National Risk Assessment of Money Laundering and Terrorist Financing in Sweden **2020/2021**

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

Published by: The Swedish Police Authority
Unofficial translation, in case of any discrepancies between the English version and the original Swedish version the latter will prevail.

Registration number: A052.211/2021

Version: August 2021

Abstract

This is the second report from the coordination function on the joint risk assessment for money laundering and terrorist financing in Sweden. This risk assessment was created by 16 government agencies and the Swedish Bar Association. The starting point of the assessment is Swedish legislation on money laundering and its 22 areas of application.[1] The report is based on a survey of threats and vulnerabilities in particular sectors. Risk assessments have been performed for each of these sectors and the risks have been compared in a national context in relation to their potential impacts on society. Money laundering risks are assessed on a four-tiered scale, while the assessment of risks related to terrorist financing is presented in qualitative terms. Finally, proposed measures for reducing the identified risks are presented.

Money laundering risk assessment

Among the businesses that are under the supervision of Finansinspektionen (the Swedish Financial Supervisory Authority), the assessment found that the highest risk level exists in the *banking* and *financial institutions*. Banks represent the fundamental financial infrastructure of the country, and more or less all laundered money needs to pass through the banking system at some stage. Financial institutions are also highly vulnerable to the risk of exploitation, particularly bureaux de change and the large-scale, unregistered trade in virtual currencies. Among the entities under the supervision of the county administrative boards, the *trade in goods sector* is assessed to have the highest threats and vulnerabilities. Risk is also assessed to be high among *company formation agents*, *business brokers* and *trust administrators*. *Gambling companies* and *real estate agents* are also at risk of being exploited for money laundering, which may go unnoticed by the businesses themselves and the involved banks. The gambling market is considered to have the highest threat level due to its broad accessibility and the ability to turn over relatively large amounts of money in a short period of time.

Risk assessment of terrorist financing

In contrast to money laundering, the purpose of which is to hide the origin of assets, terrorist financing aims to hide the destination of the money. Terrorism can often be financed with small amounts of money, and these funds may be obtained legally or illegally. Money may be collected in a variety of ways, for example, through deposits into accounts that belong to private individuals, associations, foundations

[1] See the Money Laundering and the Financing of Terrorism (Prevention) Act (2017:630), Ch.1, Section 2 first paragraph (1–22) (the areas of application that were relevant during the period reviewed). The assessment also describes a couple of other sectors in the sector catalogue, as these provide an important context in the presentation of the risk analysis.

and companies. Money transfers may take place through registered payment service providers, through payment services provided by authorised or registered institutions such as banks, credit institutions and payment service providers, as well as through unregistered money transfer agents that are not under the scrutiny of supervisory authorities, such as hawaladars. The sectors assessed to be at the highest risk of terrorism financing are the banking, payment institution and payment services sectors. Other areas that are assessed to be at risk, although to a lesser extent, are issuers of electronic money, consumer credit providers and other financial activities, including bureau de change. The Swedish gambling market should also be included in this context, considering the opportunity it presents for both cross-border transactions and the degree of anonymity.

ABBREVIATIONS

Brå	Swedish National Council for Crime Prevention (Brottsförebyggande rådet)
FATF	Financial Action Task Force
Fintech	Financial technology, a company that combines services with software technology
FOI	Swedish Defence Research Agency (Totalförsvarets forskningsinstitut)
Fipo	Financial Intelligence Unit of Sweden (Finanspolisen)
IS	Islamic State
NPO	Non-profit organisation
PKK	Kurdistan Workers' Party
PTL	Money Laundering and the Financing of Terrorism (Prevention) Act (2017:630), shortened to the Anti-Money Laundering Act in this assessment – Swedish: Lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism
PTBL	Act on penalties for money laundering offences (2014:307) – Swedish: Lagen (2014:307) om straff för penningtvättsbrott
SIMPT	Swedish Anti-Money Laundering Institute (Svenska institutet mot penningtvätt)
SNI codes	Swedish Standard Industrial Classification

Extended summary

Introduction

Sweden's effort to combat money laundering and terrorist financing is generally succeeding. The Financial Action Task Force (FATF), which has recently evaluated Sweden's anti-money laundering efforts, confirms this assertion.[2] But at the same time, money laundering is widespread in Swedish society, and criminals are constantly finding creative new ways to mask the source of their criminally acquired funds through legitimate activities. Terrorist financing occurs on a smaller scale, but is still a serious societal problem, especially since even a small amount of money can go a long way in financing terrorist activities. It is therefore important to take a risk-based approach to achieve an effective, resource-efficient regime to stop money laundering and terrorist financing, where different parts of society work in collaboration to achieve this end.

Purpose and target audience

The coordination function for measures against money laundering and the financing of terrorism has been tasked with producing a national risk assessment. The aim of the 2020/2021 risk assessment is to assess the risks in the sectors defined in the Anti-Money Laundering Act and to identify strategy-based measures that reduce risk. Furthermore, the aim is to provide assistance to supervisory authorities and support businesses. The intended recipients of this risk assessment are mainly the businesses subject to the regulations for money laundering and terrorist financing, the Government Offices and the members of the coordination function.

Risk assessment – money laundering

Sectors with significant or high risk

Financial institutions that have a high inherent risk of money laundering are banking services and other financial activities.[3] As a result of the elevated threat level, banks have established extensive routines and monitoring systems, while the smaller financial institutions are generally less equipped to address these threats. The risk level in the banking sector is therefore considered to be *significant*, i.e. lower than the level in the sector for other financial activities, where the risk is classified as *high*. The risk level for payment institutions, payment service providers and electronic money issuers is classified as *significant*.

Within the non-financial sectors, the consumer goods and retail sector is the sector assessed to have the highest threats and vulnerabilities. Cash purchases of

---

[2] See the government's website (in Swedish) www.regeringen.se/pressmeddelanden/2017/04/god-niva-pa-sveriges-system-for-bekampning-av- penningtvatt-och-finansiering-av-terrorism-enligt-fatf/ (accessed 08/03/2021).

[3] Risk is determined according to threat vulnerability. See the method section.

luxury goods offer anonymity up to a certain limit, and criminal actors do not need specialised knowledge to launder money in the sector. Other sectors where the risk of money laundering is assessed as *high* are company formation agents, business brokers and trust administrators. Businesses assessed at the *significant* risk level include business centres, postbox service companies, independent lawyers, tax consultants and businesses that offer accounting and auditing services.

The risk of money laundering is *high* for gambling companies and *significant* for real estate agents. The gambling market is considered to have the highest threat level due to its broad accessibility and the ability to turn over relatively large amounts of money in a short period of time. The real estate sector is also attractive to criminals seeking to launder and invest money, but it is not as likely to be used as other traditionally more attractive sectors.

Sectors where money laundering risks may result in the most severe consequences

It is important to emphasise that a high risk in a particular sector does not necessarily mean there is a high risk from a national perspective. In order to be able to compare one sector with another, we also need to consider the potential *societal consequences* of money laundering. Banking is the sector where money laundering has the potential to have the most severe consequences. The high volume of money that is turned over and the fact that, in principle, all forms of financial arrangements pass through the banks at some stage, means that the risk is considered high from a national perspective. Financial institutions are also assessed to be high risk at a national level. The negative societal effects of money laundering in financial institutions are assessed to be somewhat smaller compared with the banking sector, but on the other hand, the risk that money laundering actually occurs has been classified at the highest level on the scale.

There is an especially high risk for businesses that operate in the Swedish market without the necessary authorisation or license.

Risk assessment – financing of terrorism

In contrast to money laundering, the purpose of which is to hide the origin of assets, terrorist financing aims to hide what the assets are used for. Terrorism can often be financed with small amounts of money, and these funds may be obtained legally or illegally. The use of digital banking and money transfer services facilitates the collection and transfer of money and occurs through both licensed and unlicensed businesses. The sectors assessed to be at the highest risk of terrorist financing are banking services, payment institutions and payment services. Other areas that are assessed to be at risk for the financing of terrorist activities, although to a lesser extent, are issuers of electronic money, consumer credit providers and other financial activities, including bureau de change. The Swedish gambling market should also be included in this context, considering the opportunity it presents for both cross-border transactions and the degree of anonymity.

- Within certain sectors that fall under the scope of the Anti-Money Laundering Act, threats and vulnerabilities are high, which equates to a high risk of money laundering. Both public and private actors in society need to raise the level of awareness of the problems and challenges associated with combatting money laundering and take the necessary steps to reduce risk. The sectors with the highest threats are financial institutions, retail goods, company formation agents and business brokers, trust administrators and gambling companies. Additional risk-mitigation measures are also needed in the areas where the consequences for money laundering are particularly severe, including the banking and financial institution sectors.
- Risks do not only occur in sectors where transactions are used as part of money laundering schemes. There are also risks in other sectors where the conditions for money laundering can be created, for example, when criminals exploit the sector to build legitimate facades for companies or otherwise create the appearance of legitimacy for illicit transactions. These vulnerable sectors include accounting and auditing services, company formation agents and business brokers. Both types of risk presented here can be limited by strengthening the businesses' routines and monitoring systems, thus reducing vulnerabilities.
- The risk assessment highlights the need for improved opportunities to take action against operators who carry out activities without the required authorisation, license or registration. There is also a need to be better able to identify the operators who fall under the scope of the Anti-Money Laundering Act, for example, by ensuring the Swedish Companies Registration Office's anti-money laundering register is correct and up to date. Furthermore, there are sectors that are not currently covered by the Anti-Money Laundering Act, despite the fact that the activities carried out in these sectors are largely similar to activities that fall under the scope of the law.
- There are still a number of cross-sectoral challenges that need to be addressed at the national level, including identifying and counteracting complex, large-scale money laundering schemes and hijacked, fake or misused identities.

Contents

1 Introduction 12
1.1 Risk level in Sweden 12
1.2 Purpose of the assessment 13
1.3 The coordination function 13
1.4 Regulations 13
1.5 Risk assessment – focus and delimitations 14
1.6 Target group 14
1.7 Overall method and implementation 14
1.8 Sources and special challenges 15
1.9 References 16
2 The current situation in Sweden 17
2.1 Economic aspects 17
2.2 Organised crime and financial crime 18
2.3 Increased number of money laundering offences 20
2.4 Reporting to the Financial Intelligence Unit of Sweden (Fipo) 23
2.5 Overall 25
3 Financing of terrorism 26
3.1 Financing of terrorism in Sweden 26
3.2 The intent and ability of various actors to finance terrorism 27
3.3 Collection process 28
3.4 Procedure for transferring money 28
3.5 Financing of terrorism – organised crime and convictions 29
3.6 Financing of terrorism from a Europe-wide perspective 30
3.7 Overall 31
4 Risk analysis and impact assessment 32
4.1 Risk per sector based on a threat and vulnerability assessment 32
4.2 Consequences of money laundering from a national perspective 38
4.3 Consequences of terrorist financing from a Europe-wide perspective 41
5 Other risks 43
5.1 Complex schemes 43
5.2 Activities not covered under the scope of the Anti-Money Laundering Act 44
5.3 Foundations 45
5.4 The fund-raising sector and the non-profit sector 46
5.5 Private–public collaboration 47
5.6 Overall 47
6 Risk mitigation measures 49

7.Sector catalogue -assessment of money laundering and terrorist financing 55
7.1 Banking or financing business 56
7.2 Life insurance business 62
7.3 Securities business 67
7.4 Currency exchange activities and other financial activities or deposit-taking activities. 71
7.5 Insurance mediation 79
7.6 Issuance of electronic money 83
7.7 Fund operations 88
7.8 Payment institutions 92
7.9 Registered payment service providers 100
7.10 Consumer credit operations 103
7.11 Mortgage lending business 108
7.12 Real estate agent – full registration 112
7.13 Merchants 116
7.14 Pawnbrokers 119
7.15 Accounting and auditing services 122
7.16 Tax Consultants 126
7.17 Independent lawyers 129
7.18 Company formation agents and business brokers 132
7.19 Business centres and postbox service companies 136
7.20 Trust administrators 139
7.21 Board representation and nominee shareholders Trust administrators 142
7.22 Activities as an authorised auditor, approved auditor or registered audit firm 145
7.23 Advocates and law firms 150
7.24 Swedish gambling market 157
Appendix: 164
Definitions of threat, vulnerability and consequence . 164
Appendix: 166
Process and method 166
Risk scale 167
Consequence scale 169
Appendix: 171
Special challenges for county administrative boards . 171
County Administrative Boards' information collection 171
Unregistered operators 172
Registration error 172

1 Introduction

This report is the coordination function's second national risk assessment of money laundering and terrorist financing. The assessment is based on a survey of threats and vulnerabilities according to the division used in the scope of application of the Anti-Money Laundering Act. The aim of the report is to increase the understanding of the risks Sweden is exposed to in these areas and to provide proposals for how the Swedish regime can reduce these risks.

It is important to take a risk-based approach to achieve an effective, resource-efficient regime to stop money laundering and terrorist financing, where different parts of society work in collaboration to achieve this goal.[4] In Sweden, actors from a variety of segments are affected, with supervisory authorities, law enforcement agencies and business operators (private actors) being the most relevant.[5] In addition, certain parts of civil society are also at risk of being exploited for the purposes of money laundering and terrorist financing.

The effort to combat money laundering and terrorist financing does not only take place within Sweden's borders; it always extends to several levels internationally. On the global level, Sweden's fight against money laundering and terrorist financing includes cooperation within the Financial Action Task Force (FATF), and at EU level, through legislation and regulations. In addition, Sweden maintains an ongoing dialogue with neighbouring countries in the Nordic region.

1.1 Risk level in Sweden

Sweden's effort to combat money laundering and terrorist financing is generally succeeding. The Financial Action Task Force (FATF), which has recently evaluated Sweden's anti-money laundering efforts, confirms this assertion.[6] But at the same time, there a number of challenges the Swedish regime needs to overcome.

Terrorist financing occurs on a smaller scale, but is still a serious societal problem, especially since even a small amount of money can go a long way in financing terrorist activities. Currently, the threat of terrorism is at level three on a five-point scale, where the main terrorist threat comes from Islamic-motivated terrorism and far-right extremists.[7] Terrorism threatens the stability of democracy and undermines security both within Sweden's borders and abroad. In addition to

---

[4] Read more in the Swedish National Council for Crime Prevention's (Brå) report: *Money laundering and other money management – Criminal money, black money and murky money in the legal economy.* Report 2015:22 (Stockholm, 2016).

[5] Government Offices: *Combating money laundering and terrorist financing (Bekämpning av penningtvätt och finansiering av terrorism),* published 13 October 2015 (updated 29/10/2020).

[6] See FATF's website and *Sweden's measures to combat money laundering and terrorist financing.* The report can be found here: www.fatf-gafi.org/countries/st/sweden/documents/MER-Sweden- 2017.html (3/11/2020).

[7] National centre for Terrorist Threat Assessment (Nationellt centrum för Terrorhotbedömning), summary: *Terrorist threat assessment – 2021 (Bedömning av terrorhotet för 2021).* www.sakerhetspolisen.se/kontraterrorism/nationellt-centrum-for-terrorhotbedomning.html

the harm caused by human suffering, increasing injustice and the destabilisation of democracy, confidence in the financial system can also deteriorate rapidly if it is systematically used to finance terrorism.

Although the Swedish government has been largely successful in this area, a number of challenges were identified in the national risk assessment from 2019. Several of these challenges still need to be addressed within the Swedish regime. These challenges include systemic risks linked to strawmen, population registration and exploited identities, particularly considering that the Swedish system is dependent on a high level of trust in basic identification.[8] Shortcomings regarding the dissemination, access and production of information and knowledge within the Swedish regime were also highlighted in the 2019 risk assessment. In addition, the assessment highlighted the lack of resources and tools as well as the inadequate legal basis within certain areas.[9] These risks are managed in a variety of ways within the Swedish regime, even though several of these threats can only be compensated for, not completely prevented.

1.2 Purpose of the assessment

The purpose of the 2020/2021 national risk assessment is to identify and assess risks in the sectors defined under the Anti-Money Laundering Act.

1.3 The coordination function

Since 2018, the Swedish Police Authority has headed the coordination function, which is tasked with managing measures implemented to combat money laundering and terrorist financing. This function consists of the following 16 agencies, together with the Swedish Bar Association: 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 Security Service, Swedish Customs and the Swedish Prosecution Authority. The risk assessment is the result of a joint effort between the members of the function.

1.4 Regulations

The effort to combat money laundering and terrorist financing is based on two sets of regulations that form the basis for Sweden's overall capacity in these areas: administrative and penal. The phrase "*The Swedish regime against money laundering and terrorist financing*" refers to all actors who bear a responsibility under this legislation.

---

[8] Systemic deficiencies that have an impact on operators' ability to comply with the regulations regarding the "customer due diligence" process, but also the ability of supervisory authorities to verify true identities and physical population registration.

[9] The 2019 national risk assessment can be found here: www.polisen.se/om-polisen/polisens-arbete/penningtvatt/nationell- samordning-mot-penningtvatt-och-finansiering-av-terrorism/(updated 24/11/2020).

The administrative regulations, namely the Money Laundering and the Financing of Terrorism (Prevention) Act (2017:630), are central to this effort and are intended to prevent and counteract the exploitation of financial activities and other business activities for the purposes of money laundering and terrorist financing.[10] The penal regulations that primarily fall under the scope of the Act on penalties for money laundering offences (2014:307) and the Act on Criminal Responsibility for the Financing of Particularly Serious Crime in some cases (2002:444) aim to prosecute individuals who have engaged in money laundering or terrorist financing.

1.5 Risk assessment – focus and delimitations

The assessment primarily covers the Anti-Money Laundering Act and its areas of application (see Chapter 7, sector catalogue).[11] This also includes the risks of terrorist financing. Given these delimitations, it is likely that there are areas that may be vulnerable to money laundering or terrorist financing that are not analysed here, as these fall outside the scope of the law. The period analysed includes the years 2018 and 2019.

1.6 Target group

The report is primarily intended for operators who are subject to the regulations for money laundering and terrorist financing, but also for the relevant supervisory authorities, the Government Offices and the members of the coordination function.

1.7 Overall method and implementation

This report analyses *threats* and *vulnerabilities* for each sector. Threats refer to the capacity of actors to exploit a sector for money laundering or terrorist financing. Vulnerabilities refer to the limitations of and any shortcomings within each sector regarding the ability to respond to threats and prevent money laundering or terrorist financing. The overall assessment of threats and vulnerabilities provides a risk value for the individual sector, *without a comparison* with other sectors.

