. According to the National Centre for Terrorist Threat Assessment (NCT), in 2018 all Islamist-motivated terrorist attacks in the Western world with a fatal outcome were carried out by lone perpetrators. The means have been relatively simple, such as stabbing weapons, vehicles or firearms. Overall, the Swedish Security Service notes that at present, there are around 3,000 so-called threat actors in violent extremist environments in Sweden.

5.1.1 Swedish convictions – experiences

It is difficult to draw definitive conclusions about terrorist financing as knowledge is limited. Thus far in Sweden, few cases have led to prosecution and only five individuals have been convicted of terrorist financing. One challenge in the financial investigations into suspicions of terrorist financing is that it is often not possible to prove who has been the final recipient of the money. It is often about one person in a country where it is difficult to gain insight into the financial system and where it is difficult for Swedish authorities to obtain legal assistance. However, changes in legislation have created the conditions for an increased number of convictions.

In 2018 and 2019, two cases of terrorist financing have been in focus.

One man was sentenced in 2018 to six months in prison for having urged others to finance terrorist crime. On 27 November 2018, the Court of Appeal upheld the District Court's ruling. The man was convicted of posting two messages on an open Facebook account in which he urged others to donate money to terrorist organisations to buy

weapons. The ruling indicates that the act, even if it was in the early stage of a terrorist act, should nevertheless be regarded as criminal. The ruling has been appealed and the Supreme Court decided on 18 February 2019 that leave to appeal was required. In the beginning of March 2019, the District Court ruled in a case against six individuals suspected of crimes pursuant to the Act (2002:444) on Criminal Responsibility for the Financing of Particularly Serious Crime in Some Cases. While two people were freed, four of them were sentenced to between four and six months in prison for having financed the activities of the terrorist group IS. It involved, among other things, transfers of money to families who had lost a relative who had been an IS terrorist. The person sentenced to six months was the one who had transferred most money, SEK 18,000. The convictions have been appealed. These convictions point to both low complexity and small denominations, as well as the vital role that intelligence gathering plays in identifying threats at an early stage.

While the Swedish cases showed low complexity, there are cases from investigations within the EU that indicate the opposite. A major investigation in 2017 involved a Lebanese citizen who offered money laundering services to organised crime. Part of the profit from this enterprise was used to finance the military branch of Hezbollah. In another large-scale investigation in Europe, it was concluded that a number of foreign combatants in several conflict zones, such as Iraq, Syria and Libya, had received financing for their activities from family members in Europe via a network of facilitators and money transferors. In the case in question, there were close to 5,000 transfers from 2,000 senders to around 1,000 recipients. In the first case, we see an example of the close connection with the criminal environment, while in the second case we see how important facilitators can be in these contexts. These cases show that there are examples of both low-scale and higher complexity when it comes to the financing of terrorism from Europe.

5.2 Fundraising activities with legitimate funds or with seemingly legitimate purposes

It is common practice for terrorism to be financed both with legal funds and with criminal proceeds. Legal funds can be collected through traditional fundraising activities or, for example, crowdfunding via social media. This often concerns fundraising with a seemingly legitimate purpose and it is likely that not all individuals donating money know the real objective behind the fundraising. It is also common that profits from different types of commercial operations are channelled to finance terrorism. It has also happened that people have taken different types of loans to financially support terrorist-related activities. For example, the activity following the emergence of IS in Syria and Iraq whereby individuals in Sweden attempted to raise capital with the goal of financing their travel and subsistence on their journey to join the combatants in the conflict area. At the time, the Swedish Security Service identified several persons who applied for and were granted loans, including unsecured loans and SMS loans, student loans through CSN, commercial loans, car loans and car leasing. Several individuals have also financed their travel and stay using welfare allowances. People in the conflict area have also received financing from family and friends in Sweden.

5.3 Criminal proceeds to finance terrorism

Criminal proceeds used to finance terrorism derive from different types of crime, such as drug dealing, fraud aimed at both companies and private individuals, or benefit crime, for example, fraud involving assistance support. Many of the violent extremists in Sweden commit or can be suspected of committing crimes that are not considered to be ideologically motivated in order to raise money. These include, for example, unlawful appropriation, drug offences, financial crime and fraud. In recent years in Sweden, the police have seen an increasingly clear link between organised crime and crime with political or religious motives.