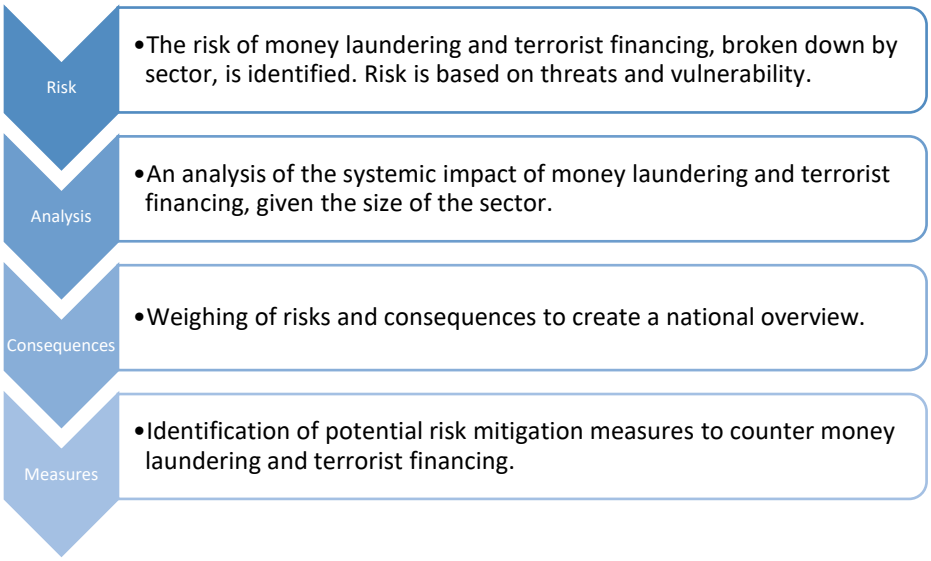
Based on the threats and vulnerabilities that are identified, the consequences that these risks may entail are then analysed. An impact assessment makes it possible to *compare* the sectors and create an overall picture at the national level. This assessment and overview aim to guide decisions regarding which sectors should be prioritised or which areas should be targeted by legislation. See also the method description in the appendix Process and Method.

Figure 1.1 outlines how the risk assessment process has been developed and how the different phases are connected.

[10] The law is supplemented by an ordinance and several regulations.

[11] As of 01/10/2019, pursuant to the fourth Anti-Money Laundering Directive.

FIGURE 1.1
Risk assessment process



1.8 Sources and special challenges

Sources from all members of the coordination function have been used in this risk assessment. A particularly important source of documentation has been the reporting to the Financial Intelligence Unit of Sweden (Fipo) during the period investigated. Crime statistics collected from the Swedish National Council for Crime Prevention and the Swedish Tax Agency, as well as questionnaire responses from operators and material obtained from operators, were also used as a basis for the analysis. All members of the coordination function have contributed extensive expertise in the assessment of threats and risks. In addition, the assessment has included dialogue and the exchange of information with industry and sector representatives, as well as with the non-profit sector to a certain extent. The documents collected have been subject to discussion and analysis in joint working group meetings.

When taking inventory of documentation for parts of the analysis, it was noted that access to information was limited for certain sectors. It has been especially challenging to identify reliable documentation for the sectors under the supervision of the county administrative boards. One reason for this is that, in terms of the various sectors, the county administrative boards are limited in their supervisory responsibilities according to what is prescribed in the Anti-Money Laundering Act. The supervisory responsibilities of the county administrative boards also cover a broad range of sectors that differ significantly. The information provided by the county administrative boards is largely based on information from the survey that the county administrative boards conducted at the beginning of 2020, as well as trends and information gathered during their supervisory activities.

For this reason, the information and conclusions the county administrative boards provide for each sector can be seen as estimates.

1.9 References

In *Chapter 2*, the national risk assessment is introduced by establishing a context. Here, a general overview of the situation in Sweden is described based on the situation, vulnerability and general crime trends. The purpose of this section is to highlight the overall factors that impact the risk profile in Sweden. *Chapter 3* presents an analysis of the occurrence of terrorist financing in Sweden. The assessment details the capacity of different actors to finance terrorism, approaches to raising funds and the transfer of funds, as well as the general consequences this may have. The chapter concludes with a look at terrorist financing based on a Europe-wide perspective. *Chapter 4* presents an analysis of the current risk level in Sweden. The chapter describes both the main threats and vulnerabilities in the different sectors, as well as the consequences of the identified risks at the national level. *Chapter 5* presents a discussion of the challenges associated with developing a risk assessment broken down by sectors and the consequences this may have for the understanding of the identified risks. *Chapter 6* presents proposals for risk mitigation measures that can be implemented at the national level. Lastly, *Chapter 7* presents the risks of money laundering and terrorist financing in the various sectors. A more detailed description of the definitions, method and process, as well as special challenges, can be found in the appendix.

2 The current situation in Sweden

This chapter briefly introduces the context in which money laundering and terrorist financing occur in Sweden. On the one hand, the chapter presents an overview of specific trends in the Swedish economy, and on the other hand, it outlines a picture of money laundering and profit-driven predicate offences. The chapter also describes the frequency of reporting to the Financial Intelligence Unit of Sweden (Fipo), the number of crimes reported to the Swedish Police Authority and cases received by the Swedish Economic Crime Authority. The purpose is to provide a background for the period during which the risk assessment was conducted. The main observations presented in the chapter are:

- **Less cash at the banks.** Swedish banks are handling cash to a lesser extent than before. Therefore, organised crime increasingly targets cash-intensive companies and currency exchange businesses.
- **Legal structures.** The work to combat money laundering and terrorist financing is being hampered by the use of legal structures to conceal illicit activities and the beneficial owners behind the activities.
- **Strawmen and identification.** The system depends on a high level of trust in the primary verification of a person's identity. Therefore, the activities of straw men and the misuse of identities are issues that are especially problematic for the Swedish regime.
- **Commonly occurring predicate offences.** The main forms of profit-driven crime that are closely linked to money laundering are fraud, drug trafficking and other financial crimes.
- **Higher rate of prosecution for money laundering offences.** The coordination function notes an increase in the number of suspected fraud cases that result in a conviction for money laundering when the evidence is insufficient to prove who committed the act of fraud.
- **Increased reporting.** Operators' reporting of suspicious transactions and activities to the Financial Intelligence Unit of Sweden (Fipo) has increased in recent years. However, reporting in several sectors still occurs to a very limited extent.
- **Technological development creates new challenges.** The authorities included in the coordination function need to be better equipped to keep pace with technological developments in the Swedish economy, which continuously creates new opportunities for criminals to engage in money laundering.

2.1 Economic aspects

Sweden is an open and modern economy with a comparatively large financial sector in relation to the country's GDP. The fast pace of technological development in IT and finance means new services and products are constantly emerging.

The financial system is largely dominated by card transactions, and the handling of cash therefore happens on a much smaller scale. The use of cash is declining among the general public.[12] Several bank branches in Sweden have now completely stopped over-the-counter cash transactions due to low demand and high costs.[13]

Swedish authorities believe that cash is generally associated with a high risk of money laundering and terrorist financing. Large cash transactions often raise suspicion. Several Swedish authorities have noted that actors in organised crime are showing an increased interest in cash-intensive businesses, bureau de change or money transfer services, as a result of the reduced amount of cash circulating in society.

The large scale of Sweden's financial sector, coupled with the advanced financial services that involve transactions via the cross-border payment system, affect the level of risk exposure for money laundering and terrorist financing. The opportunities offered by new types of payment solutions, such as prepaid cards, mobile wallets and virtual currencies, can make criminal organisations less dependent on cash and create new avenues to deal in illicit funds.

Given the prevailing trends in the Swedish economy and the ability of organised crime to rapidly adapt to new developments, a number of new opportunities and risks regarding money laundering and terrorist financing are rapidly emerging. For example, technological development in some financial services results in increased anonymity and reduced traceability in terms of information, which can create new opportunities for unscrupulous actors to move criminal proceeds. It is therefore important to adapt legislation to respond to these developments so that new services are also subject to the provisions of the Anti-Money Laundering Act. It is also important for the authorities within the coordination function to have the capacity to keep pace with technological developments. In order to ensure that this can occur, authorities need to be able to continuously acquire *knowledge* of new technological solutions and *legislation* needs to be continuously adapted so that new services are subject to the provisions of the Anti-Money Laundering Act.

2.2 Organised crime and financial crime

From an international perspective, Sweden is generally seen as a country with a low level of crime.[14] Sweden consistently ranks close to the top on international indices, such as the Rule of Law Index and the Corruption Perceptions Index.[15] [16]

---

[12] It should be mentioned here that there are still segments in society where the handling of cash occurs to a higher degree than it does for society as a whole. There are also indications that cash is being used to an increasing extent in some circles.

[13] There is an interest in preserving the use of cash for the benefit of society (for example, in the event of a crisis). See the report: *Secure access to cash* (SOU 2018:42). Found here: www.regeringen.se/49cf6d/contentassets/79026c9e608946bdbfa60067ddae0c0d/tryggad-tillgang-till-kontanter-sou-201842.pdf (retrieved 14/12/2020).

[14] See the Financial Action Task Force's (FATF) evaluation of Sweden, MER Sweden 2017: www.fatf-gafi.org/publications/mutualevaluations/documents/fur-sweden-2018.html (retrieved, 12/12/2020).

[15] Ranked 3rd in the *Corruption Perceptions Index 2018, Transparency International*. Found here: www.transparency.org/cpi2018 (retrieved 11/12/2020).

Nevertheless, Sweden does face a large number of challenges in these areas. Organised crime has an impact on certain local communities, financial crime is significant and the predicate offences to money laundering vary significantly. Crime committed in Sweden increasingly has international elements and is becoming increasingly cross-border in nature. This type of crime is also increasingly using legitimate structures to conceal illegal activities. Specialised criminal services are being developed and marketed in ways that largely resemble commercial business models.

Organised crime generates proceeds from a variety of criminal activities, and this money needs to be laundered in order to be used for legitimate transactions. Among other sources of illicit funds, large sums can be raised through tax offences. These approaches are generally connected to unreported taxes and fees relating to labour, primarily in the construction, cleaning and transport sectors. In order to be able to circumvent tax rules so the businesses can pay cash wages evading income and employment tax) in large-scale operations or finance other expenses, funds in accounts need to be able to be converted into cash. Some schemes also include the use of services, such as those provided by a financing or factoring company. In more complex cases, elaborate schemes are developed where criminals run their own invoicing, financing or exchange office. Welfare crime, drug dealing, excise tax fraud and fraud are other predicate offences that tend to generate large profits.[17]

It has also been established that a large part of the profit from organised crime comes from various types of financial crime. In 2018, for example, the Swedish Tax Agency reported a total of 14,874 violations, of which 10,221 were tax crimes and 1,865 were accounting crimes. The corresponding figure for 2019 was a total of 12,019 reported crimes, of which 7,884 were tax crimes and 1,368 were accounting crimes. Large sums of money are raised in organised crime from tax avoidance schemes related to undocumented labour.[18]

It has been assessed that organised crime has a continued need for cash in order to be able to profit from various predicate offences and for the illegal purchase of and payment for goods and prohibited/restricted goods. However, the use of strawmen and frontmen reduces the need for cash, as more accounts and identities can be used to easily execute and conceal transactions. This means that the number of people who may be suspected of being involved in criminal schemes is increasing. The relationship between predicate offences and money laundering is becoming increasingly complex, which creates a number of challenges for law enforcement agencies, supervisory authorities and operators in terms of the ability to grasp the prevalence of and modus operandi used within organised crime.

---

[16] Ranked 4th in the *Rule of Law Index 2020, World Justice Project*. Found here: worldjusticeproject.org/sites/default/files/documents/WJP-ROLI- 2 0 2 0-Online_0.pdf (11/12/2020).

[17] It should be noted here that temporary funding has been allocated to strengthen the fight against welfare crimes and other financial crime, including money laundering.

[18] Note that in the statistics of reported crimes, there may be multiple suspected offences (which can also affect long term prosecution statistics).

Organised crime has long exploited the competitive advantage offered by the avoidance of taxes, VAT, fees and duties in the consumer goods sector. This has an impact on the business community as it threatens competitive neutrality. But it also contributes to the creation of an informal economy where goods and services are exchanged both with and without cash. Trade-based schemes, where criminal money is laundered through the import of goods, also provide advantages for organised crime while undermining legal trade. In trade-based schemes, perpetrators often follow the majority of applicable rules. This makes the schemes difficult for individual authorities to detect and requires collaboration and the exchange of information between different actors.

2.3 Increased number of money laundering offences

Financial crime, including money laundering, constitutes a major problem for society. The Act on penalties for money laundering offences was therefore enacted as a tool to combat this type of crime.[19] As mentioned earlier, money laundering is a type of crime that is motivated by concealing and assimilating one's own – or someone else's – criminally obtained funds. Any criminal activity that can generate criminal money can thus constitute a predicate offence for money laundering.

Since the Act on penalties for money laundering offences entered into force, the number of reported money laundering offences has increased significantly. At the end of 2019, the number of crimes reported during the year was close to 7,000. This can be compared with an average of 500 reported crimes per year during the years 2010–2013, when the previous money laundering legislation was in force. There are likely a number of different factors that influence the number of crimes that are reported. The significant increase in reported crimes can, for example, be related to the fact that changes in the legislation that came into force in 2014 meant that the law can be applied to more situations, and that the authorities' knowledge of the law increased, and more crimes are therefore classified as money laundering. Another reason may be the increase in the number of reports for certain types of profit-motivated crime that may be predicate offences for money laundering. During the most recent ten-year period, for example, both the number of fraud cases reported and the number of reported benefits fraud cases have increased sharply, both of which are examples of profit-motivated crimes.

It can be noted in the crime statistics that total number of reported fraud cases has increased by 113 percent during the most recent ten-year period.[20] One of the most important drivers for this increase includes technological developments that enable criminals to find new ways to commit fraud.[21] Fraud committed via the internet can also impact a large number of people. The visibility of various criminal activities is also dependent on how well the control functions operate, as well as the

[19] As of 1 July 2014.

[20] Documentation obtained from the Swedish National Council for Crime Prevention's (Brå) reporting statistics.

[21] See the Swedish National Council for Crime Prevention's *Crime Trends in Sweden Until 2015* (editor Wallin Lisa) (2017:5).

resources allocated to detect and investigate these crimes.[22] The number of reported benefits fraud cases has increased by 120 percent over a ten-year period.[23] In 2019, 20,700 benefits fraud cases were reported, about 75 percent of which were violations committed against the Swedish Social Insurance Agency.[24]

Another example of profit-driven crime is drug-related crime. The profits from the illicit drug trade are an important source of income for organised crime, and for many criminal networks, drug dealing constitutes the network's primary income. A significant portion of the profit from the drug trade is spent on legitimate activities, for example, pub visits, gambling, exclusive cars, travel, designer clothing, gold jewellery and expensive watches.

What various money laundering schemes have in common is that they all aim to conceal the criminal origin of the property. Different types of crime may require different approaches. Therefore, a variety of sectors may be exploited at different times and situations, depending on the nature of the scheme in question. Typically, the complexity and number of measures in the money laundering scheme increase along with the amount of money involved, as larger sums often require this level of complexity. In addition, more complex criminal schemes can involve the formation of new companies or acquisition of existing companies for use as tools in the criminal act, which may require access to other measures and sectors.

Swedish research and international research have both demonstrated that financial crime yields greater benefits for the perpetrator than traditional crime, such as drug-related crime, dealing in/receiving stolen goods or human trafficking. Potential explanations for this are that criminals involved in financial crime basically appear to be running legitimate businesses. This means that they are better able to exploit societal structures to shield and enable their criminal activities. Furthermore, criminals who are involved in financial crime often have more resources at their disposal, both in terms of their own knowledge and in their ability to recruit suitable employees. Most financial crimes that are detected by or reported to authorities are discovered through government checks or by official receivers in bankruptcies. Taken as a whole, this means that a variety of sectors under the scope of the Anti-Money Laundering Act may be exploited depending on what measures are required to conceal the criminal origin of the profit or make it more difficult to trace criminal profits in the particular case.

Another way to illustrate how money laundering occurs is to examine the statistics of cases submitted to the police during the period 2018–2019.[25] This is presented in Chart 2.1

---

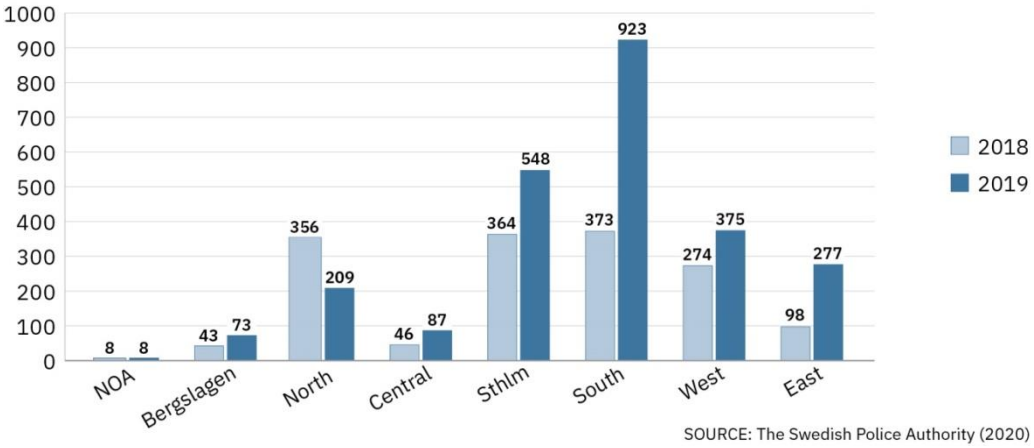
[22] See the Swedish National Council for Crime Prevention's *Fraud in Sweden* by Shannon, David; Hradilova, Selin Klara; Skinnari, Johanna; and Hörnqvist, Linda (2016:9).

[23] For further information on prosecutions and handled crimes, see the Swedish National Council for Crime Prevention *Processed crimes – crime statistics*: www.bra.se/statistik/kriminalstatistik/handlagda-brott.html (accessed 09/03/2021).

[24] See the following statistics from the Swedish National Council for Crime Prevention www.bra.se/statistik/statistik-utifran-brottstyper/bedragerier-och-ekobrott.html (retrieved 07/03/2021).

[25] A single *case filed* may contain one or more crimes, so the number of reported crimes is always more than the number of cases filed.

CHART 2.1
Number of cases received in 2018 and 2019



SOURCE: The Swedish Police Authority (2020)

The statistics cover all types of cases received that concern money laundering offences in the years 2018–2019 (money laundering, aggravated money laundering, misdemeanour money laundering and commercial money laundering).[26] The statistics are also revealing from a geographical perspective, as the majority of cases are handled in the South of Sweden and in the Stockholm region. This indicates, in part, that crime is a big city phenomenon, but also that all of Sweden is affected to some extent.

In addition to the table presented above, it can be noted that the Swedish Economic Crime Authority has received a large number of reports of suspected money laundering and commercial money laundering during the period 2018–2019. For 2018, 716 suspected cases of money laundering and commercial money laundering were registered. For 2019, the figure was 910 suspected cases.[27]

Finally, a recent analysis of almost 700 judgments in money laundering cases sheds light on how money laundering occurs. The review, which is based on an analysis of all judgements that have gained legal force in the period 2018–2019[28], illustrates that money laundering in Sweden is widespread and varied. The main observations of the analysis show:

- **Perpetrators.** A total of 1,589 defendants were identified during the period. Of these, 1,125 were charged with money laundering-related crimes (of which nine are counted in at least two judgements in the sample). The majority of defendants are men, who account for about 76 percent of the observations; 24 percent are women. The average age of defendants is just over 30 years, with a median age of 27 years. The age difference between the sexes is marginal.

[26] Refers to the crime codes used by the police: 5121–5126.

[27] The statistics refer to suspected crimes, not reports. Criminal suspicion can arise during the course of the investigation.

[28] The coordination function *Review of money laundering judgements 2018–2019* http://polisen.se/om-polisen/polisens-arbete/ penningtvatt/nationell-samordning-mot-penningtvatt-och-finansiering-av-terrorism/ (retrieved 05/02/2021) (2020).

- **Main predicate offences.** Fraud is the most common predicate offence for money laundering. Fraud cases account for 75 percent of predicate offences and occur in 79 percent of the prosecuted cases. Fraud cases can include both those who make the account available to criminals and the criminals who commit the act. Fraud takes a variety of forms, with vishing (via telephone) being the most common. In addition, fraud includes smishing scams (SMS) and phishing scams (web). The results presented above can be compared with the results reported by the Swedish National Council for Crime Prevention (Brå) in their study, which concluded that "... in a majority of the rulings (74 percent) for the period 2015–2017, some form of fraud has been a predicate offence for money laundering offences".[29]
- **Primary tools used in criminal acts** Apart from direct bank transfers, payment transfers via mobile applications and ATM withdrawals are the most common tools identified in the examination of the judgements. Payment transfers via mobile applications were used by about 53 percent of the defendants in some part of the money laundering chain. Withdrawals through agents include both cash withdrawals using banking services and currency purchases/cash withdrawals from exchange bureaus.

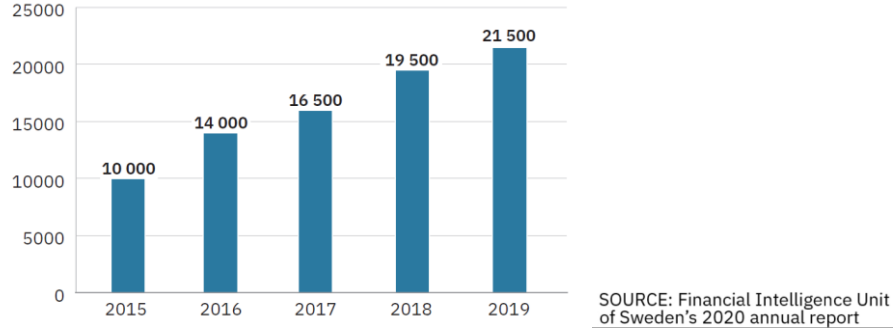
  Taken as a whole, this means that a variety of sectors under the scope of the Anti-Money Laundering Act may be exploited, depending on what measures are required to conceal the criminal origin of the funds or to make it more difficult to trace criminal funds.

2.4 Reporting to the Financial Intelligence Unit of Sweden (Fipo)

Another way to gain a greater understanding of the context for money laundering in Sweden during the relevant period is to look at the number of reports that are made to the Financial Intelligence Unit of Sweden (Fipo).[30]

In 2019, Fipo received a total of 21,695 money laundering reports from 285 unique operators bound by the reporting obligation. This is an increase of 12 percent compared to the reporting for 2018, and an increase of over 110 percent over the past five years (see Figure 2.2).

CHART 2.2 Number of reports received 2015–2019



SOURCE: Financial Intelligence Unit of Sweden's 2020 annual report

[29] Swedish National Council for Crime Prevention (Brå): *Money laundering offences: A follow-up of the application of the law* Report 2019:17.

[30] For recent figures, visit the Swedish Police Authority's website at polisen.se/om-polisen/polisens-arbete/finanspolisen/ (26/01/2021).

The increase may be due to the fact that more operators are subject to the reporting requirement during the period than in previous years (see Table 2.1[31]). The increase may also be due to increased requirements when the Money Laundering and the Financing of Terrorism (Prevention) Act (2017:630) entered into force.

TABLE 2.1

Reports received by Fipo 2018–2019 (by industry)*	2018	2019
Banking and financing activities, incl. credit market companies	14,421	16,831
Life insurance business	32	42
Securities market	10	19
Financial activities with a reporting duty	166	493
Insurance brokers	..	..
Electronic money institutions (EMI) (incl. agents' reporting)	50	39
Fund activities	..	..
Payment service businesses	3,764	3,045
Alternative investment funds	..	..
Consumer credit activities	149	185
Mortgage business	..	..
Real estate agents	..	23
Gambling services	474	614
Professional trade in goods	37	83
Pawnbrokers	6	6
Auditing (approved or authorised auditor or registered auditing firm)	7	20
Accounting or auditing services (not approved or authorised auditor or registered auditing firm)	16	19
Tax consultants	..	..
Advocate or associate at a law firm	..	6
Lawyer, other independent	..	..
Company formation agents, trust administrators, etc.	..	..
Supervisory authorities	23	19
Other authority (that handles cash) according to the Money Laundering and the Financing of Terrorism (Prevention) Act Chapter 4, Section 4, Para. 2	133	239
TOTAL	**19,306**	**21,695**

* The Payment Services sector includes both payment institutions and registered payment service providers, including currency exchange with card payments. Consumer credit activities were brought under the scope of the Money Laundering and the Financing of Terrorism (Prevention) Act (2009:62) on 01/07/2014. Gambling services were brought under the scope of the Money Laundering and the Financing of Terrorism (Prevention) Act (2017:630) on 01/08/2017. The professional trade in goods sector includes auction companies and companies trading in means of transport, scrap, precious gemstones, antiques and art at a value exceeding EUR 5,000. Blank rows in the table indicate that the industry reported five or fewer reports during the year.

Source: Financial Intelligence Unit of Sweden's 2020 annual report

[31] Two errors were detected in the statistics that were originally presented; these concern reporting to Fipo for 2019, partly the summation of the total number of reports, and partly the number of reports in the gambling sector. The total number of reports for 2019 has been adjusted from 21,709 to 21,695. The number of reports for the gambling sector has been adjusted from 481 to 614. Other sectors are not affected.

As shown in the table above, the largest numerical increase is in banking and financing activities, and this is a trend that has continued for several years. An increase is also evident in financial activities with a reporting duty and reporting from other authorities.[32] Reporting from the professional trade in goods sector is still low.[33]

2.5 Overall

The purpose of this chapter has been to place money laundering in a national context through a description of the Swedish economy and financial crime and to present a review of the number of reported money laundering offences and reports to the Financial Intelligence Unit of Sweden (Fipo). This provides a background for the national risk assessment and helps put the risk reduction measures in the proper perspective.

[32] The Swedish Enforcement Authority is engaged in development work in the areas relevant to the risk assessment and has been allocated temporary funding to strengthen efforts to counter welfare crimes and other financial crime, including money laundering.

[33] The Swedish Police Authority: *Financial Intelligence Unit of Sweden's annual report*, (2019) p.22. Found here: polisen.se/om-polisen/polisens-arbete/finanspolisen/(retrieved 11/12/2020).

3 Financing of terrorism

This chapter presents the ways terrorist financing can manifest itself, from a Swedish and European perspective. The account provided here looks at the capacity and approach different actors use to raise funds and transfer money, as well as the consequences this may have. The analysis here indirectly affects all sectors, but individual sector assessments can also be found in Chapter 7 (see the sector catalogue). Lastly, the chapter presents an overall picture of terrorist financing in Europe, which is deemed to be relevant for Sweden.
The main observations presented in the chapter are:

- **Difficulties presenting evidence.** To date, there have been few convictions in Sweden relating to the financing of terrorism. However, individuals suspected of financing terrorism have been prosecuted for other crimes, as the financing of terrorism in a number of cases overlaps with other financial crimes and organised crime.
- **Supporters of terrorist organisations.** Over the last ten years, there has been an increasing number of people in Sweden who are supporters of terrorist organisations and who have participated in the activities of these organisations.
- **Low cost of financing.** Several of the terrorist attacks that have been carried out in Europe have been executed by individual actors without specialised knowledge and with limited funding. This means that the threat of a terrorist attack is difficult to identify before the attack occurs. However, terrorist organisations do have a greater need for financial resources when it comes to infrastructure, recruitment, propaganda and operational activities.
- **Digital banking services.** The use of digital banking and money transfer services facilitates the collection and transfer of money.
- **Hawaladars.** Hawaladars are known to be used as a means to finance terrorism. At the same time, they are difficult to regulate, as the system is often the only way to transfer legitimate money to certain geographical regions.
- **Courier activities.** The transfer of money to terrorist organisations also takes place through courier activities.

3.1 Financing of terrorism in Sweden

Operators are obliged to report the suspected financing of terrorism to the Financial Intelligence Unit of Sweden (Fipo). These reports may involve transactions or irregular behaviour that may be suspected of being linked to terrorist financing. Unlike money laundering – where the origin of the assets is the critical aspect – it is the ultimate purpose of the transaction that drives terrorist financing. There is thus no need for a series of predicate offences and many terrorist crimes have been financed with relatively small amounts of money that have been acquired through

legal activities.[34]

The Act on Criminal Responsibility for the Financing of Particularly Serious Crime, in certain cases (2002:444) stipulates that, in certain cases, it is prohibited to collect, provide or receive money or other property. This is the case when the purpose is to support terrorist activities). This means that an individual is guilty of financing terrorism if he or she transfers money or other property to people who are planning or are actively engaged in carrying out terrorist crimes. The assets do not need to be used specifically in connection with a terrorist attack. The provisions also aim to combat the financing of, for example, recruitment and training activities connected to terrorist crimes and other particularly serious crime.[35] The Swedish Security Service receives regular notifications that actors in Sweden are financing terrorism. These are individuals and organisations that, primarily through small amounts of money, are suspected of financing terrorism abroad. Some of these suspected operations are well organised and include a number of different individuals and organisations, both in Sweden and abroad. In several cases, there is overlap with other criminal activities.

The majority of the funding originating from Sweden during the period analysed here is estimated to go to criminal and terrorist organisations outside Europe, including the Islamic State (IS), Al-Qaeda, the PKK and al-Shabaab. The growth of IS and the ongoing internationalisation of violence-promoting Islamist extremism in Sweden – combined with the digital transformation in society – are considered to be contributing factors to an increase in the financing of terrorism in the 2010s.

The number of people residing in Sweden who have previously been members of foreign terrorist organisations has never been as high as it is today, and a number of individuals from Sweden currently collaborate with organisations abroad. In the event that new organisations emerge with the ability to recruit thousands of individuals around the world, it is likely that financing for these terrorist activities will also originate from Sweden.

Experience on the international level shows that financing the planning, preparation and execution of a terrorist attack does not require a large amount of money. This means that it is crucial to prevent even small amounts of money from reaching the intended recipient, as this helps to reduce the risk of terrorism and weakens the financial capacity and operations of terrorist organisations.

3.2 The intent and ability of various actors to finance terrorism

A highly motivated financier can collect and transfer money quickly, easily and without significant costs. The individual does not need to have access to special resources, such as specialised knowledge, advanced tools or complex schemes. Therefore, a financier of terrorism does not need to be an individual with special abilities; however, international contacts are considered to be an important factor if

[34] The Swedish Police Authority: Financial Intelligence Unit of Sweden's annual report (2019), p 14. Found here: polisen.se/om-polisen/polisens-arbete/finanspolisen/ (retrieved 26/01/2021).

[35] The Swedish Police Authority: Financial Intelligence Unit of Sweden's Annual Report 2019, p 14.

the money is to ultimately reach the intended recipient. By using several collection methods and intermediaries, both in Sweden and abroad, the financier's ability to go undetected increases.

Communication through social media and the use of digital banking and money transfer services facilitates the collection and transfer of money. Actors suspected of terrorism by the Swedish Security Service use and attempt to exploit public funds to finance their activities.

3.3 Collection process

Money that is suspected of being used to finance terrorist activities often comes from a variety of sources. This money might be income through gainful employment, public grants for private individuals/organisations or business activities and the sale of goods, services, property or companies. Capital from these sources can be acquired legally or illegally, and in a number of cases, both. These actors can collect money from a variety of sources, only a portion of which is intended to finance terrorism. In recent years, individuals have also used funds from loans and lines of credit that have not been repaid.

Funds are also collected through charitable donations. The donations take place, for example, through individuals or organisations that carry out fund-raising campaigns where they publicly or secretly encourage people to donate money. In some cases, it is clear to the donors that the money is intended to finance a terrorist organisation, while in other cases; donations are requested under the guise of providing support in a crisis situation or conflict region.

Methods used to collect funds include depositing money in accounts held by private individuals, associations, foundations and companies. In some cases, deposits are made through mobile payment solutions. The Swedish Security Service have also noted that some actors openly state that they are collecting money for terrorist organisations, but they actually put the money in their own pockets and no financing of terrorism takes place.

In addition, it is also suspected that there are Swedish actors living in Sweden who work for terrorist organisations that are active abroad. The actors actively collect funds from the larger community, but also recover money from individuals and business people who, for fear of reprisals, may feel forced to give money. These activities can be likened to an illegal tax collection, extortion and protection racket.

3.4 Procedure for transferring money

When money is to be transferred from Sweden to terrorist organisations abroad, legitimate businesses that are subject to an authorisation obligation are exploited for illegal purposes. These businesses are mainly banking and credit institutions, as well as payment service providers and issuers of electronic money. Money is also sometimes transferred by individuals and groups who do not have authorisation in accordance with the Payment Services Directive (2010:751), so-called unregistered payment service providers.

These actors include Hawaladars, which provide an informal way to send money based entirely on trust, independent of the international financial system. Hawaladars can apply for permission to act as a money intermediaries and currency exchange agents and be granted authorisation from the Swedish Financial Supervisory Authority if the business meets certain requirements. It can be stated here that the use of traditional Hawalas is a challenge in itself for Swedish authorities, as it can be difficult to know how much of a Hawala's activities are legitimate and how much are criminal.

As the Swedish Defence Research Agency (FOI) states in 2020 analysis, it is also known that the strict regulation of Hawalas entails large costs and risks, as the money transferred often serves an actual humanitarian need in a number of vulnerable countries.[36] Increased anti-terrorism legislation, particularly regulation in the US banking and finance sector, has led several banks with broad reach and cross-border products and services to restrict the ability to transfer money through Hawalas, regardless of whether the funds represent a legitimate or illegal transfer. This has had a significant impact on the international stage and has also affected customers and actors in Sweden.[37]

Parts of the Swedish non-profit/NGO sector also confirm this problem. Due to stricter regulations in the effort to combat money laundering and the financing of terrorism, several humanitarian organisations have been impacted, as a number of banking and financial institutions have adopted more restrictive policies on the transfer of funds to high-risk countries.[38] This has already meant that Swedish actors who want to transfer funds are forced to seek out unscrupulous actors and alternative payment intermediaries, a problem that is likely to continue. The negative consequences of the new regulations may be unintentional, but they can sometimes have a significant impact. Several examples from the non-profit sector include closed accounts, extensive documentation requirements to prove the origin of money, and problems regarding the purpose of the transfer (correspondent banks abroad).

Courier operations are another way to transfer money to terrorist organisations and involve the physical transport of cash across borders. This is generally done through intermediaries in other countries that are suspected of working for terrorist organisations in the Middle East.

3.5 Financing of terrorism – organised crime and convictions

Individuals suspected of financing terrorism are often engaged in other criminal activities. It is then suspected that the criminal proceeds are intended, exclusively or in combination with other capital, to finance terrorist activities.

Several analyses have found that the financing of terrorism often overlaps with

---

[36] The Swedish Defence Research Agency (FOI), Anders Strindberg: *Hawala: An overview of the challenge from a terrorist financing perspective* (09/11/2020).

[37] Ibid.

[38] Workshop with Sweden's fund-raising organisations: *Exchange of knowledge on money laundering and terrorist financing* (21/10/2020).

other financial crime and organised crime. Tax offences, accounting crimes, theft, benefits fraud, drug-related offences, smuggling and illegal trade in tobacco and other goods are all examples of offences that can finance terrorism. The purchases of goods and services with black money can therefore have far greater consequences than the buyer anticipates. In much the same way, the increase in labour exploitation in recent years and the prevalence of labour migration may contribute to the financing of terrorism and other particularly serious crimes. The overlap with other criminal activities also affects the number of judgements in this area.

To date, Sweden has had few convictions for the financing of terrorism. The lack of convictions can be explained in a number of ways; for example, there are challenges regarding the evaluation of evidence and what the legislation requires. It is also possible that there is a greater focus on prevention than prosecution. An analysis completed by the Swedish Defence Research Agency (FOI) found that the low number of convictions is a result of the fact that Swedish authorities – similar to several equivalent authorities in Europe – ultimately prosecuted individuals for other crimes.[39] However, there were two important convictions during the period assessed here. One judgement was handed down by the Supreme Court in 2019 against a male perpetrator. He was convicted for using his Facebook account to encourage people to transfer money to Jabhat al-Nusra, the Islamic State and Ahrar al-Sham for the purchase of weapons.[40] In the second case, the Svea Court of Appeal convicted three people for sending money to IS.[41]

3.6 Financing of terrorism from a Europe-wide perspective

A recent assessment estimated that almost 1,191 individuals have been convicted of terrorist offences in the EU during the period 2015–2018.[42] Of these 56 convictions, about 5 percent of the individuals were prosecuted for financing of terrorism classified as a primary or secondary offence. In addition, about 100 individuals have been prosecuted in various legal cases where financing of terrorism has occurred but where other criminal classifications have been applied.

According to Europol, funds that are generated in Europe can leave the EU in a variety of ways.[43] Common modes of transfer are the Hawala banking system, corporate structures and commercial transactions, as well as various forms of money transfers (remittances). Europol contends that cash transfers, money services and Hawalas are often used in combination, particularly to distribute money among the Hawala intermediaries involved.[44]

---

[39] The Swedish Defence Research Agency (FOI), Michael Johnsson: *The effectiveness of EU action against terrorist financing 2010–2019. High costs, difficult-to-measure results* (09/11/2020).

[40] See Supreme Court, Judgement B5948-17 (13/11/2019).

[41] See Svea Court of Appeal, Judgement B3392-19 (12/06/2019).