5.4 Low sums and non-complex financing schemes

The remittance of money for terrorism is carried out using simpler money laundering schemes, mostly cash handling and money transfer and often across national borders. In this case, it is not a question of primarily concealing the origin of the money but rather the goal of concealing the recipient (person or organisation) and country. The monetary transactions are often small-scale with low amounts and relatively basic setups. This is mainly done through payment service companies, other types of money remitters or with money couriers.

There are also examples of suspicious transactions in connection with the export and import of goods, where financial funds are conveyed out of the country in conjunction with this activity. However, it is very difficult to distinguish terrorist financing from other types of capital flows abroad. Discussions are under way regarding the extent to which terrorists use virtual currencies for transfers. There are regular calls on social media to donate to terrorist movements by way of virtual currencies. However, there are no indications that any major flows of virtual currencies are being directed to the financing of terrorism.

5.5 The hawala money transfer method

Hawala is considered to be a commonly used form of transferring money with the goal of financing terrorism. Hawala is used to transfer money between two parties without money being sent physically or electronically. Instead, a broker known as a hawaladar is used. This broker credits each party for the transfers and settles these periodically. Reports from financial operators, intelligence information and the international exchange of information suggest that this is a commonly used method. This method, which is referred to under other names, is used over large parts of the world and is often relatively unregulated. The majority of hawala transfers are made using legal money and without criminal intent. The method is used partly for traditional reasons and partly because transfers are often made to regions where the regulated banking sector is weak or non-existent. Business operations in Sweden are often conducted without having been registered correctly and without the due diligence and other documentation that financial actors should have. Certain operators have customers who exclusively transfer money from criminal activity.

Hawala entails that cash is quickly made available abroad and that international transfers are not traceable. The hawala system is used firstly in the case of traditional hawala, and secondly within new financial payment solutions based on hawala methods. In terrorist financing, it is a way of avoiding the monitoring of transferred funds and also allows for sanctions to be circumvented.

5.6 Cross-border flows and flows within Sweden

As an activity, terrorist financing knows no boundaries. Operators in Sweden can be assumed to both send and receive money through their support activities to terrorist organisations. Individuals who in one way or another finance terrorism often have social relationships with each other, and capital changes ownership through loans and debts, payment of goods and services, personal financial contributions and criminal activity. Several of the individuals in the violent Islamist environment in particular originate from other countries and send capital to their family and friends abroad. This means that the financing flows are likely to be both incoming and outgoing from Sweden. The assessment is that there are fewer incoming flows. In addition, it can also be very difficult to distinguish between financial transactions aimed at terrorist financing and transactions with another purpose.

The previous risk assessment on terrorist financing described a geographical distribution of threat activities and flows, i.e. how funds tend to be conveyed across the borders. The study outlined the following flows:

- Strictly domestic financing; all stages are conducted in Sweden.
- Domestic financing via other countries; the funds are generated and used in Sweden, with an intermediary abroad.
- Incoming financing; the funds are generated abroad and used in Sweden, with an intermediary within and outside Sweden.
- Strictly foreign financing; all stages are conducted outside Sweden.
- Foreign financing via abroad; the funds are generated and used abroad, with an intermediary in Sweden.
- Outgoing financing; the funds are generated in Sweden and used abroad, with an intermediary within and outside Sweden.

All forms of flows are likely to occur, including during the 2017–2018 assessment period. Primarily however, the flow has been from Europe to third countries, and it is rare that the flow has been in the opposite direction. At the same time it is, for example, not impossible for proceeds in conflict zones such as Iraq and Syria to be placed in Europe. These flows can constitute both money laundering and terrorist financing.

5.7 Self-financing

In recent years, several terrorist attacks in Europe have not required any external financing. Several of these attacks have, for example, been self-financed, not least when the attack has been carried out by lone individuals using basic methods. In

many cases, there has also been so-called microfinancing within groups, and often using private funds. It is therefore possible for one individual to finance an attack without fundraising or transferring money. A parallel can be drawn to the findings outlined in a Swedish Defence University report from 2017. The individuals who travelled from Scandinavia to join IS self-financed their trips “through the use and misuse of social welfare allowance and other state benefits, in combination with relatively low-profile crimes such as loan and credit card fraud, tax fraud, bankruptcy applications and false bookkeeping”.

Another study of 40 jihadist cells that have planned attacks in Europe showed that close to 90 per cent of them have been involved in income-generating activities. Half of the attacks were self-financed and several were financed through local and legal fundraising activities.