[42] The Swedish Defence Research Agency (FOI), Michael Johnsson: *The effectiveness of EU action against terrorist financing 2010–2019. High costs, difficult-to-measure results.* (09/11/20200).

[43] European Union terrorism situation and trend report (TE-SAT) 2020 p 24. www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020

[44] Ibid.

Furthermore, Europol notes that individual terrorists and small cells, as well as individuals who travel abroad to participate in terrorist organisations, often finance their own activities through legitimate income or through fraud and petty crime. The financing of larger groups and terrorist organisations with a hierarchical structure differs significantly from the financing of terrorist attacks and activities committed by individual actors or small groups.[45]

Experience from Europe shows that terrorist organisations need access to financial resources for the preparation and execution of terrorist attacks, but also to maintain their infrastructure, recruitment, propaganda and operational capacity. Operational capacity can relate to training, indoctrination, salaries, financial compensation for family members and logistics.[46] These acts of financing seldom constitute a punishable offence, and the largest proportion of the funding is likely to go to the activities described above. In the experience of the Swedish Security Service the conclusions reached in other European countries also apply to Sweden.

3.7 Overall

Money laundering is about concealing the origin of money, while terrorist financing aims to hide the ultimate purpose of the assets. Terrorism can often be financed with small amounts of money, and these funds may be obtained legally or illegally. The collection and transfer of the assets can take place quickly, easily and at a minimal cost. Actors do not need to have any type of expertise, but international contacts are an important factor if the funds are to reach the intended recipient.

Funds can be collected in a variety of ways, including through charitable donations. Methods used to collect funds include depositing money in accounts held by private individuals, associations, foundations and companies, and funds can be sent through payment intermediaries. Money transfers may take place through registered payment service providers, through payment services provided by authorised or registered institutions such as banks, credit institutions and payment service providers, as well as through unregistered money transfer agents that are not under the scrutiny of supervisory authorities, such as hawaladars.

[45] Ibid p. 22.
[46] Ibid.

4 Risk analysis and impact assessment

This chapter presents a risk assessment in relation to money laundering and terrorist financing within the scope of the application of the Money Laundering and the Financing of Terrorism (Prevention) Act (PTL). First, a risk analysis is presented based on an assessment of existing threats and vulnerabilities for each sector (Chapter 7). The potential consequences of money laundering or terrorist financing are then analysed and ranked. The main observations presented in the chapter are:

- **High-risk sectors.** Gambling, trading in goods and exchange service providers are examples of sectors with a high risk of money laundering. This also includes company formation agents, business brokers and trust administrators.
- **High threat level in banking.** Banking is the sector where money laundering has the potential to have the most severe consequences at a national level. Banks have taken comprehensive measures to reduce the risks, but the threat level remains high, as almost all money laundering goes through the banking system at some stage.
- **Confidence in the economic and legal system.** Complex, large-scale money laundering schemes can involve services delivered by auditing/accounting firms, individual auditors and advocates. Through the exploitation these businesses, money laundering can have a significant impact on the level of confidence in the economic and legal system.
- **Facilitators.** Real estate agents and independent lawyers are among the operators who may be exploited as facilitators for money laundering, which can have negative effects across society.
- **Relevant to the financing of terrorism.** The sectors that have been assessed as relevant for terrorist financing are the banking sector, payment institutions, payment service providers, consumer credit, other financial services (virtual currencies), issuers of electronic money, exchange service providers and gambling companies.

4.1 Risk per sector based on a threat and vulnerability assessment

Presented here is an analysis of the threats and vulnerabilities within the individual supervisory areas under the Anti-Money Laundering Act. The results are particularly relevant for operators and supervisory authorities, but also for other actors in the Swedish anti-money laundering regime, as different actors need to work together to reduce the risk levels.

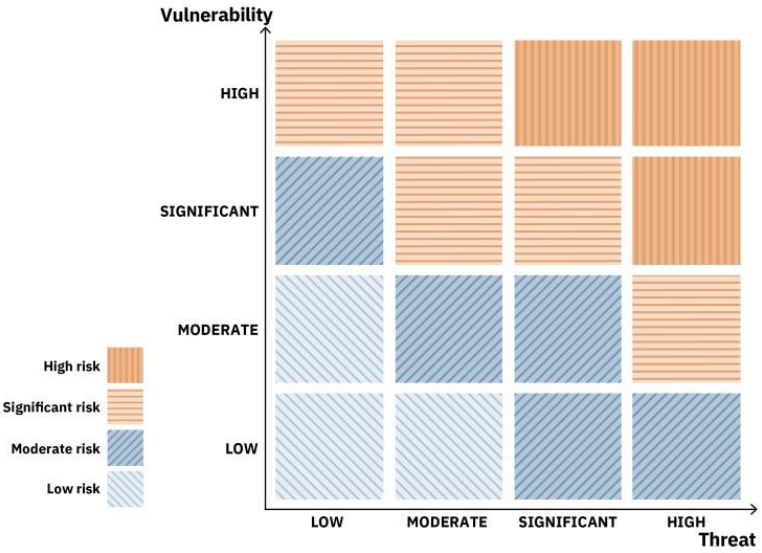
The analysis is based on date collected for the years 2018–2019 for the sectors that were under the scope of the Anti-Money Laundering and the Financing of Terrorism (Prevention) Act (PTL) during the period.[47] The risk of money laundering

[47] The threat and vulnerability assessments are weighed to create a risk level as illustrated in the matrix above. See appendix Process and Method for a more detailed description.

has been quantified, while the risk of terrorism financing is described in qualitative terms for the sectors where it has been assessed to be relevant.

4.1.1 Quantitative sector analysis of the risk of money laundering

Table 4.1 shows the results of a threat and vulnerability analysis in relation to money laundering and the risk in each sector. The assessment has resulted in a four-tiered scale with the levels low (1), moderate (2), significant (3) and high (4).[48] The results are based on the matrix shown beside the table.



Each sector has been assessed in terms of both threats and vulnerabilities in relation to money laundering. A sector is exposed to threats by actors who want to exploit it for money laundering. Vulnerability is a deficit in the sector in terms of the ability of operators to prevent money laundering. The combination of these two factors determines the overall risk level for the sector. This means, for example, that a high threat profile can be mitigated by low vulnerability, or that a lower threat profile can still be considered problematic if the level of vulnerability is high.

As shown in Table 4.1, there are wide differences in risk levels. However, none of the sectors in the table are assessed at the lowest risk level. *Level 1* indicates that criminals do not use the sector for money laundering (threat) or that there is a negligible risk of money laundering due to effective barriers and control systems (vulnerability). The different sectors have been defined based on the wording in the relevant paragraph in the legislation. The division of sectors should thus not be interpreted as "industries", but according to the type of authorisation or registration a certain operator holds. For example, banks may offer services that are also included in other financial sectors, such as payment intermediation, housing loans and fund management. In that case, however, the overlapping services are still included in the banking sector. The division of sectors is described in more detail in the sector catalogue (see Chapter 7).[49]

[48] The assessment scale is defined in more detail in the appendix Process and Method. The Process and Method section also describes how the threat and vulnerability assessments are weighed to create a risk level (where vulnerabilities are weighted more heavily than threats).

[49] The sector catalogue provides a more detailed picture of threats and vulnerabilities as well as potential approaches to address these. It also outlines the risks of terrorist financing for the sectors where it is deemed to be relevant.

TABLE 4.1

Results of the sector analysis in relation to the risk of money laundering for the years 2018–2019			
Sectors under the supervision of the Swedish Financial Supervisory Authority	**Threat**	**Vulnerability**	**Risk**
Financial institutions*	4	3	4
Banking or financing activities	4	2	3
Payment institutions	3	3	3
Registered payment service providers	3	3	3
Issuers of e-money	3	3	3
Fund management	3	2	2
Securities market	3	2	2
Mortgage business	2	2	2
Consumer credit activities	2	2	2
Insurance brokers	2	2	2
Life insurance business	2	2	2
Sectors under the county administrative boards	**Threat**	**Vulnerability**	**Risk**
Retail goods	4	4	4
Company formation agents and business brokers	4	3	4
Trust administrators	4	3	4
Independent lawyers	3	3	3
Business centres and postbox service companies	3	3	3
Accounting or auditing services (not approved or authorised auditor or registered auditing firm)	3	3	3
Tax Consultants	2	3	3
Pawnbrokers	2	2	2
Sectors with their own supervisory bodies	**Threat**	**Vulnerability**	**Risk**
Gambling companies	4	3	4
Real estate agents	3	3	3
Auditors	3	2	2
Advocates	2	2	2

* Compare to Section 1 of the Act on Currency Exchange and Other Financial Activity, where currency exchange and other financial activities are defined as two different types of activities. The common definition is *financial institutions*.

4.1.2 High threat level for banks and financial institutions

Among the activities that are under the supervision of Swedish Financial Supervisory Authority, the threat level is deemed to be highest for banks and financial institutions. Banks represent the fundamental financial infrastructure of the country, and more or less all laundered money needs to pass through the banking system at some stage. The financial institution sector is also highly vulnerable to the risk of exploitation, particularly exchange service providers and the large-scale, unregistered trade in virtual currencies. For example, the illegal drug trade in Sweden, which is considered an importing country, relies on the ability to exchange profits for other currencies in order to be transferred abroad and reinvested in new supply.[50] Virtual currencies are a prerequisite for the illegal drug

[50] Since 1 January 2020, trading in virtual currencies is subject to a registration requirement in accordance with LVA. As discussed in the method section, the scope of this report is limited to the years 2018–2019. At the time, this activity was not regulated in the law.

trade on the Darknet and are used to launder criminally acquired funds.[51]

In response to the high threat level, banks have established extensive routines and monitoring systems to combat money laundering, while smaller financial players are generally less equipped to deal with the threat. The risk level in the banking sector is therefore considered to be *significant* and lower than the level in financial institutions, where the risk is classified as *high*.

The risk level for payment institutions, payment service providers and electronic money issuers is classified as *significant*. The threat level is deemed to be lower compared to financial institutions, but the services banks provide are attractive to those seeking to launder money. When it comes to e-money, risks arise mainly when foreign suppliers offer services on the Swedish market. This can relate to foreign accounts or prepaid anonymous cards, which are money laundering tools that are very easy to acquire.

In terms of payment service providers, there is a general trend towards more integrated business models. In addition to payment intermediation, other services are also offered, such the exchange between fiat money and virtual currencies. This means that the companies active in the sector increase their risk exposure in relation to other sectors, such as financial institutions, which are considered to be at a *high* risk level.

Fund management and the securities market can be attractive for money laundering, as transactions involving large sums of money do occur and may not arouse suspicion. However, as it takes a relatively long time to conclude a transaction, the risk is deemed to be *moderate*, the second lowest level. The mortgage and consumer loan, insurance brokers and life insurance sectors are also assessed as *moderate* in terms of risk.

4.1.3 There is a high risk that the trade in goods sector will be exploited for money laundering

The county administrative boards' supervisory assignments cover a number of sectors within areas of activity with a wide degree of variation. Among these areas of activity, trade in goods is considered to have the highest level of threats and vulnerabilities. The cash purchase of luxury goods provides criminal actors with anonymity up to a certain amount limit and does not require specialised knowledge. At the same time, risk awareness and knowledge of the Anti-Money Laundering Act are generally assessed as low among the operators in the sector. The risk in the trade in goods sector is therefore classified as *high*.

The risk of money laundering for company formation agents, business brokers and trust administrators is also assessed as *high.* The risk for trust administrators primarily relates to the high opportunity to remain anonymous, in combination with the limited information the supervisory authorities have about the operators in Sweden.[52] With regard to company formation agents and business brokers, the

[51] The darknet is a part of the internet that often requires special software to access the websites.

[52] Trusts are a legal structure that is not covered under Swedish law, but there may be foreign trusts with administrators or beneficiaries residing in Sweden. Foreign trusts can also own assets in Sweden, regardless of where the beneficiary or administrator is located.

services they provide are considered to be of interest to actors in more advanced money laundering schemes. Over the long term, the companies that threat actors gain access can facilitate large transactions.

Business centres and postbox service companies can be important pieces of the puzzle in a money laundering scheme by offering business addresses that appear to be legitimate. One difficulty encountered by operators, supervisory authorities and law enforcement agencies is determining who is actually using an address. This is a vulnerability that contributes to the risk of money laundering in the sector being assessed as *significant*. In more advanced, large-scale schemes, this sector usually plays an important role.

Activities assessed at the *significant* risk include independent lawyers, tax consultants and businesses that offer accounting and auditing services. What these types of activities have in common is that they can be exploited in a variety of ways to legitimise a scheme, even if they are not directly involved in the transactions. Actors with legal representatives are often perceived to have a higher degree of legitimacy, and can be considered to have already been subject to customer due diligence measures. This, in turn, can lead to decreased vigilance in other sectors, thus reducing the chance that a money laundering scheme will be detected in other parts of the chain.

Due to the high rate of cash used in the sector, pawnbrokers can be exploited by criminals to launder criminal profits. But the pawned asset can also be acquired through criminal activities. Compared with the trade in goods sector, risk awareness and knowledge of the Anti-Money Laundering Act are considered to be relatively good in the sector. The risk in the sector is therefore assessed as *moderate*.

4.1.4 *Gambling – a high-risk sector*

Gambling companies and real estate agents are also at risk of being exploited for money laundering, which can go unnoticed by the businesses themselves and the banks. From the banks' perspective, a payment received from these sectors can appear to be legitimate, for example, a gambling win or a down payment for a real estate transaction. The operators' own access to information about the transactions is often limited, which makes it difficult to evaluate the origin of the money. The gambling market is considered to have the highest threat level due to its broad accessibility and the ability to turn over relatively large amounts of money in a short period of time. The real estate sector is also attractive but is likely to be used to a lesser extent. The risk in the sector is therefore assessed as *significant*.

4.1.5 *Facilitators*

Auditors and advocates can be used as facilitators, as their services can lend a seal of approval to financial statements or transactions that are part of a business scheme. This means that the sectors can be used as a means to give otherwise suspicious schemes an appearance of legitimacy. However, operators in these sectors generally take thorough customer due diligence measures, which reduces

vulnerability. The risk of these sectors being exploited for money laundering has been assessed as *moderate*.

4.1.6 Sector assessment of terrorist financing

Banks, payment institutions and payment service providers are the sectors where terrorist financing is believed to occur to the greatest extent. This is mainly due to the large scale and broad accessibility in the sectors, but also because the services provided in the sectors are suited to the purpose.

The key risk for sectors that may be exploited for terrorist financing is assessed based on the same factors as for money laundering. The same conditions apply to control mechanisms within each sector; however, the knowledge of terrorist financing schemes is generally lower, which affects the likelihood of detection and the accuracy of the reporting. The fact that the vast majority of transactions are handled in the banking sector at some stage, also factors into the risk of terrorist financing. The ability to detect terrorist financing is further complicated by the difficulty identifying unique risk indicators.

It is also assessed that terrorist financing can occur through issuers of electronic money and consumer credit, but to a lesser extent compared with the sectors indicated above. The services offered in these sectors are attractive to those seeking to carry out activities related to terrorist financing, but the level of exploitation is less extensive due to the size of the sectors relative to the sector that includes banks, payment institutions and payment service providers. A certain degree of knowledge is also required to be able to use the services of foreign issuers of e-money. Knowledge and capacity are also required for criminals to be able to exploit the lending system. But even if the consumer credit sector, banking sector (unsecured loans) and financing sector are exploited to a small extent, individual cases can have significant consequences, as even relatively small amounts of money are enough to do a great deal of damage.

The financing of terrorism is deemed to occur in the Swedish gambling market and in financial institutions through the use of exchange service providers and the extensive, unregulated trade in digital currencies. However, it is difficult to estimate to what extent this occurs.

The knowledge that digital currencies are used to finance terrorist activities has been gained from intelligence information and in reporting to the Financial Intelligence Unit of Sweden (Fipo). It is not believed that the use of digital currencies for these purposes is widespread, but the actual extent is difficult to assess. The fact that digital currencies are well suited for withdrawing money anonymously suggests that this channel is likely to be used.

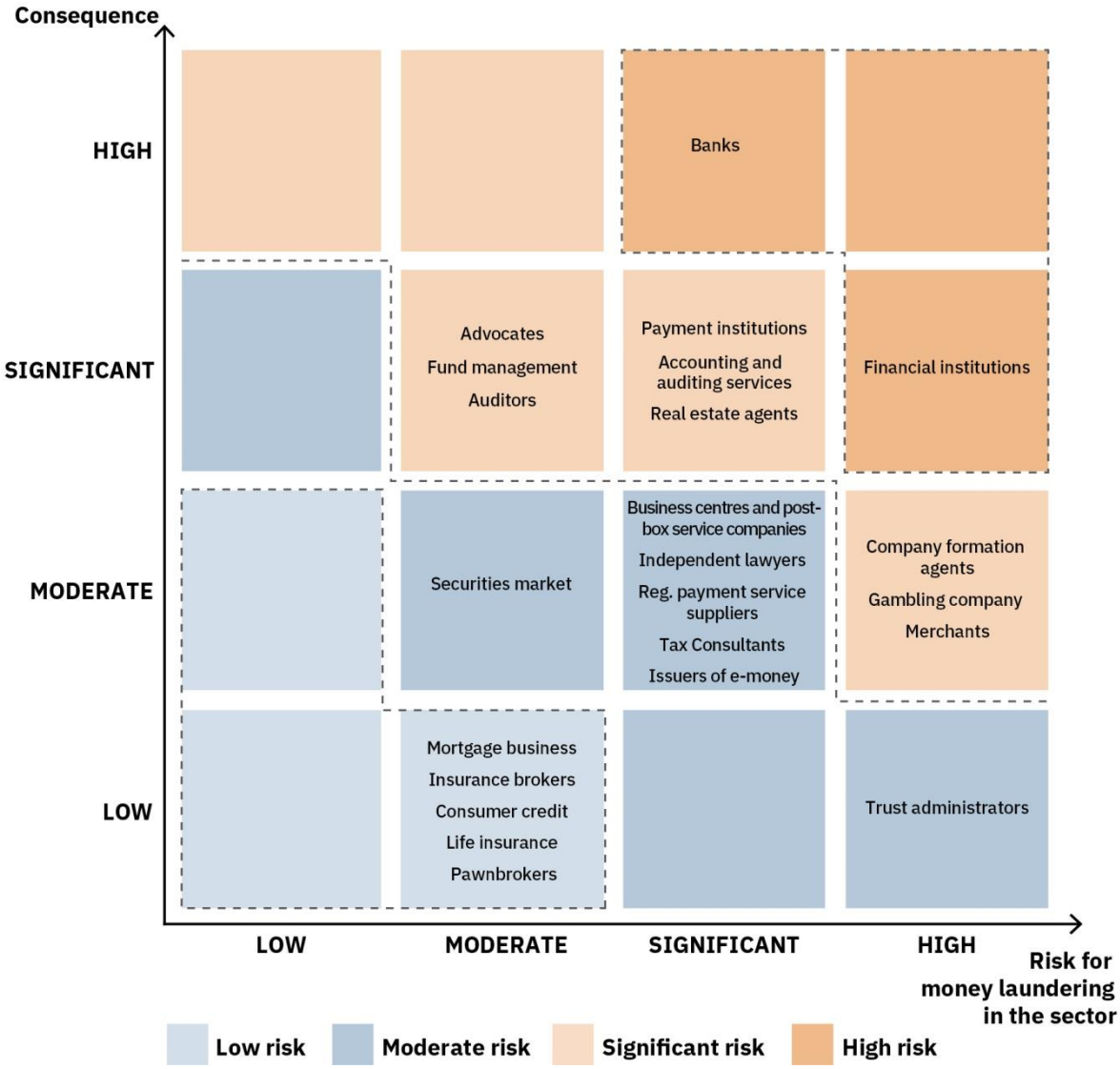
The Swedish gambling market is also relevant in this context, namely due to the possibility of foreign transactions and anonymity, for example, through the use of strawmen. There is intelligence information that gambling accounts are used by actors engaged in the financing of terrorism, but the extent of this cannot be assessed here either.

4.2 Consequences of money laundering from a national perspective

In order to be able to create a national threat and vulnerability profile, the analysis has been supplemented with an assessment of the consequences money laundering in each sector can have on society. This section describes how the risks in the different sectors contribute to the national risk profile. Just because a sector's risk is assessed as high, does not necessarily mean it has a major impact from a national perspective.

The impact assessment is based on the sector's size and the role the sector can play in large-scale money laundering schemes. The assessment also accounts for the impact money laundering can have on society in general. For example, this may apply to the impact on financial stability, confidence in the economic and legal system or the impact on market prices. Matrix 4.1 illustrates how the different sectors contribute to the national risk profile. In this assessment, the risk presented by money laundering in the individual sectors is evaluated in relation to the potential consequences if money laundering does occur in the sector (in no particular order within each box).

MATRIX 4.1
Consequences of money laundering at the national level (assessment of the years 2018–2019)



4.2.1 Money laundering through the banking sector may result in the most severe consequences

Banking is the sector where money laundering has the potential to have the most severe consequences. The Swedish banking sector is relatively large, not only compared with other sectors but also by international standards. The large volume of transactions and the fact that, in principle, all forms of money laundering pass through the banking sector at some stage, means that the risk is considered high from a national perspective. The exploitation of the sector for money laundering can potentially have a negative impact on confidence in the financial system and damage Sweden's reputation internationally.

Financial institutions are also assessed to be high risk at a national level. Although the potential negative societal effects are assessed to be significantly smaller compared to the exploitation of the banking sector, the risk of money

laundering has been classified as *high*.

Other financial activities are relatively less important for the national risk profile. Payment institutions and fund companies are the sectors that are assessed to contribute to the risk at the national level, which is considered significant. The potential consequences of exploitation are assessed to be more limited in scope for securities companies, payment service providers and issuers of e-money, and the sectors are therefore classified as *moderate* in the national risk profile.

The financial institutions where money laundering is assessed to have the least potential impact on a national level are insurance brokers and life insurance companies, as well as housing credit and consumer credit companies. It is worth noting that the majority of housing credit and consumer credit activities are provided by banks. The sectors noted here only include companies that fall under this specific category in the legislation, which also hold a relatively small market share in the issuance of such loans (see also the sector catalogue).

Risk in non-financial sectors. In the threat and vulnerability analysis (previous section), the trade in goods sector is identified as high-risk for money laundering. The sector is the only sector rated at the highest level for both threats and vulnerabilities. However, from a national perspective, the level of risk in the sector is only rated as *significant*. One important reason for this is that the use of cash in Sweden is among the lowest in the world, which limits aggregate risk. The likelihood of general, negative societal effects, if it is discovered that one or more operators have been exploited or contributed to money laundering, is also deemed to be low.

There are other activities outside the financial sector that affect national risk exposure. These sectors include gambling companies and real estate agents. These sectors have a relatively high turnover, and any occurrence of large-scale money laundering would have a noticeable impact on society. If real estate agents can be exploited as facilitators, criminals can realise the benefit of their criminally acquired funds by purchasing real property. Large-scale real estate purchases made with black money could also affect market pricing in an area. The occurrence of money laundering in the gambling sector is likely to have less of an impact on the country as a whole, but the risk is deemed to be higher that this could occur.

Accounting and auditing services, individual auditors and advocates are also deemed to be at a *significant* risk level in the weighted, national risk assessment. Despite extensive customer due diligence measures, money laundering can occur in a way that is difficult for operators to detect.[53] For example, operators may need knowledge of who their customers' customers are, or knowledge of who is ultimately behind complex and cross-border schemes.

In the event that large-scale money laundering occurs, the consequences are deemed to be significant. These sectors play a central role in the country's economic system, particularly in the prevention of financial crime. The occurrence of money laundering in these sectors therefore has the potential to damage confidence in the

[53] It should be noted here that operators who offer accounting and auditing services generally do not take thorough customer due diligence measures.

entire system, not just in individual operators or industries.

The risk of exploitation for money laundering for company formation agents and business brokers has been rated as high. However, the sector does not have the same level of importance for overall confidence in the system as, for example, auditors and advocates. Therefore, the potential consequences of money laundering are also considered to be less severe. The overall assessment is that money laundering in these sectors would have a *significant* impact on the national level.

4.2.2 Money laundering in smaller sectors has a limited national impact

Independent lawyers (jurist in Swedish) and tax consultants can be exploited in the same way as auditors and advocates, that is, to lend legitimacy to transactions and business schemes. The sector can also be exploited by facilitators, but the consequences of this are deemed to be less severe. This is partly due to the fact that the customers' turnover is often lower in the sector, and partly due to the fact that independent lawyers and tax consultants do not have the same essential role in the financial and legal system. From a national perspective, these sectors are therefore assessed as *moderate*, despite the fact that the risk that the sectors will be exploited for money laundering is significant.

Business centres and postbox service companies are considered to have the same level of risk. These services can function as links in a money laundering chain by offering business addresses that appear to be legitimate. The risk of money laundering for these businesses is also considered to be significant but given the fact that the sector is relatively small, the potential consequences are deemed to be limited.

The risk of trusts being exploited for money laundering is classified as *high,* but since a trust is not a legal structure supported under Swedish law, the potential consequences of money laundering are considered to be limited. The sector is therefore only classified as a *moderate* risk in the national profile.

The small number of pawnbrokers and low transaction amounts mean that the sector is not attractive for money laundering to any great extent. The potential consequences of money laundering are therefore considered to be relatively small nationally, and pawnbrokers' activities are deemed to have a *low* risk in the overall risk profile. The same applies to sectors such as insurance brokers, life insurance companies and housing and consumer credit companies.

4.3 Consequences of terrorist financing from a Europe-wide perspective

In examining terrorist financing, the same principles apply to the impact assessment as for money laundering, even though the risks have not been assigned a *quantified* level. There are some important differences that affect the overall assessment. In terms of the scale, the financing of terrorism is relatively insignificant in relation to money laundering. Therefore, it does not pose the same threat to the economic system as money laundering. On the other hand, the financing of terrorism has the potential to damage confidence in the financial

system and impact Sweden's reputation internationally, and the ultimate consequence of undetected terrorist financing is a terrorist attack.

Banking is also the sector where the impact of terrorist financing is deemed to be greatest. Terrorist financing is less widespread than money laundering, but it still has the potential to damage confidence in the Swedish financial sector, both within Sweden and outside the country's borders. Furthermore, financial institutions are also assessed to have a widespread risk at the national level. Although the potential negative societal effects are assessed to be significantly smaller compared to the exploitation of the banking sector, the risk of money laundering has been classified as *high*. Given that the true extent of terrorist financing is difficult to assess, the impact assessment will also reflect this uncertainty. But given that large sums of money can be handled quickly and anonymously, across national borders, through trading in virtual currencies, the financing of terrorism can have significant consequences on a national level.

Furthermore, the potential consequences are deemed to be more severe in the sector compared with money laundering in cases where payment institutions, payment service providers and issuers of electronic money are used to finance terrorist activities. One reason for this is that even when a small amount of money is transferred to another country, it can have a tremendous impact on the financing of terrorism.

5 Other risks

This chapter describes the risks that have been identified during the risk assessment that are in need of particular attention. The risks presented here include schemes that often tend to extend across several individual sectors that fall under the scope of the Money Laundering and the Financing of Terrorism (Prevention) Act (PTL), which can be difficult to identify for operators in the individual sectors. Special attention is given to activities that fall outside the scope of the Act, risks that are linked to legal entities and challenges that are linked to foundations in Sweden. In addition, this chapter also highlights the potential negative consequences for parts of the non-profit sector as a result of an operators' overly strict interpretation of the money laundering regulations. The main observations presented in the chapter are:

- **Complex schemes:** The 2019 risk assessment highlighted the problems presented by complex money laundering schemes. This remains a problem. Operators in these sectors find it difficult to detect systematic or organised schemes where a legal entity is used as a tool for criminal purposes in multiple sectors or to exploit several different operators.[54]
- **Sectors that is overlooked.** There are sectors that are not currently covered by the Anti-Money Laundering Act, despite the fact that the activities carried out in these sectors are largely similar to activities covered by the Act. For example, cash purchases of goods over EUR 5,000 are covered by the Anti-Money Laundering Act, but not cash purchases of services.
- **False identities.** Limited companies and other legal entities are used as tools in a variety of criminal schemes that include, for example, money laundering, where the company representatives often use hijacked, false or misused identities.
- **Foundations.** Foundations are used as tools for criminal activities and as a part of money laundering and terrorist financing schemes. Relevant, up-to-date information is not easily accessible, which complicates the work of law enforcement.
- **The fund-raising sector.** There are areas covered under the scope of the Anti-Money Laundering Act (e.g. the fund-raising sector), where the strict interpretation of regulations on suspicious transactions have had negative consequences for individual actors, despite the fact that these actors were carrying out activities for legitimate purposes.

5.1 Complex schemes

The starting point for the report is a risk assessment of the individual sectors. At the same time, it is common for crimes to span across several sectors. This means

[54] The issue of complex schemes was also raised in the previous national money laundering risk assessment.

that there is a risk that operators who only see part of a scheme will not detect the larger money laundering scheme. Similarly, crimes can also span across several operators in one and the same sector.

For example, individual operators may have difficulty detecting systematic or highly organised schemes in which a legal entity is used as a criminal tool in several different sectors or where several different operators are exploited.[55] The same applies to schemes where hijacked, false or misused identities are systematically used, which may be difficult for individual operators to detect.[56]

Much the same way that legal entities are exploited for the purposes of money laundering, they are also knowingly used in terrorist financing schemes, though without being a direct link in a transaction chain. These may be legitimate companies, foundations and economic associations that support a radicalisation activity or an activity that does not immediately form the basis for financing terrorism but does so over the long term. The operators' level of knowledge therefore needs to be improved so that they are better equipped to detect more complex cross-sector criminal schemes. An important piece of the puzzle here may be to involve more authorities to enable suspicious money laundering schemes to be detected more often.

Legal entities that are systematically used as tools to facilitate criminal activities can be detected through the control activities of various authorities (e.g. the Swedish Companies Registration Office and the Swedish Tax Agency). For example, by creating a clearer focus in the authorities' appropriation directions in terms of how to effectively combat complex money laundering schemes, the efforts of the Swedish regime will likely become more effective.

5.2 Activities not covered under the scope of the Anti-Money Laundering Act

The division of businesses into sectors in the Anti-Money Laundering Act clearly stipulates which operators are subject to the provisions of the act.[57][58] Given this distinct division, there are several activities that fall outside the scope of the law, and thus also this risk assessment. Operators in sectors that fall outside the scope of Anti-Money Laundering Act have no obligation to take customer due diligence

[55] Companies and other legal entities are often used as tools in various types of crime, including money laundering. See, e.g. the Swedish National Council for Crime Prevention (Brå): Administrative measures against financial and organized crime Part 1: Authorisation to conduct operations (2015:15) and the Swedish National Council for Crime Prevention (Brå): Criminal infiltration of companies (2016:10).

[56] Compare to the discussion within the EU for a comprehensive European supervisory authority: www.eba.europa.eu/eba-calls-eu-commission-establish-single-rulebook-fighting-money-laundering-and-terrorist-financing (retrieved 19/01/2021).

[57] Advocates and independent lawyers are only covered under the scope of the Anti-Money Laundering Act with respect to certain specific legal services.

[58] Any operator in a sector regulated in the Anti-Money Laundering Act must report this to the responsible supervisory authority, and if required, obtain authorisation. Sectors under the supervision of the county administrative boards must independently register with the Swedish Companies Registration Office's anti-money laundering register (this applies to all sectors under the supervision of the county administrative boards except the Pawnbroker sector, wherein operators may only conduct activities after receiving a permit from the county administrative boards).

measures or report suspected money laundering or terrorist financing. However, some of these actors are likely to have access to information that would allow them to detect suspicious transactions or activities. These include electronic ID services, electronic transfer services and giro payment services, trade in cryptocurrencies and certain activities in the fintech sector. Additionally, cash trading in services is not covered under the scope of the Anti-Money Laundering Act, despite the fact that the conditions do not differ significantly compared with cash trading in goods, which is covered under the Act. See additional information in Chapter 6, risk-mitigation measures.

5.3 Foundations

Another risk area that presents a special challenge in Sweden is foundation activities. Foundations are not covered under the Anti-Money Laundering Act in their capacity as a legal entity, but can, on the other hand, be covered if they conduct activities in one of the sectors under the scope of the Act. However, few foundations conduct the type of activities that fall under the scope of the Anti-Money Laundering Act. On the other hand, foundations that conduct fund-raising for certain purposes are covered by the so-called right to request information (Chapter 4, Section 6 of the Anti-Money Laundering Act).[59] This entails an obligation to provide all information needed at the request of the Swedish Police Authority or the Swedish Security Service. The reason is that fund-raising activities are vulnerable to exploitation for the purpose of financing terrorism.

Law enforcement agencies have emphasised that foundations are used as a tool for criminal activities and as a part of money laundering and terrorist financing schemes. One of the challenges faced by law enforcement agencies is therefore to be able to quickly and easily obtain relevant and up-to-date information about foundations and their representatives.

The county administrative boards are responsible for registration of foundations at the regional level within their areas of supervision. However, registration in the county administrative boards' registers does not mean that a foundation gains legal capacity; foundations already gain legal capacity at the time of formation. This is also reflected in the foundation register, which is in no way constitutive. The scope of the register is limited and does not contain the foundations' documents, date of formation, date of entry and exit of the board members and annual reports made by the company register.[60] The fact that the register is not comprehensive in nature and does not definitively establish the responsible parties, may also mean poorer compliance in reporting changes to the register. The inconsistent ability to access relevant, up-to-date information on foundations, in turn, complicates the work of law enforcement agencies.

There is also a risk that foundations can be used as a tool for criminal activities

[59] Fund-raising foundations are obliged to register, but many fail to do so without consequences.
[60] However, the information is available from the county administrative boards even if it is not included in the material sent for registration.

in cases where other association forms offer less opportunities for anonymity and are subject to stricter regulations. for example, Chapter 9, Section 42 of the Swedish Companies Act (2005:551) stipulates that in the event of suspicion of a crime, a company auditor shall report this to a prosecutor and notify the company board. No corresponding provisions are found in the Foundation Act. Risks associated with foundations can be reduced through increased knowledge and the more efficient exchange of information between relevant authorities.

5.4 The fund-raising sector and the non-profit sector

In addition to the areas that fall under the scope of the Anti-Money Laundering Act, there are several other areas that can potentially be exposed to money laundering and terrorist financing that have not been included in the sector assessment. The FATF's observations at the international level show that the fund-raising sector often attracts criminal actors, both for the purposes of money laundering and terrorist financing. Organisations may or may not be aware that they are being exploited for these purposes. There is also evidence from Sweden which indicates that Swedish fund-raising organisations may be vulnerable, especially for the financing of terrorism (see, e.g. section 3.3).

There are also challenges associated with fund-raising organisations that have received increasing attention in recent years. A number of fund-raising organisations in Sweden and Europe encounter a certain degree of suspicion when they need to transfer money to high-risk countries. Despite having thorough documentation, organisations have sometimes come under suspicion of dealing in illicit funds. There are frequent examples of organisations that have had bank accounts closed when the banks found that they could not properly account for the intended purpose of the funds in the recipient country, despite the fact that the organisations themselves have placed stringent demands on their own operations. This presents a challenge that could steer organisations away from established transmission channels towards other high-risk channels.

In addition to the difficulties several fund-raising organisations have encountered at the national level, representatives of the fund-raising sector also contend that there are challenges with the correspondent banks. While some banks green light transfers from these organisations, transfers are sometimes halted by other correspondent banks, where the requirements to provide information about, for example, the origin and purpose of money are even higher.

Additionally, it has emerged during the risk assessment that some fund-raising organisations have proposed a code of conduct for established and trusted organisations so that it is easier to transfer money to fund activities in, for example, high-risk countries. In addition to a clearer insight into the origin of money, more and more fund-raising organisations are looking for clearer guidance on the responsibility to report where the money goes. some members of the non-profit sector are also requesting a dialogue with the relevant authorities so they can carry out their activities in a way that better manages risk. It should be noted that it is not only fund-raising organisations that are affected by the problems described

above. Gambling companies and payment service providers are other actors engaged in activities where banks sometimes choose to terminate individual customer relationships if they assess that they are generally associated with high risk.

5.5 Private–public collaboration

In order to be able to respond to new risks and, for example, increase reporting to the Financial Intelligence Unit of Sweden (Fipo), proactive strategies are needed in collaboration between the public and private sectors. Since the operators have insight into new risks and criminal strategies, this creates the foundation for a better, risk-based approach and thus an improved ability to detect suspected money laundering and terrorist financing.

In order to strengthen public–private cooperation, information must be shared within the Swedish regime. Actors from within the regime need to share both operational and strategic information; in the same way, private actors need to be vigilant and report information to relevant authorities. Several collaborations have emerged in recent years that have proven to be effective in this respect (e.g. SAMLIT).[61] Another potential approach is to create platforms where supervisory authorities and law enforcement agencies can participate in industry forums in order to increase knowledge of how operators in the various sectors conduct their business and carry out transactions. In order to improve the ability of operators to identify and report money laundering and the financing of terrorism, the operators have emphasised that supervisory authorities need to be transparent in their assessments. This can create increased predictability for operators so that they can live up to the expectations that are imposed on them.