6 Vulnerabilities – terrorist financing

This section presents an overall assessment of the vulnerabilities relating to terrorist financing that affect the Swedish regime from a government authority perspective.

- Limited knowledge on terrorist financing
- Few intelligence reports and suspect reports are linked to terrorist financing
- Insufficient control over disbursements and allowances
- Limited ability to act against cross-border shipments of cash

6.1 Limited knowledge on terrorist financing

The nature of the terrorist financing that exists in Sweden today makes it generally difficult to detect for those business operators covered by the Anti-money Laundering Act. Many business operators also lack knowledge on terrorist financing. As a result, measures to counteract terrorist financing are not taken, or those that are taken risk being ineffective. This also means that the number of reports submitted to the Financial Intelligence Unit is relatively low. Even among the supervisory authorities, the awareness of terrorist threats and terrorist financing is limited. This results in there also being a lack of knowledge on the risk areas for terrorist financing that are found within the authorities' area of responsibility. The inadequate knowledge on this phenomenon impacts on the conditions required to conduct effective oversight.

6.2 Few intelligence reports and suspect reports are linked to terrorist financing

In 2018, around 200 intelligence reports from the Financial Intelligence Unit concerning suspected terrorist financing were brought to the attention of the Swedish Security Service. The fact that the number of these reports was so small may be due to several factors; firstly, financing activities can be unusual, secondly, there may be difficulties for business operators and the Financial Intelligence Unit to separate terrorist financing from money laundering, and thirdly, business operators may have difficulty recognising activities linked to terrorist financing. Finally, it may be the case that terrorist financing activities are being conducted without the involvement of businesses subject to the reporting obligation.

Furthermore, despite good cooperation between several government agencies to combat terrorist financing, such as between the Swedish Security Service, the Swedish Tax Agency, the Swedish Economic Crime Authority and the Swedish Police Authority, there is potential for increasing the flow of information between the agencies. The Swedish Economic Crime Authority and Tax Agency conduct intelligence work to combat financial crime but the agencies do not primarily look for activities linked to terrorist financing. This means that terrorist financing that involves financial crime schemes may not be recognised as part of terrorist financing,

and therefore risks not being brought to the attention of the Swedish Security Service. Similarly, combatting terrorist financing is not part of the remit of Swedish Customs, which can mean that this activity is not detected or dealt with effectively. In recent years, this vulnerability has been reduced through increased collaboration between the agencies concerned. Nevertheless, it is likely that financing schemes are not being mapped to the extent that may be possible, and it is probable that potential financing schemes are instead being investigated as other crimes.

6.3 Insufficient control over disbursements and allowances

Vulnerabilities related to terrorist financing can also be linked to a lack of control systems in society's benefits system. For example, individuals travelling to conflict areas have in some cases used benefits and allowances to finance the journey. In many cases, there is no opportunity for disbursing agencies to withhold payments to natural and legal persons upon suspicion of terrorist financing. Other types of subsidies, for example to organisations, can also be used for terrorist financing, and even in this case there may be no legal possibility of restricting payments.

6.4 Limited ability to act against cross-border shipments of cash

As pointed out in the threat analysis, cross-border shipments of cash are used in terrorist financing. At present, Swedish Customs has limited powers to act against such shipments coming in or out of the EU. Swedish Customs also has no scope to inspect and detain cash in the case of movement between Sweden and other EU Member States.

7 Risks – terrorist financing

This section presents an overall assessment of the risks relating to terrorist financing that affect the Swedish regime from a government authority perspective.

- Knowledge and reporting – suspected terrorist financing is not being detected
- Difficult to track and monitor transactions
- Public subsidies are being used for terrorist financing
- Financing of violent environments

7.1 Knowledge and reporting – suspected terrorist financing is not being detected

Terrorist financing facilitates and enables terrorist organisations and networks to grow in Sweden and abroad. The law enforcement authorities and the Swedish intelligence services play a vital role in obtaining information at an early stage in order to detect suspicious behaviour. The submission of reports to the Financial Intelligence Unit from all operators covered by the regulations is of central importance. It is often that reporting provides essential information to the law enforcement authorities.

Business operators play a crucial role in the work with detecting terrorist financing. There is much to suggest that terrorist financing is being conducted without it being reported to the Financial Intelligence Unit. This is likely due to knowledge regarding terrorist financing being relatively low among many of the business operators. It may also be due to the fact that terrorist financing often involves smaller amounts and legally earned or raised money, making it difficult to detect. The relatively low level of reporting implies a deficiency in the system's ability to provide early warnings of suspected terrorism.