5.6 Overall

Operators have a limited ability to detect, prevent and combat money laundering and terrorist financing, as money laundering schemes often involve several different sectors and operators. Some operators are subject to the reporting obligation in the Anti-Money Laundering Act, while actors who engage in similar activities are not subject to the reporting obligation. This poses a risk in the sector, and there is a special challenge in relation to legal entities in this context. As operators only have insight into their own activities, it is difficult to detect systematic or highly organised schemes where a legal entity is used as tool for criminal activities in several different sectors.

---

[61] Through the SAMLIT (Swedish Anti-Money Laundering Intelligence Task Force) initiative, the Swedish Police Authority is engaged in collaboration with Sweden's five largest banks: Danske Bank, Handelsbanken, Nordea, SEB and Swedbank. The Swedish Bankers' Association also participates in the initiative. Previously, information exchange took place between each individual bank and the Swedish Police Authority; through the Anti-Money Laundering Act, the police also have the right to request information. In order to strengthen anti-money laundering efforts, the participating banks are now meeting with the police's intelligence unit at the National Operations Department (NOA) to share information on, for example, new approaches used by criminals, types of crime or other patterns that might be able to be jointly identified.

Furthermore, the scope and content of the foundation register are limited. Knowledge about foundations within Sweden is also low. The inconsistent ability to access relevant, up-to-date information limits and complicates the work of law enforcement agencies.

Finally, there is also a need to examine how parts of civil society are affected by operators' “risk appetite”, as several organisations (e.g. fund-raising organisations) work directly with high-risk jurisdictions. This is an especially important step, as the non-profit sector serves an important function in a democratic society.
The fund-raising sector highlights a number of unintended consequences resulting from the strict application of regulations.

6 Risk mitigation measures

Sweden has good access to resources to prevent and combat the risks of money laundering and terrorist financing. The country has the knowledge, regulations, capacity and organisation in place or under development, something that has been confirmed on the international level. However, criminal actors are constantly seeking to develop new schemes, thus creating new conditions to facilitate criminal acts.

Further action is needed to address threats and reduce vulnerabilities. This risk assessment identifies and presents several risks of money laundering and terrorist financing that require further action. Below are eleven proposed risk mitigation measures based on the assessment:[62]

1. Confirm ultimate beneficial ownership

The 4th EU Money Laundering Directive requires member states to establish a register of data on the ultimate beneficial ownership (UBO) of legal entities. On 1 August 2017, the Act on the Registration of Beneficial Owners (unofficial translation of the Swedish title lagen om registrering av verkliga huvudmän) entered into force, and on 1 September of the same year, the Swedish Companies Registration Office started maintaining a register. The register aims to disclose which natural persons have controlling influence over companies and other legal entities. The register is also intended to reinforce the operators' obligation to take customer due diligence measures. The information collected in the register will make it more difficult to carry out money laundering and terrorist financing in Sweden.

Proposals:

In a number of reports, the Swedish Companies Registration Office has put forward proposals for changes to current legislation to further enhance the capacity to prevent crime.

- UBOs should therefore be reported when a company or legal entity is registered for the first time.
- Foreign natural persons should be required to verify their identity by enclosing a certified copy of a passport.
- Certain items in the legislation should be clarified to make it easier for both those registering and operators.
- It does not constitute a breach of confidentiality when operators, such as banks, are required to report incorrect information on UBOs in the register to the Swedish Companies Registration Office. Such a rule should be introduced so that notification can contain detailed information about what is incorrect in order to increase the quality of the register. The ability to impose a fine should be

[62] During the work to complete this risk assessment, additional risk-mitigation measures were identified that will be followed up on internally by the coordination function.

supplemented with the ability to issue a decision on compulsory liquidation or de-registration.

- The information in the register of beneficial owners should be confirmed by the legal entity once a year.

2. Introduce a periodic reporting obligation for the county administrative boards' and the Swedish Gambling Authority's supervised entities

The analysis of threats and vulnerabilities in relation to the county administrative boards' supervisory responsibilities indicate that operators generally have a low level of knowledge of money laundering regulations. The introduction of a periodic reporting requirement would increase knowledge and awareness of the Anti-Money Laundering Act among these operators. Even though the introduction of this requirement would be resource-intensive, the measure would also facilitate the proper maintenance of the register, as the county administrative boards would then be able to continuously identify operators who are no longer subject to the legislation.

Furthermore, the county administrative boards have limited information on operators (which has been identified in the sector catalogue). In order to be able to effectively conduct supervision with a focus on risk, the county administrative boards need access to up-to-date, relevant information from operators under their supervision.

The Swedish Gambling Authority is currently able to request the information and documents needed for money laundering supervision in accordance with the Gambling Act (Chapter 18, Section 4) (2018:1138). Information that is needed for a risk classification is also requested based on the above-mentioned provision in that the risk classification in turn constitutes the basis for supervision. However, there is no clear legal basis for regularly requesting this information from operators. The introduction of a periodic reporting requirement would close the gap between the authority and the supervised entities in these matters and increase continuous self-monitoring among the operators; for example, by having companies regularly respond to questions about the existence of governing documents and when these were last updated. As a whole, the above proposals would contribute to more effective supervision, where the authority is able to intervene quickly if a supervised entity is clearly failing to comply with the legislation.

Proposals:

- Introduce a periodic reporting requirement for operators who are under the supervision of the county administrative boards. An amendment to the Anti-Money Laundering Act would grant the county administrative boards authority equal to that granted to the Swedish Financial Supervisory Authority in the same act (Chapter 8, Section 1, p. 21). This would give the county administrative boards access to up-to-date, relevant information from operators under their supervision.
- Introduce a periodic reporting requirement for operators who are under the

supervision of the Swedish Gambling Authority by granting the agency authority under the Anti- Money Laundering Act (Chapter 8, Section 1).

3. Swedish Companies Registration Office's anti-money laundering register

The analysis here indicates that there are deficits in the Swedish Companies Registration Office's register in terms of the operators who should be subject to a registration requirement, which makes it difficult for the county administrative boards to carry out their supervisory responsibilities. Therefore, there is a need to expand the assignment of the Swedish Companies Registration Office to verify and update register data.[63] Currently, not all changes in the Swedish Companies Registration Office's business register are "contagious", that is, they are not automatically applied to the anti-money laundering register. If an operator is deregistered in the Swedish Companies Registration Office's register, this also applies to the anti-money laundering register.

However, the operator is responsible for updating the information in the register. This means that there are activities that have been terminated and de-registered with the Swedish Companies Registration Office, but which remain in the anti-money laundering register. The Swedish Companies Registration Office should also be able to examine the de-registration of an activity that is subject to registration according to the SNI codes. It is anticipated that the proposed measures would improve the anti-money laundering register and ensure it contains up-to-date information.

Proposal:

- Expand the assignment of the Swedish Companies Registration Office to include the verification and updating of information in the anti-money laundering register. This proposed measure would reduce the administrative burden and the additional workload placed on the county administrative boards due to the initiation of cases for operators who are no longer covered under the scope of the legislation.

4. Requirement for registration in the goAML (Anti-Money-Laundering System) for activities that are registered in the Swedish Companies Registration Office's anti-money laundering register

Introduce a requirement that operators who are registered in the anti-money laundering register also register in the Financial Intelligence Unit of Sweden's (Fipo) system goAML. The proposed measure is expected to create better conditions for Fipo to make inquiries and send targeted information.

---

[63] Some updating needs to be done in the register. For example, the company name and registered office are changed, which is then changed in the business register and in the anti-money laundering register. If an entity is deregistered in, for example, the limited liability company register or the trade register, the company is de-registered by the Swedish Companies Registration Office in the anti-money laundering register. Information regarding the de-registration of entities is then sent in a notification to the relevant county administrative board.

Proposals:

- Introduce a requirement that all operators who are registered in the anti-money laundering register also register in the Financial Intelligence Unit of Sweden's (Fipo) system goAML.

5. Unregistered operators

The risk assessments for several sectors indicate that there are a number of operators who are not registered with the Swedish Companies Registration Office. This problem is particularly evident among operators who fall under the county administrative board's areas of responsibility. The ability to issue a sanction charge against operators who are not registered in the Swedish Companies Registration Office's anti-money laundering register, but who nevertheless conduct activities subject to the reporting duty, would reduce the risks. The proposed measure would allow fewer operators to avoid registration due to the risk of financial consequences.

Proposal:

- Introduce an amendment to the Anti-Money Laundering Act (Chapter 7) which gives the county administrative boards the right to issue a sanction charge against businesses that are obliged to register but have not done so.

6. Improved opportunities for investigation and intervention against financial actors who operate without authorisation or fail to register

This risk assessment has shown that there are operators who do not register or register incorrectly with the Swedish Financial Supervisory Authority and therefore are not included in supervision. The risk is especially evident in several sectors: currency exchange (financial institutions), money transfer (payment institutions and registered payment service providers) and management of and trading in virtual currency (financial institutions). In order to counteract these risks, it is important that the Swedish Financial Supervisory Authority has the tools it needs to effectively detect and take action against such actors. The success of this effort also requires well-functioning collaboration and the exchange of information between both authorities and private companies.

Proposal:

- Review relevant business law. The purpose is to improve conditions for the Swedish Financial Supervisory Authority so the agency can effectively detect and act against actors who operate without authorisation or fail to register.

7. Institutions under supervision that conduct covert, criminal activities

One risk that is clearly identified in this report is that there are currency exchange operations and money transfer operations (and their agents) who conduct criminal activities in addition to their legitimate activities. The Swedish Financial Supervisory Authority is not a law enforcement agency and has a limited ability to

detect these kinds of issues in connection with its authorisation review process and general supervision responsibilities. The risk is particularly evident in the currency exchange (financial institutions) and money transfer (payment institutions and registered payment service providers) sectors. Much the same way as the Swedish Financial Supervisory Authority needs additional authority to handle actors, who operate without authorisation or fail to register, it is also important that the authority has the tools it needs to effectively detect and prevent companies under its supervision from being used for criminal purposes. A continuous, in-depth collaboration between law enforcement agencies is also vital to achieving success in this effort.

Proposal:

- Review and modernize relevant business legislation and other regulations as needed. This proposal aims to improve the conditions for the Swedish Financial Supervisory Authority to be able to effectively detect and prevent companies under the authority's supervision from being exploited for criminal purposes.

8. Swedish Standard Industrial Classification (SNI)

There is a need to give the county administrative boards an easy way to identify businesses that are subject to the registration requirement in the Swedish Companies Registration Office's anti-money laundering register. One possible measure could be to review the SNI codes for activities that are or may be affected by the Anti-Money Laundering Act. The proposed measure would lead to a significantly reduced administrative burden in the county administrative boards' external review activities. However, there is a risk that operators will choose a different SNI code to avoid supervision. Therefore, there needs to be consultation between the Swedish Companies Registration Office, the county administrative boards and the Swedish Tax Agency.

Proposal:

- Create individual SNI codes for the sectors under the supervision of the county administrative boards or change them so that they relate to occupational categories instead of services.

9. Expand the reporting obligation

One conclusion drawn from the sector analysis is that there are important parts of the financial infrastructure that are not subject to the reporting obligation. There is therefore a need to expand this requirement. Such a measure would result in expanded reporting from more links in the transaction chain, thus providing significantly improved opportunities to detect money laundering.

Proposals:

- Expand the reporting obligation to include actors who provide electronic identification services that are used when establishing customer relationships and signing transactions. Clearing and settlement services that perform transactions – both individual and batch payments – should also be covered under the scope of

the Anti-Money Laundering Act, as their position in the flow of a transaction enables them to detect transaction patterns that an individual operator cannot.

- Expand the scope of the Anti-Money Laundering Act to include cash purchases of services with a value exceeding the equivalent of EUR 5,000, in order to harmonise with applicable legislation on the cash purchase of goods.

10. The Swedish Tax Agency's centralised automated mechanism

It is important for authorities to be able to quickly verify the identity of account holders and safe deposit boxes in financial companies. Today, this process is carried out manually through targeted inquiries to the financial companies. The Swedish Tax Agency's centralised automated mechanism makes the search process much simpler, which helps prevent the financial system from being exploited for money laundering or terrorist financing. Gambling accounts are not included in the Account and Deposit Box systems Act (unofficial translation, Swedish title lagen om konto- och värdefackssystem). It is possible to hold and hide assets in a gambling account. Therefore, in order to combat money laundering and terrorist financing, requirements to report are needed.

Proposals:

- Gambling companies should be covered under the scope of the Account and Deposit Box systems Act (unofficial translation, Swedish title lagen om konto- och värdefackssystem).

11. Prevent and complicate the misuse of identities through stronger customer identification

One of the conclusions in the 2019 national risk assessment was that borrowed, stolen or false identities are often used in money laundering schemes. Although there are currently a large number of initiatives aimed at counteracting this risk, the problem still persist.

Proposal:

- Continue to implement measures that reduce the chances of using false or misused identities. This can be done, for example, through more stringent requirements that include biometric authentication[64], the establishment of tenant-ownership registers and access to quality-assured information for addresses in the population register.

[64] See also the proposals presented in connection with the *Reporting of Government Assignments on Measures against the Financing of Terrorism* (Ju 2018/01649/PO, Reg. no. 2018-8405).

7. Sector catalogue -assessment of money laundering and terrorist financing

The following chapters present the first summary of the sectors that fall under the scope of the Anti-Money Laundering Act.[65] The summary shows the broad range of activities that are directly affected by Swedish legislation to combat money laundering and terrorist financing. The catalogue describes each sector's unique character, size, primary activities and key figures. This is also the first presentation of the assessment of threats and vulnerabilities for each sector.
The assessment includes a quantitative assessment of the risk of money laundering, as well as a qualitative assessment of the threats and vulnerabilities associated with terrorist financing.

[65] The sector catalogue has been developed using the EU's supranational risk assessment as a guideline.

7.1 Banking or financing business

Overall sector risk:

Sector

The core activities of the banking and financing business are deposit and lending services. Other financial services may also be offered in the sector, such as payments and transfers, securities transactions and the issue of cards.

General description of the sector and related products or activities

Banking and financing businesses serve as intermediaries for payments via payment systems and receive money in accounts. Activities in the sector also includes the provision of credit and providing credit guarantees or acquiring receivables or enable leasing for financing purposes.

The sector includes several different types of banks, with commercial banking being the most common. Commercial banks are limited companies that have been granted authorisation from the Swedish Financial Supervisory Authority to conduct deposit operations. There are also other forms of banking, such as savings banks, niche banks and credit unions.

The activities of these banking operations may be very similar or significantly different than commercial banks, and the risk associated with these operations may vary.

Banking or financing operations may – with certain exceptions – only be conducted after being granted authorisation by the Swedish Financial Supervisory Authority. Prerequisites and conditions are set out in the Banking and Financing Business Act (2004:297) and the Banking and Financing Business Ordinance (2004:329). In the case of savings banks, there are also rules set out in the Savings Banks Act (1987:619).

Key figures*	**Total for entire sector**
Number of companies	152
Companies' turnover	SEK 8,596 billion
Companies' balance sheet total	SEK 596,618 billion
Number of employees	50,603
Number of established business relationships	44,896,707
Total Number of natural customers	**39,285,063**
Total number of legal customers	**1,871,420**

* All data in the table were obtained from the Swedish Financial Supervisory Authority's periodic reporting for money laundering, report F880, with a reference date of 31/12/2019. The table may therefore contain data that differ to some extent from the current situation.

Money laundering – description of risk scenario including known approaches (modus operandi)[66]

- Money transactions linked to previous criminal activities are deposited into bank accounts. The money is quickly moved further, either to other banks in Sweden or abroad. A relatively common form of fraud is a BEC scam (Business E-mail Compromise Fraud). In a BEC scam, companies are convinced to make incorrect payments to an account controlled by the perpetrator of the fraud. This means that money laundering that is carried out inside Sweden is most likely the result of fraud that has been committed abroad. The arrangement can also work in reverse.
- Cash withdrawals that originate from fraud or other criminal activities are made by what are known as money mules. The mules hand over the cash to the UBO for a certain form of commission.
- It is often young people – sometimes unknowingly or under threat – who are used as frontmen for criminal money when criminal proceeds are to be transferred through payment intermediaries.

Threat – money laundering

Scope

There are many different types of products and services offered in the banking sector. This means that transactions carried out for the purpose of money laundering can pass through the banking sector temporarily, even if the threat actor does not use the sector as the primary means for money laundering. The use of payment intermediaries is also considered a factor that increases the attractiveness of the sector for money laundering.

Threat actors can quickly complete transactions using a number of products offered in the sector. This increases the threat of money laundering, as the speed of transactions makes it difficult to detect the origin of the funds. The accessibility and large number of users in the sector also contribute to the extent of money laundering. In addition, the large turnover creates a potential to launder large volumes of cash.

Capacity of threat actors

It is quite easy to open bank accounts and use the products and services in the banking sector. Therefore, certain money laundering schemes are not difficult to carry out. For example, cash can be deposited into an account and a series of smaller deposits can be made. However, the opportunity for money laundering is

[66] Several products offered in the banking sector are also offered in other sectors where the risk modus operandi is described. The risk assessment of the banking sector includes all bank products.

becoming increasingly limited due to stricter controls. Complex money laundering schemes, on the other hand, may require a higher capacity on the part of the threat actor, for example, certain knowledge or access to a contact network.

Anonymity

Legal entities frequently use the sector, particularly in the more extensive money laundering schemes. Even if a natural person or legal entity is not anonymous, it is possible to remain anonymous by using strawmen, frontmen or false documentation. By using a legal entity, anonymity can be increased along with the threat of money laundering.

Overall assessment

Money laundering can be carried out quickly and can involve large sums of money. In some of the less complex money laundering schemes, the threat actor is not likely to need any special capacity. Customers are usually not anonymous in the sector, but it is possible to use strawmen or frontmen.

In summary, the threat of money laundering in the sector is assessed as high (4).

Vulnerability – money laundering

Ability to detect money laundering

The sector has good resources for risk management and good control systems. Risk management is usually structured in the three lines of defence model. The first line of defence is operational management, i.e. the people who work with the operation of the business. These individuals are responsible for identifying, monitoring and managing the operational risks of the business, including risks linked to money laundering and terrorist financing. The second line of defence consists of functions for risk management and regulatory compliance. These functions monitor, evaluate and in some cases support first-line risk management and regulatory compliance. The third line of defence consists of functions that provide independent assurance through audit (internal or external), which evaluate both risk management and regulatory compliance performed in the first and second line of defence. The second and third lines of defence are generally strong in the sector. In addition, the larger institutions have established frameworks for identifying, measuring, monitoring and reporting the level of particularly important risks. To further strengthen risk prevention measures, there are monitoring systems for customer transactions as well as established routines and processes.