7.2 Difficult to track and monitor transactions

The threats and vulnerabilities chapters describe how threat actors with the goals of terrorist financing can use transfers that are difficult to detect and investigate. Both new and traditional financial payment solutions are used for this purpose. The traditional hawala method is to be considered a risk as transfers are untraceable. Although most instances of transfers using hawala are probably legitimate, there have been several cases where hawala is a suspected instrument for terrorist financing. Another risk is that several of the hawaladars in Sweden are not registered for supervision. It is therefore important that the Swedish regime works to a greater extent with shutting down illegitimate operators in this form of activity. One trend in this context is that this traditional form of hawala transfers has also transitioned into modern technology, for example, via new payment platforms and mobile apps.

7.3 Public subsidies are being used for terrorist financing

The threat analysis indicates that terrorist financing can be done with both legally and illegally earned money. In Sweden, it has also been relatively common, for example, for individuals to travel to conflict areas and finance their journeys using different forms of public benefits or student loans from CSN. The small sums used in terrorist financing increase the possibilities of using benefits and loans that make detection more difficult. In many cases, there is also no opportunity to deny payment. In addition, there is a risk of public aid being paid to organisations that drive violent radicalisation forward.

7.4 Financing of violent environments

In recent years, a trend in the Western world, that lone individuals carry out attacks with low complexity and cost, could be interpreted to mean that terrorist financing is an increasingly minor problem in Europe as the perpetrators do not utilise any external financing in the execution of their attacks. However, individual attacks cannot in all cases be disassociated from the violent environments' overall costs for recruitment, logistics and propaganda, something which is a premise for the self-financed attack to be carried out at all.

When it comes to financial transactions to support recruitment, radicalisation and propaganda, there is reason to suspect that money flows go both to and from Sweden. Therefore, financial assets used to support recruitment and radicalisation in extremist environments, or used to bankroll the spread of propaganda on a global arena, create the very premise for the lone individual's intent to carry out an attack. There is thus a need to view terrorist financing in a significantly bigger context than simply as support for individual attack plans or established terrorist networks. Financial support for violent environments, within and outside Sweden, also needs to be counteracted in order to effectively prevent terrorism.

8 Strategic measures

A departure point for the work with a national risk assessment is that a country is to identify, analyse and understand its risks in relation to money laundering and terrorist financing. The following are the needs for targeted measures that have been identified on the basis of the threats, vulnerabilities and risks identified in this report. The strategic measures below have taken into account the Government's strategy regarding how an effective regime in this area could look. According to this document, an effective regime is based, among other things, on knowledge-promoting activities, cooperation, information management and effective regulation. The proposals for strategic measures are presented in no specific order.

8.1 Increased knowledge gathering and sharing between agencies

There is currently no comprehensive overview of money laundering in Sweden. There is a need to continuously build knowledge regarding the areas within which money laundering occurs, for example:

- the size of the sums that can be linked to different original offences
- the industries within which money laundering occurs
- the money laundering schemes that are used
- how the Swedish economy is affected by money laundering
- the size of the criminal proceeds being brought out of Sweden
- how criminal proceeds flow into Sweden and are integrated in the Swedish economy

In order to chart the progression of money laundering and terrorist financing over time, a clearer handle on statistics is needed. Clearer knowledge on when, where and how cases are handled would strengthen the Swedish regime and allow for improvement measures. By increasing the collection of statistical data on, for example, supervisory cases, seizures, repossessions, resource use, reports, court rulings and reports of suspicion, knowledge within the Swedish regime can be strengthened. Through such an analysis, it will also be easier to monitor developments in the area and clarify the need for resources and prioritisation.

Alongside the statistics, the work of the Swedish regime would probably be improved if the individual government agencies were instructed and given the resources to conduct a yearly situation analysis. For the supervisory authorities, there is a need for regular evaluation of the risk-based supervisory activities within that authority, i.e. how well the procedures and legislation are applied and identifying the main risk areas among the entities being supervised.

Furthermore, an internal vulnerability analysis would also be needed to examine how well the supervisory authority's work corresponds to the overall objective of an effective Swedish regime. For law enforcement authorities, there is a need for a comprehensive annual situation report regarding money laundering and terrorist financing, as well as an analysis of internal vulnerabilities pertaining to how effective

the agency is in combating money laundering and terrorist financing. There is a general need to increase and disseminate knowledge on the methods of operation for money laundering and terrorist financing. As threat actors constantly try out new methods and shift focus, it is essential that the system is vigilant and at the forefront to be able to stay on top of these. Knowledge in this regard lays the foundations for the agencies' risk management capacity and contributes to helping business operators and supervisory authorities to understand and counteract the risks of money laundering and terrorist financing in their various operations.

In order to increase the possibility of knowledge dissemination, there is a need to review the appropriateness of extending the number of government agencies to be covered by the Act (2016:774) on reporting requirements in cooperation against certain organised crime, LUS. There may also be a need to revise the confidentiality regulations with a focus on the ability of non-law enforcement agencies to protect classified information received by the agencies from the authorities investigating crime.

Several supervisory authorities have common challenges in their work, for example, in connection with the risk classification of entities being supervised, and the imposition of fines and sanctions. In order to increase the efficiency of the Swedish regime, there is a need for a continued exchange of knowledge between the supervisory authorities, including the Swedish Bar Association.

8.2 Information exchange and dissemination to business operators

The Financial Intelligence Unit is a key player in terms of receiving and processing knowledge on suspected cases of money laundering. On occasion, the FIU issues strategic reports. The analyses are important for business operators and law enforcement authorities, but also for the supervisory authorities. There is an interest in the analyses being performed more frequently, in them being disseminated more clearly, and in them being distributed to both government agencies and business operators given their strategic and cross-sectoral content. Certain categories of business operators are under-represented in the statistics on reports submitted to the FIU. Information campaigns are needed to persuade these operators to increase their reporting.

In parallel, the quality of the reports that come in also needs to increase. Quality-enhancing measures could include training courses or other activities aimed at increasing knowledge. At present, much of the exchange of information between government agencies and trade organisations takes place on an ad hoc basis. The agencies would benefit from establishing closer cooperation with the trade organisations in terms of knowledge on money laundering and terrorist financing. The Swedish Security Service needs to regularly inform agencies, business operators and trade representatives on terrorist financing with the aim of raising awareness and competence.

8.3 Agency governance

There is a general need for a clearer and more coherent focus on defining which priorities will govern and guide the Swedish government agencies' work to combat money laundering and terrorist financing. At present, the coordination function's members (aside from the Swedish Bar Association) serve under different ministries within the Government Offices of Sweden. The agencies are therefore governed based on different premises. This can sometimes lead to conflicts of objectives, for example, concerning work prioritisation and resource allocation in the efforts to combat money laundering and terrorist financing. In addition, there is a need to ensure that the members of the coordination function, in particular the Swedish Companies Registration Office, the Swedish Tax Agency, Swedish Customs and the Swedish Enforcement Authority, are given a clearer mandate and effective tools to combat money laundering and terrorist financing (see needs for each agency under section 8.5).

8.4 Specific focus areas

The coordination function's assessment is that the following areas contribute to money laundering and terror financing risks in Sweden, which is why measures may need to be taken within the following areas:

- Sweden is one of the world's most cash-less countries. At the same time, cash is used to a significant extent in several money laundering contexts. Further measures to limit the possibilities of large-scale cash handling would likely make it difficult for criminals to launder money.
- Stolen or false identities are in many cases a prerequisite for money laundering schemes. There is therefore a need to map the systematic use of stolen and false identities and develop concrete measures to prevent this.
- Technological development has resulted in a number of new financial payment solutions that, for example, increase the possibilities of anonymisation and quick transactions. This is a sector under heavy development. The law enforcement authorities therefore need to ensure the ability to handle these technical challenges.
- Technological developments have also meant that there are business operators that would be able to detect money laundering but which are currently not subject to the reporting obligation under the Anti-Money Laundering Act. An increased reporting obligation would likely increase the efficiency of the Swedish regime. For example, there may be a need for issuers of e-identification, credit bureaus and third party providers that enable payment intermediation or the transfer of funds to report suspicious transactions to the FIU.
- Under current regulation, all supervisory authorities and government agencies handling cash have a reporting obligation pursuant to the Anti-Money Laundering Act. As money laundering and terrorist financing can occur in several other situations, there is a need to ensure that other agencies are also subject to the reporting obligation.