Larger credit institutions often offer complex products and services and have a wide variety of customers. IT systems and databases are not always homogeneous. This makes it difficult to create an efficient, well-functioning risk management system to prevent money laundering and terrorist financing. The sector also has a broad customer base that includes, for example, corporate customers with complex ownership structures. This makes it possible for threat actors to remain anonymous in addition to the fact that transaction amounts for these customers

can be very high. It can therefore be difficult to identify the beneficial owner. There are also vulnerabilities associated with false documentation.

Regulatory compliance

There is generally good awareness and knowledge of the money laundering regulations in the sector. Organisational conditions are also assessed as good, and the larger institutions have dedicated significant resources to their control functions. Furthermore, extensive customers due diligence measures are being implemented. However, the sector may be vulnerable when actors who apply for products or services online are only identified using BankID. There is also a risk that threat actors will use strawmen and hijacked identities.

Overall assessment

Access to resources, organisational conditions, risk culture and the degree of maturity may differ within the sector. However, overall, risk awareness and organisational conditions in the sector are deemed to be good. On the other hand, larger credit institutions may find it difficult to create efficient, well-functioning control systems, due in part to the complexity of the products and services they offer. customer due diligence measures are implemented, but in cases where strawmen are used or complex ownership structures exist, threat actors can remain anonymous.

In summary, vulnerability to money laundering in the sector is assessed as moderate (2).

Description of risk scenario including known approaches (modus operandi) to terrorist financing

- Bank accounts are used to collect funds for financing terrorism to varying degrees. This can be done in a number of ways, including through payment intermediaries, cash deposits or bank transfers. When the account has accumulated the desired amount, the money is then transferred. This is done using a variety of methods, in transactions that often mean the money leaves the banking sector and Sweden. These transactions may involve card transactions through payment institutions. But the money can also be transferred through registered payment service providers, for example, through electronic money institutions, cash withdrawals or bank transfers. Terrorism is financed through cross-border transactions in the banking sector to a lesser extent, but these transactions can occur as the first of many steps in a financing scheme.
- Credit can be obtained by false pretences and without the intention of being repaid. This makes it possible for large sums of money to be transferred abroad. One way the money leaves Sweden and enters the recipient country is for the account holder (or another person who is authorised to use the bank card) to travel abroad, for example, to a country that borders the country that is the ultimate destination of the illicit funds. Actors make as many cash withdrawals in the third country as possible, until the bank manages to block the account. If

large sums of money are involved, the funds will likely be divided among several users.

- Operators in the *Currency Exchange and other financial activities* sector can be exploited to systematically execute transactions in order to finance terrorism. In these cases, the transactions made through the bank account are part of a larger scheme.

Threat – financing of terrorism

Scope

In terms of the extent of terrorist financing, the conditions that play a critical role for money laundering also apply. The banking sector is easily accessible for the purpose of financing terrorism, but the scope is still assessed to be significantly lower than it is for money laundering, both in terms of how frequent it occurs, and the amount of money involved.

Although the modus operandi of using of bank lending is unusual for financing terrorism,
a relatively large amount of credit can be granted to an individual borrower.

Capacity of threat actors

No special abilities or knowledge are required to carry out a simple scheme to collect funds or to send individual transactions for the purpose of financing terrorism. However, actors who systematically collect funds and do so to a more significant extent, need to find ways to conceal the ultimate purpose of the money. This likely requires more familiarity with how the approach should be implemented and which banking services to choose, which is more difficult for the bank and authorities to detect.

When it comes to exploiting a line of credit, the prerequisites for obtaining credit by demonstrating creditworthiness or the ability to obtain credit by falsely demonstrating creditworthiness are required. Knowledge of the credit history system is required to be able to take out several smaller lines of credits without the intention of repaying.

The opportunities to open a bank account are the same as for money laundering. Knowledge of the bank's customer due diligence procedures increases the ability to avoid being reported or being locked out of the bank's services in the event of abnormal transactions.

Anonymity

In terms of the financing of terrorism, similar conditions apply for anonymity as for money laundering. Foundations are used for more systematic and extensive financing of terrorism. This is likely due primarily to a lack of ability to gain insight into the composition of a foundation and the activities it conducts.

Vulnerability – financing of terrorism

Opportunity to detect terrorist financing

The banks' control systems are outlined in the section on money laundering, and the vulnerabilities described here also apply to the financing of terrorism. However, in terms of the terrorist financing, it is also an aggravating circumstance that the banking sector is used as one of many sectors in a long chain. The ability to detect terrorist financing is therefore more complicated than it is for money laundering. This difficulty also relates to the fact that it is the ultimate purpose of the money that is in question – not the origin or modus operandi – thus making it more difficult for the banking sector to detect the relevant transactions. The fact that terrorist financing schemes can involve small amounts of money is another aspect that makes its detection and potential severity so complicated.

The difficulty of detecting misused lines of credit is related to the potential for performing credit checks and how well these checks reflect the real picture. Inaccurate income information can be used, and in addition to this, there is a certain backlog for lines of credit that have recently been granted. This is a fact that is widely known and has been abused for the purpose of financing terrorism.

Regulatory compliance

The same assessment as for money laundering applies here.

7.2 Life insurance business

Overall sector risk:

Sector

The Life insurance sector offers different types of savings insurance as well as risk insurance that is linked to these plans.

General description of the sector and related products or activities

Life insurance can basically be divided into two types: savings insurance and risk insurance. Savings insurance includes pension and endowment insurance and risk insurance includes life insurance as well as medical and accident insurance. When a life insurance policy is paid out depends on whether one or more insured are living, and this can be a lump sum or a periodic payment.

In the case of savings insurance, the customer can choose a traditional life management where the insurance company manages the money with a guarantee of a future result. However, the customer can also choose *unit-linked* life insurance and make the investment decisions themselves. Unit-linked insurance can in turn be divided into unit-linked fund insurance with investments in various funds and into custodian insurance where the investment (in addition to funds) is made in other financial instruments. The potential financial instruments are specified in the insurance company's investment guidelines and in the insurance contract.

The insurance policies are distributed either by the insurance companies themselves or through intermediaries (insurance brokers). The sale and management of unit-linked insurance is often done directly on the insurance company's website. In Sweden, the largest fund and custody account insurance companies are bank owned.

The life insurance sector is primarily regulated by the Insurance Business Act (2010:2043).[67]

Insurance is essentially a national product that is strongly linked to tax legislation. For this reason, the risks that can be linked to life insurance also differ between countries. This is reflected in the customer base in the sector, where a significant majority of customers in the insurance sector (both natural persons and legal entities) are domiciled in Sweden.

67 Additional rules that govern the sector (including Swedish Financial Supervisory Authority's regulations) can be found at www.fi.se/sv/forsakring/regler/forsakringsforetag/ (retrieved 14/02/2021).

Key figures*	Total for entire sector
Number of companies	40 **
Companies' turnover	SEK 200 billion
Companies' balance sheet total	SEK 4,165 billion
Number of employees	6,752
Number of established business relationships	11,513,412
Total Number of natural customers	**7,874,188**
Total number of legal customers	**1,088,483**

* All data in the table were obtained from the Swedish Financial Supervisory Authority's periodic reporting for money laundering, report F880, with a reference date of 31/12/2019.The table may therefore contain data that differ to some extent from the current situation.

** Of these, bank-owned companies account for a majority of the key figures in the table.

Money laundering – description of risk scenario including known approaches (modus operandi)

- Threat actors (or frontmen) make deposits into savings insurance. Endowment insurance is used most frequently, with subsequent renewals or pay outs according to the insurance contract. The policy is paid out to either the holder of the account or the beneficiary (layering and integration). The UBO may be the insurance policy holder or, alternatively, the beneficiary of the insurance upon opening an account or at a later stage.
- For the purpose of money laundering, a company is pledged, in whole or in part, by using corporate bonds as part of the scheme. A securities company issues the corporate bond. The bond – from which investors can benefit through their custody account insurance – is obtained through an insurance broker. The company then repays the bond with funds acquired through illegal activities (layering and integration). The money obtained through the bond issue can also be used to finance other illegal activities. The scenario also includes other types of structures where the investor can influence or control the security in which the funds are invested (placement).
- Acquisitions of insurance companies that offer unit-linked fund insurance and custody account insurance. The products are very profitable in that there are sizeable kickbacks from the fund companies. Therefore, the business model is attractive for investors all over the world and consists of various associations created solely for the acquisition (so-called Special Purpose Vehicles/SPVs). Due to the fact that ownership structures and products can be complex, transparency is also reduced. This can be exploited for advanced money laundering schemes (placement, layering and integration).

Threat – money laundering

Scope

The sector's products normally have a long turnover rate, and the products often have provisos attached that prevent early repurchases. Due to these factors, the sector is assessed to be less attractive for money laundering and the scope of money laundering schemes is reduced in the sector.

Ability of threat actors

Threat actors need to have a certain level of knowledge of the products and an opportunity to plan their approach. Criminals who have the knowledge and ability to attempt more advanced schemes in the sector are considered to be the main threat. It cannot be ruled out that the volume of laundered money may be high in individual cases and that schemes that are more difficult to detect are used to a greater extent.

Anonymity

The use of strawmen makes it more difficult to trace transactions in cases where companies are part of the criminal scheme. Schemes have been identified on the international level, where collaborators or insiders have been involved by, for example, packaging complex products. As the insurance company is owned by foreign holding companies, a threat profile for money laundering associated with these companies is also noted.

Overall assessment

Products sold in the sector have typically had a long turnover rate, and the products often have restrictions that prevent or make early repurchases impossible. Threat actors also need to have a certain degree of knowledge and capacity to carry out more advanced money laundering schemes in the sector. It cannot be ruled out that the volume of laundered money may be high in individual cases and that schemes that make it difficult to detect are used.

In summary, the threat of money laundering in the sector is considered to be moderate (2).

Vulnerability – money laundering

Ability to detect money laundering

The transaction speed in the sector is relatively low, and the sector is not exposed to cash. Transactions are mainly domestic in character (within Sweden). The traceability of domestic transactions – which are largely administered via Swedish credit institutions – is generally considered to be good.

The life insurance products that are deemed to pose the greatest risk of money laundering are endowment insurance, and custody account insurance in particular. Custody account insurance plans have a short investment horizon (at least 1 year) and investment opportunities are open. There can also be vulnerability to money laundering in cases where life insurance companies are owned through foreign

holding companies, as the opportunity for supervision of foreign owners is very limited.

Regulatory compliance

Several of the life insurance companies' regulatory compliance functions acknowledge in their own assessments that the risk of money laundering is one of the major risks that the companies need to address. However, the regulatory compliance functions are often relatively small, especially in relation to the size of major credit institutions. For smaller life insurance companies, this function may consist of only one person. The internal audit function is also small in comparison to the equivalent function in the credit institution sector. In addition, the function can sometimes be outsourced.

Some of the companies' internal audit functions have increased the proportion of audits that focus on regulatory compliance. However, resources are limited, and the companies often fail to create the right conditions to adequately address money laundering risks. If the functions in the second and third lines of defence have limited resources, influence and authority, there is a risk of inadequate risk awareness within the organisation.

There may also be a risk for conflicts of interest related to business and remuneration models. This holds especially true in cases where business relationships are established with the involvement of intermediaries. In these cases, it can lower the incentive to strengthen organisational conditions.

The funds invested in the insurance policies rarely go through the life insurance companies themselves. Most payments are handled through the traditional banking system. The vulnerability becomes more significant when an insurance company is also owned by a bank. This type of transaction is therefore examined by credit institutions that have a relatively high capacity to monitor transactions. However, the life insurance companies themselves need to identify, monitor and manage the risks associated with money laundering. They cannot rely solely on the (potential) measures taken by other operators. The extent and quality of internal controls can vary between companies in the sector. The larger companies typically have more resources to carry out controls. Many of the companies' regulatory compliance functions and internal audit functions have identified major deficits in control procedures.

Additionally, the sector accounts for a very small proportion of the reports made to the Financial Intelligence Unit of Sweden (Fipo). This is likely attributable to a combination of the vulnerabilities outlined above.

Overall assessment

The transaction speed in the sector is relatively low, and the sector is not exposed to cash. Transactions are mainly domestic in character and the traceability of domestic transactions is generally deemed to be good.

In summary, vulnerability to money laundering in the sector is assessed as moderate (2).

Risk – financing of terrorism

There are currently no known scenarios in which the sector is used to finance terrorism within the framework of the national risk assessment. Therefore, the risk of terrorist financing in the sector has not been assessed.

7.3 Securities business

Overall sector risk:

Sector

Operators in the securities business make investments or offer professional investment services. The securities sector is often cross-border in nature, and companies in this sector may offer services in several different jurisdictions.

General description of the sector and related products or activities

The securities market is dominated by banks that are authorised to offer investment services. The securities companies are relatively small, and a majority of employees, as well as the majority of sales and turnover, are attributable to a handful of companies. There are several small companies in the sector.

Securities companies are mainly regulated by the Securities Market Act (2007:528).[68] Chapter 2, Section 1 of the law stipulates which products and services may be offered. The most common services are: 1) receipt and forwarding of orders for one or more financial instruments, 2) execution of orders on behalf of clients, 3) portfolio management and 4) investment advisory services. The trade in securities can either be done directly by the securities company (item 2), or indirectly through advisory services or brokerage of orders (items 1 and 4).

In order to carry out operations in the securities sector, authorisation is required from the Swedish Financial Supervisory Authority. There are also securities companies that have several different types of authorisations, for example, for securities and insurance brokerage.

Key figures*	**Total for entire sector**
Number of companies	122 **
Companies' turnover	SEK 10,785,010,136
Companies' balance sheet total	SEK 14,625,663,207
Number of employees	2,219
Number of established business relationships	497,060
Total Number of natural customers	**602,050**
Total number of legal customers	**42,306**

* All data in the table were obtained from the Swedish Financial Supervisory Authority's periodic reporting for money laundering, report F880, with a reference date of 31/12/2019.The table may therefore contain data that differ to some extent from the current situation.

** There are only 93 securities companies based in Sweden. The remaining companies are a number of

68 See www.fi.se/sv/marknad/regler/vardepappersinstitut/ (retrieved 14/02/2021) for a complete list of applicable rules, including the Swedish Financial Supervisory Authority's regulations.

banks that are also authorised to provide investment services as well as branch offices of securities companies based abroad. Several securities companies also have a significant number of tied agents. The number of tied agents has increased from about 260 in 2012 to almost 400 in 2020. There are six tied agents in Sweden working on behalf of foreign EEA securities companies. In addition, there are about 2,900 EEA securities companies with cross-border operations in Sweden.

The table is based on data mainly from a few large companies.

Money laundering – description of risk scenario including known approaches (modus operandi)

- Threat actors can use the sector's legitimate products in person or through frontmen. For example, a threat actor can buy and sell securities with money acquired through illegal activities. The purpose is to layer or integrate the funds.
- By concealing the UBO's identity, for example, by using frontmen or complex corporate structures, individuals with insight into how the sector functions can commit insider trading. Insider trading means that the threat actor uses non-public information to generate profits in their own securities account. The criminally acquired profits can then converted through trade in other securities and layered through the financial system to accounts within Sweden and abroad.
- By controlling several accounts in different securities companies, threat actors can trade securities between these accounts. The purpose is to manipulate and influence prices, known as market manipulation. Any profits acquired through this type of crime can be converted through other securities transactions and layered through the financial systems to accounts within Sweden or abroad.
- Securities companies can also act as a channel for pure investment fraud. These can be financial products that prove to have no value or lower value, which are designed and then offered to consumers in the market. The criminally acquired profits from these fraudulent products can then be converted through trade in other securities and layered through the financial system to accounts within Sweden and abroad.

Threat – money laundering

Scope

The scope and frequency of money laundering in the sector is deemed to be relatively low, while the volume of money that can potentially be laundered is considered to be high. Some threat actors use the sector's products to layer and integrate criminally acquired funds. There are also actors who use the sector to commit predicate offences for money laundering. For example, these offences can include fraud or the use of corporate bonds as part of a criminal scheme.

Ability of threat actors

For more complex money laundering schemes, threat actors also need a certain level of knowledge about the sector as well as facilitators. For actors with a high capacity - that is, knowledge, capital and facilitators – there are significant

opportunities for money laundering in the sector.

Anonymity

The ability to remain anonymous when carrying out transactions in the sector is deemed to be low. Therefore, there is always a risk that frontmen will be used, which makes it difficult to identify the beneficial owner.

Overall assessment

There are some indications that a threat actor fitting a particular profile uses the sector's products to layer and integrate funds. The volume of money that can potentially be laundered in the sector is deemed to be high.

In summary, the threat of money laundering in the sector is deemed to be significant (3).

Vulnerability – money laundering

Ability to detect money laundering

The sector includes cross-border companies that operate with authorisation from so-called tax havens. These presence of these operators helps increase the sector's vulnerability to money laundering.

Vulnerability is also increased by actors who transfer funds to and from jurisdictions with less efficient AML/CTF systems.

In order to reduce the vulnerability to money laundering in the sector, actors who carry out transactions must always be able to be identified. Therefore, vulnerability increases when securities are traded through corporate structures that are complex or not completely transparent.

The rules that certain types of cross-border transactions are to be reported to the Swedish Tax Agency reduce the vulnerability to money laundering to a certain extent. Another factor is that the sector is essentially cashless.

Regulatory compliance

A large proportion of companies in the sector have only a few employees. This often means that the business's control functions are small. This can affect the way money laundering risks are managed and limit a company's risk level of risk awareness. Reports from the companies' functions to ensure regulatory compliance are relatively limited in scope and deficiencies are seldom identified.

In order for an adviser to become licensed through SwedSec, certain knowledge of money laundering regulations is required.[69] The requirements include knowledge of customer due diligence measures, transaction monitoring and reporting of suspicious transactions to the Financial Intelligence Unit of Sweden (Fipo). In the course of supervision activities, shortcomings in risk management are frequently discovered in the sector. For example, it is found that companies do not always comply with their own internal instructions in practice. It can also be that a

[69] SwedSec grants licences based on knowledge requirements and testing and has an established disciplinary procedure in cases of rule violations.

company's controls (as described in internal regulations) are not always implemented, or only to a limited extent.

During the years 2018–2019, only a small number of suspicious transactions were reported to the Financial Intelligence Unit of Sweden (Fipo), which may be indicative of under-reporting.

Overall assessment

The sector is cash-free and all actors who complete transactions must be able to be identified. However, companies in the sector generally suffer from organisational challenges and shortcomings in internal risk management. Furthermore, it is possible that cases go under-reported to the Financial Intelligence Unit of Sweden (Fipo).

In summary, vulnerability to money laundering in the sector is assessed as moderate (2).

Risk – financing of terrorism

There are currently no known scenarios in which the sector is used to finance terrorism within the framework of the national risk assessment. Therefore, the risk of terrorist financing in the sector has not been assessed.