- There is a risk that subsidies, benefits or other disbursements from the public sector are being used for terrorist financing. There may therefore be a need to investigate erroneous payments and look into how better control functions can be created to reduce these.
- There is also a risk of funds for terrorist financing being collected through traditional fundraising activities or crowdfunding online. There may therefore also exist a need to review whether fundraising activities need to be subject to further control so as to reduce the risk of being exploited for terrorist financing.

8.5 Specific needs and measures in relation to individual government agencies

There are a number of needs that concern individual agencies, but which would as a whole strengthen the Swedish regime and yield risk-reducing effects:

The Swedish Companies Registration Office

The Swedish Companies Registration Office needs to have an expanded regulatory framework with a clearer law enforcement focus in order to:

- Identify and verify that company representatives really exist and that these are not well-known within organised crime.
- Identify and verify that the specified addresses and other supporting information are correct, and check (as well as prevent or deny) that specified company representatives and accountants are legitimate and are not linked to organised crime.
- Adjust the confidentiality legislation to increase the ability of the Swedish Companies Registration Office to receive classified information from other agencies.
- Establish clearer directives and resources to increase the national capacity to combat money laundering.
- Be able to work more proactively and prevent companies being used as tools for criminal activity.

Therefore, the Swedish Companies Registration Office would need an expanded crime prevention role in its assignment description.

The Swedish National Council for Crime Prevention

The Swedish National Council for Crime Prevention, Brå, has in recent years developed in-depth analyses linked to money laundering. Brå's collective knowledge could to a greater degree be used operationally, for example, to develop methodological manuals, courses, conferences and as a basis for training. Brå is currently working, in collaboration with the coordination function, on a research project concerning money laundering offences.

In order to further deepen the knowledge on money laundering, the possibilities of additional research projects in the future should be considered.

The Swedish Economic Crime Authority

The Swedish Economic Crime Authority needs to increase its ability to gather knowledge and experience from its work with cases concerning money laundering and also increase its capacity to effectively disseminate knowledge internally, but also to convey this to business operators and supervisory authorities. The Swedish

Economic Crime Authority should also promote and contribute to the development of money laundering statistics.

The Swedish Estate Agents Inspectorate

Today, only individual physical estate agents are subject to supervision. In order for the Swedish Estate Agents Inspectorate to be able to carry out effective supervision, the real estate agencies, in which individual real estate agents conduct their activities, should also be subject to oversight. Another important aspect of this is the possibility for the supervisory authority to carry out site inspections at a real estate agency. This would give the Inspectorate access to the company premises and the right to access and review material on site. The Inspectorate is also in need of knowledge-enhancing efforts regarding methods and tools for carrying out risk assessment, risk classification, and risk-based supervision. To this end, the Inspectorate needs to be allocated additional resources.

Swedish Financial Supervisory Authority

In 2018, Swedish Financial Supervisory Authority was allocated additional resources with the aim of strengthening the work to combat money laundering and terrorist financing. However, Swedish Financial Supervisory Authority has identified the need for further resources in the coming years in order to increase the agency's knowledge, develop cross-border collaboration and provide adequate and effective supervision.

The Swedish Enforcement Authority

The Swedish Enforcement Authority needs to be able to request that a person paying cash provides identification. At present, this is only possible in the case of certain executive sales. The money laundering risks would also be reduced if the Enforcement Authority no longer needed to accept cash.

The County Administrative Boards

Business operators covered by the Anti-Money Laundering Act and the oversight of the county administrative boards are not engaged in activities requiring a licence (aside from pawnbrokers). Business operators covered by the Anti-Money Laundering Act and the supervision of the county administrative boards must provide notification of the registration of their business to the Swedish Companies Registration Office's Beneficial Ownership Register, aimed at preventing money laundering. Notification to this register is, according to the Anti-Money Laundering Act, a requirement for conducting the business activity covered by this obligation.

One problem for the county administrative boards is that there are business operators conducting business activity subject to the notification requirement but which are not fulfilling this obligation. This may be due to the business operator not being aware of the requirement, or that despite this knowledge they still neglect to submit notification of their business for various reasons. This means that there is probably a significant pool of business operator subject to the notification requirement that the

county administrative boards are unaware of. There is a need for measures linked to the following areas:

- Improve the conditions for performing a conduct review on foreign representatives.
- The possibility of amending the confidentiality legislation so as to increase the scope of the county administrative boards to initiate supervision after receiving classified information from other agencies.
- The possibility of imposing penalties on those business operators subject to the notification requirement that have not notified their registration to the Swedish Companies Registration Office's Beneficial Ownership Register. As the county administrative boards are to employ a risk-based approach to counteract money laundering and terrorist financing, the county administrative boards are required to carry out a risk assessment of the entities being supervised by the boards. At present, the county administrative boards need to develop methods and tools to carry out risk assessment, risk classification and risk-based oversight, as well as knowledge-enhancing initiatives. With this in mind, the boards are in need of resource reinforcements.

The Swedish Police Authority

The Police Authority needs to establish clearer responsibility for dealing with issues linked to money laundering and terrorist financing. As it looks today, there are highly qualitative insights and expertise spread across the authority. This would also involve work with situation reports, development needs and training initiatives for the authority's work with combating money laundering.

Through the establishment of the Police Authority's plan to combat serious and organised crime, the fight against nation-wide criminality with a special focus on money laundering has been prioritised in police operations. The regional level is chiefly responsible for the current focus. However, the knowledge and capacity to take on this responsibility, especially in terms of investigating more complex, often cross-border money laundering schemes is insufficient.

The Financial Intelligence Unit needs to increase its staff and be given operational support in order to be able to meet the demands on Sweden's FIU according to FATF's regulations and EU legal acts. The assignments are expected to increase in number.

The Swedish Inspectorate of Auditors

With the current regulatory constraints, the Swedish Inspectorate of Auditors does not have the scope to perform conduct reviews according to Chapter 7, Section 6 of the Anti-Money Laundering Act in conjunction with the registration of auditor firms or in the supervision of certified auditors and registered auditor firms. The Swedish Inspectorate of Auditors only has the possibility of accessing information from the criminal records in conjunction with examining the suitability of persons who the authority is considering to approve or authorise.

The corresponding restrictions apply to information in the register of suspects. In practice, this means that the Inspectorate cannot access information from the criminal records or register of suspects for auditors under the Inspectorate's supervision for any other purpose, such as performing a conduct review as part of its oversight or in conjunction with a person assuming a management position in an auditor firm. Furthermore, shareholders and members of the board of a registered auditor firm may be individuals that do not come under the ordinary supervision of the Inspectorate, i.e. individuals who are not approved or authorised auditors and who the Inspectorate has thus never had the opportunity to look up in the registers.

The Swedish Tax Agency

There is a need to review how the Swedish Tax Agency can more clearly counteract money laundering:

- There needs to be an easing of the confidentiality restrictions between the various branches of operations within the agency so that information regarding such money laundering transactions that do not reach the level of filing a police report can be forwarded from the taxation organisation to the intelligence organisation within the Tax Agency Fraud Unit (SBE) and be included in the exchange of intelligence information that regularly takes place between law enforcement authorities' intelligence units. Easing confidentiality restrictions would also enable SBE to provide information on suspected money laundering linked to tax crime to the Tax Agency's control unit within the taxation organisation.
- Money laundering offences should be included in SBE's crime directory (which can currently only be investigated at the request of a prosecutor).
- Working to prevent and counteract identities, coordination numbers and population database registration from being misused and exploited by criminal operators.
- The agency should be obligated to inform prosecutors of suspected offences under the Act on Penalties for Money Laundering Offences and the Act on Criminal Responsibility for the Financing of Particularly Serious Crime in some cases.

The Swedish Gambling Authority

To prevent the gambling market from being used for money laundering and terrorist financing, the Swedish Gambling Authority considers that in-depth knowledge is required on, above all, complex international money laundering networks. This can be achieved through increased operational cooperation both nationally and internationally with government agencies and business operators for the exchange of experience and information regarding new money laundering methods.

Swedish Customs

Swedish Customs currently lacks the mandate and authority to detain cash shipments in conjunction with border crossing. If the agency was given this opportunity (without obligation), this would contribute to greater efficiency in combating suspected money laundering and terrorist financing. For example, a mandate under the Anti-Money Laundering Act and Financing Act would entail that Swedish

Customs would be able to seize money and take other coercive measures in a criminal investigation.

Swedish Customs has no direct mandate to focus work on money laundering and terrorist financing. In this context, such a mandate would facilitate collaboration between Swedish Customs and other agencies included in the cooperation group against money laundering and terrorist financing. It would also clarify that there may be a link between customs criminality and money laundering and terrorist financing.