7.4 Currency exchange activities and other financial activities or deposit-taking activities.

Overall sector risk:

Sector

Currency exchange encompasses all businesses that are allowed to conduct currency exchange activities, regardless of the authorisation or registration the business holds.

Other financial activities are a broad category with companies that engage in several different types of activities across different sectors. Examples include companies that conduct activities in leasing, factoring, grassroots financing and virtual currencies.

Natural persons or legal entities that conduct currency exchange or other financial activities are collectively referred to as financial institutions.

General description of the category and related products or activities

Currency exchange

Currency exchange is the professional trade in foreign bills and coins, including traveller's checks issued in foreign currency.[70] In order to conduct currency exchange activities to a significant extent, businesses must be registered with the Swedish Financial Supervisory Authority. Companies must be registered in accordance with the Act on currency exchange and other financial services (1996:1006) (LVA) if the activities fall under the scope of the Anti-Money Laundering Act.

Companies that are registered as currency exchangers in accordance with the Act on currency exchange and other financial services are limited to trading in cash transactions – that is, the exchange of bills, coins and traveller's checks. In order for a business to offer currency exchange services through card payment, the business must obtain authorisation from the Swedish Financial Supervisory Authority to operate as a payment service provider.

Currency exchange operations can have different types of authorisations or registration. Which authorisation or registration is needed depends on the services the company wishes to offer. The "typical" currency exchange business may, for example, be authorised to conduct money transfer operations in accordance with the Payment Services Directive (2010:751) (LBF). Currency exchange activities can

[70] If the activity is classified as a professional operation and involves the management of or trading in virtual currencies, it is considered as other financial business.

also be conducted by banks.

There are also foreign companies that offer money transfer services. These businesses are established in Sweden through agents. The agents are allowed to offer currency exchange services in addition to money transfers after registering with the Swedish Financial Supervisory Authority. As the majority of operators offering currency exchange services have different types of authorisations or registrations, certain key figures and assessments may overlap with other sectors in this risk assessment.

Other financial activities

All companies in the *Other financial activities* category are required to register with the Swedish Financial Supervisory Authority and are subject to money laundering regulations. Registration entitles the operator to offer all services that registration permits in accordance with the Act on currency exchange and other financial services (LVA).

This category is regulated by Act on currency exchange and other financial services (LVA) and is defined as a professional operation. The category covers the management of or trading in virtual currency, or operations that primarily include one or more of the activities (as described in Chapter 7, Section 1 paras 2 (2, 3, 5-12) of the Banking and Financing Business Act (2004:297). For example, these activities can be about granting and brokering loans (corporate loans) or participating in financing (factoring, leasing).

Since 1 January 2020, this activity is subject to a registration requirement under the Act on currency exchange and other financial services (LVA). Activities in this category include the exchange between digital currencies and traditional currencies, exchange between different virtual currencies, or transfer of digital currencies (for example between different wallets). Even before the new law entered into force, the Swedish Financial Supervisory Authority considered those who sold digital currencies that were used as a means of payment as agents engaged in other financial activities that could be subject to supervision under money laundering legislation. More specifically, the activity is covered by the concept of provision of means of payment (Chapter 7, Section 1, Paragraph 2, (5), Payment Services Directive).

Of all the companies that are subject to the registration requirement under the Act on currency exchange and other financial services (LVA), a significant portion are registered in the category *Other financial activities*. Apart from digital currencies, there are a range of activities that fall within this category, all with different types of risk. Examples include activities within leasing, factoring and grassroots financing. Any company that wishes to register to engage in other financial activities must specify the type of activity that the company intends to conduct. However, this is not registered in the Swedish Financial Supervisory Authority's company register.

Deposit-taking activities

A company engaged in deposit-taking activities receives repayable funds from the general public. Upon termination, these funds are made available to the creditor

within a maximum of one year. A company that engages in deposit-taking activities may receive a maximum of SEK 50,000 per consumer in deposits, in accordance with the Deposit-taking Activities Act (Section 9).

Deposit-taking activities may only be conducted by limited companies or economic associations that are registered in accordance with the Deposit-taking Activities Act (2004:299). Companies that have registered under the Deposit-taking Activities Act are primarily economic associations, mainly HSB. Some limited companies are also registered.

As of the time this analysis was performed, the government has put forward a proposal which would mean that the majority of companies that are authorised to conduct deposit-taking activities will vanish from the sector.[71] The government is proposing that the Deposit-taking Activities Act be repealed and that the operators covered under the scope of the act will be required to apply for authorisation to conduct banking or financing activities. However, this change does not apply to certain economic associations that engage in deposit-taking activities, which will continue to be covered by the current law. The new law is proposed to enter into force on 1 January 2021.[72]

Key figures*	**Total for entire sector**
Number of companies	263
Companies' turnover	SEK 29,935,420,366
Companies' balance sheet total	SEK 230,030,804,114
Number of employees	4,918
Number of established business relationships	786,097
Total Number of natural customers	**658,420**
Total number of legal customers	**140,756**

* * All data in the table were obtained from the Swedish Financial Supervisory Authority's periodic reporting for money laundering, report F880, with a reference date of 31/12/2019. The table may therefore contain data that differ to some extent from the current situation.

Money laundering – description of risk scenario including known approaches (modus operandi)

- The exchange of cash obtained from criminal activities for another currency can occur in the sector. The exchange agent can also accept bank transfers, including mobile payments, and exchange this for cash. The exchange itself makes it more difficult to track the origins of the money further and thus enables washing of the

[71] Referral to the Council on Legislation: Strengthened consumer protection in the deposit market.

[72] The Deposit-taking Activities Act (2004:299) was repealed on 01/01/2021. However, the act still applies to economic associations which, prior to the date the Deposit-taking Activities Act entered into force, were registered under that law and which, within the framework of non-financial activities, conduct deposit-taking activities for members of the association who contribute to the financing of the association's activities. Furthermore, in the case of other economic associations and limited companies that were registered in accordance with that law before it entered into force, the repealed law continues to apply until the end of 2021. See Act (2020:1026) on the repeal of the Deposit-taking Activities Act (2004:299).

criminal exchange. Exchange can also be made for cryptocurrency via one or more accounts that the exchange agent holds through companies or private individuals who trade in cryptocurrency.

- A significant share of the trade in cryptocurrencies involves private individuals who have not registered their activities with the Swedish Financial Supervisory Authority. Significant sums of cryptocurrency are turned over by these individuals without being subject to supervision or checks in accordance with the regulations on money laundering. Payment for cryptocurrencies is often made through ordinary private bank accounts. It is not uncommon for amounts to be traded that are significantly higher than the exchanger's declared annual income.[73]
- Through activities such as leasing, black money can be integrated and layered. At the same time, this approach provides the person who wants to integrate the money access to the product being leased.

Threat – money laundering

Scope

The sector is very diverse, with a large number of operators active in areas such as currency exchange, digital currencies, factoring and leasing. This means that potential threat actors can also vary depending on the type of operator. Currency exchange offices are often easy to access, and transactions are carried out in real time.

The sector is otherwise characterised by a low proportion of physical offices and a product range that is relatively simple and easily accessible.

Currency exchange offices have been infiltrated by criminal organisations, which use them to carry out their activities. High volumes of money can thus be easily converted into legitimate currency.

Ability of threat actors

While currency exchange does not typically require any special capacity or expertise, some capacity is required to utilise other money laundering approaches that have been identified in the sector.

Anonymity

Over-the-counter currency exchange involves a physical visit to the currency exchange bureau, which reduces the ability to remain anonymous, provided that an ID verification is carried out. But it is possible for threat actors to use strawmen when exchanging currency.

Operators are obliged to take customer due diligence measures, as prescribed by Anti-Money Laundering Act, in transactions that individually or together amount to the equivalent of EUR 15,000 or higher (unless it is a business relationship). Threat

[73] *Financial Intelligence Unit of Sweden's annual report*, (2019) pp 12-13.

actors can make structured currency exchanges within certain limits below this threshold as a means to reduce the risk of detection and reporting ("smurfing"). This opportunity is deemed to increase the threat of money laundering in the sector.

The trade in digital currencies increases the threat of money laundering, as digital currencies are by design pseudo-anonymous and easily accessible. It is also common for legal entities to be used in money laundering schemes, which increases the ability to remain anonymous.

Overall assessment

Given the size and diversity in the sector, it is believed that there are a large number of threat actors who conduct money laundering in the sector. The sector is characterised by easy accessibility and accommodates a diverse group of operators. This group also includes operators who are deemed to present a higher risk.

In summary, the threat of money laundering in the sector is assessed as high (4).

Vulnerability – money laundering

Ability to detect money laundering

Companies that provide currency exchange services mainly serve customers who exchange cash for travel, but the segment also includes high-risk customers.

The exchange of money for the purpose of money laundering can be done by exchanging Swedish kronor to or from another currency, or by exchanging monetary amounts in Swedish currency. As the use of cash is continuously decreasing in Sweden, the exchange of Swedish currency can present a risk and exposure to money laundering. The cash-intensive nature of the industry also means limited traceability and a certain vulnerability to money laundering. Since cash is not traceable, there is always the possibility that the individual exchanging currency is completing the transaction for another party or provides false identity documents. Due to these conditions, the sector is deemed to be particularly vulnerable to money laundering.

The sector *Other financial activities* is considered to have a very low, almost non-existent, use of cash. Cross-border transactions also occur in the sector. The exchange of digital currencies, in particular, is transactions that are regularly cross-border in nature. There is also an inherent pseudo-anonymity in these types of transactions. Digital currencies are traceable when the transaction itself can be traced, but the sender and recipient often remain anonymous. Grassroots financing is also characterised by a degree of vulnerability to money laundering due to cross-border transactions. Grassroots financing can take several different forms and often has different financing options.[74] Funds can either be sent abroad immediately as part of the financing solution or sent abroad at a later stage.

Transactions made through a currency exchange and transactions with digital

[74] Swedish Financial Supervisory Authority, *Grassroots financing in Sweden – a survey*, 2015.

currencies can be carried out quickly, which increases the assessed level of vulnerability to money laundering in the sector.

Additionally, after a company has obtained registration, there is nothing to prevent these companies from pursuing one or more of these activities (as specified in Chapter 7, Section 1, para. 2 (2, 3, 5-12) of the Payment Services Directive) without applying for a new registration. It is also impossible to ascertain the types of activities the companies conduct based solely on their registration.

Regulatory compliance

Risk awareness in the sector varies between the different activities. This is due in part to the fact that certain activities are relatively new, and partly because a certain segment of the sector consists of actors who are smaller in scale. It is also assessed that awareness and knowledge of money laundering regulations is weak, and the supervision of currency exchange companies has revealed a substantial number of shortcomings.

Given that the sector largely consists of smaller companies, it is a challenge to create the conditions to manage the risks associated with money laundering, for example, when appointing AML functions.

Many of the companies engaged in currency exchange activities are only able to carry out manual monitoring. At the same time, the exchange is usually completed immediately. There is therefore a risk in this business model that operators will not have the opportunity to take adequate customer due diligence measures at the time of the exchange. This creates a high degree of vulnerability, leaving the sector exposed to exploitation for money laundering.

There are customers in the sector with a high degree of violent capital. As many companies in the sector are small and locally based, this increases the risk that the companies will either assist in and/or fail to report suspicious transactions due to threats or fear of retaliation. There are also a number of smaller actors in the sector who are more likely to depend on recurring transactions. There are also operators – especially in digital currencies – who refrain from reporting for their own financial gain.

There are also operators who conduct activities in the sector that are subject to the registration requirement without applying for, or being granted, registration with the Swedish Financial Supervisory Authority. This mainly applies to trading in digital currencies.[75] This, in turn, increases the risk of regulatory non-compliance and increases vulnerability to money laundering.

On the international level, there are frequent warnings that currency exchange companies are instruments for money laundering. There are indications that this is also the case in Sweden.

[75] See, e.g. the Financial Intelligence Unit of Sweden's annual report 2019.

Overall assessment

The sector is diverse, and the risks can vary depending on the type of activity.

In summary, the vulnerability to money laundering in the sector is deemed to be significant (3).

Description of risk scenario including known approaches (modus operandi) to terrorist financing

- Currency exchange is deemed to be a potential way money can be used to finance terrorism. The purpose of the exchange is often to take money out of the country and to bring cash out of Sweden through the use of couriers. It is generally difficult to exchange larger amounts of Swedish kronor abroad. Therefore, the exchange to another more widely used currency usually takes place in Sweden before the money is taken out of the country by couriers. But large amounts of Swedish kronor are sometimes brought out of the country as well. The potential to use the Swedish cash thus exists, even if it appears to be limited to certain specific contexts.
- Operators that offer trading in digital currencies are used to finance terrorism in much the same way as described for money laundering. However, the purpose of using digital currencies is to conceal the recipient, to a greater extent, rather than the sender. But the approach provides a high degree of anonymity for both parties. Currency exchange businesses that are registered in Sweden are used in this context, but foreign actors and unregistered businesses are also active.

Threat – financing of terrorism

Scope, ability of the threat actor and anonymity

Currency exchange is an easily accessible service in terms of the number of offices, but to the extent that larger amounts are to be exchanged for more unusual currencies, this generally does not occur through the actors who mainly handle tourist currency. It is more likely to occur at a few niche offices that are known and trusted. In these cases, threat actors need special capacity, namely knowledge of which exchange agents can be used for this type of transaction.

As far as the trade in digital currency, these services are becoming increasingly accessible and easy to use, which is expected to increase the scope, though the threat is increasing from low levels. This applies, in particular, when exchanging to cryptocurrencies in smaller amounts. The risk associated with placing a monetary value against a fluctuating exchange rate is deemed to keep the scope low, as the purpose is only to carry out a transaction.

In terms of anonymity, the same factors are crucial for the financing of terrorism as for money laundering.

Vulnerability – financing of terrorism

Opportunity to detect terrorist financing

The same aspects described in the section on money laundering also apply to terrorist financing. Exchanges that involve small amounts of cash differ to some extent from exchanges made by tourists in terms of travel patterns and currency, but this is not always the case. Travel to an unusual destination and the use of a certain currency are, by themselves, not indicators that the exchange can be suspected of financing terrorism. This presents difficulty in terms of deciding what should be reported.

In terms of the trade in virtual currencies on registered exchanges, there is some traceability if an analysis can be made in several stages. This differs from the banking sector, as banks have banking secrecy requirements to consider. The operator has a unique overview of the entire transaction chain.

In terms of regulatory compliance as it relates to the financing terrorism, no further assessment is made other than what applies for money laundering.

7.5 Insurance mediation

Overall sector risk:

Sector

Insurance brokers are natural persons or a legal entity that serves as an intermediary on behalf of an insurance company.

General description of the sector and related products or activities

Insurance distribution is conducted by insurance brokers and is mainly regulated by the Insurance Distribution Act (2018:1219).[76] The provision of life insurance products requires authorisation. The law was updated in 2018 in connection with a new directive on insurance distribution (IDD).

The sector is characterised by many small operators, and companies usually have one to five employees. But there are also larger banks and securities companies that are authorised to act as insurance intermediaries. In much the same manner as described in the section *Life insurance,* the *Insurance distribution* sector is divided into non-life and life insurance. The analysis provided below only covers life insurance brokers.

Within the category life insurance distribution, one must distinguish between life insurance and insurance-based investment products (often endowment insurance). The same distinction also applies to the insurance companies' own distribution activities. The greatest risks of money laundering arise when distributing insurance-based investment products.

If an insurance broker distributes insurance and insurance-based investment products, an insurance company is always the contracting party for the customer. The insurance company is therefore the actual owner of the financial instruments in an insurance-based investment product. All deposits and renewals are done through the insurance company. However, the insurance broker bears initial responsibility for taking customer due diligence measures.

Life insurance brokers may not design or hold the insurance-based investment products for which they serve as intermediaries. The payment for brokered transactions does not go through the broker but through another operator who offers payment services. Unlike some other countries (for example the US), it is not possible to resell life insurance in Sweden.

---

[76] Read more at www.fi.se/sv/forsakring/regler/forsakringsformedlare / for a complete list of the regulations governing insurance distribution, including Swedish Financial Supervisory Authority's regulations.

Key figures*	Total for entire sector
Number of companies	716**
Companies' turnover	SEK 36,058,468,638
Companies' balance sheet total	SEK 41,387,010,481
Number of employees	2,490
Number of established business relationships	890,738
Total Number of natural customers	**738,179**
Total number of legal customers	**370,456**

* All data in the table were obtained from the Swedish Financial Supervisory Authority's periodic reporting for money laundering, report F880, with a reference date of 31/12/2019.The table may therefore contain data that differ to some extent from the current situation.

* * The number of authorised legal entities will soon increase due to the restructuring of one of the largest brokerage firms. The number of licenses for natural persons will decrease for the same reason.

Money laundering – description of risk scenario including known approaches (modus operandi)

- Business relationships that include intermediaries are the main risk scenario. These relationships can present an increased risk due to a lack of customer due diligence measures. The savings products can also be purchased by customers who intend to use them somewhere in the money laundering chain. Initial customer due diligence measures must be performed by the intermediary (broker) in the business relationship. However, the majority of brokers in the sector are smaller actors and small companies, which are generally less able to carry out effective customer due diligence measures than the larger actors. For example, smaller brokers have less access to system support for screening PEP/sanction lists.
- The risk scenario is also amplified by a conflict of interest that characterises the sector. The conflict concerns the commission that the broker receives from the life insurance company for brokering a transaction. An effective customer due diligence process would likely result in more denied transactions. Therefore, the financial incentives for a smaller broker – where each individual transaction has an impact on profitability – can lead to sacrifices in the customer due diligence process. This is also assessed to increase the risk of abnormal or suspicious transactions (promotion of layering and integration). For example, this might be a larger deposit for a life insurance savings product just before retirement.
- The risk scenario also includes the risk that the life insurance company will rely on the broker's initial customer due diligence measures. This can have a negative impact on the quality of the company's own customer due diligence measures and the subsequent monitoring of the business relationship.

Threat

Scope

The threat profile in the sector is similar to the threat profile described in the section *Life insurance business*. The sector's products normally have a low turnover rate, and the products often have provisos attached that prevent or make early repurchases impossible. Repurchases can be a modus operandi for money laundering. It is assessed that money laundering does not occur to a large extent in the sector, but the volume of money that can potentially be laundered is high.

Capacity of threat actors

Threat actors need to have some knowledge of the products in the sector as well as the ability to plan money laundering schemes. These factors reduce the accessibility of life insurance products for threat actors. They also reduce the attractiveness of using life insurance products – including distributors – for the purpose of money laundering. The threat profile is considered to be slightly enhanced when savings products are sold through insurance distributors. The reason for this is that these operators do not have the same ability to carry out initial customer due diligence measures as the larger life insurance companies.

Anonymity

It is difficult to operate anonymously in the sector.

Overall assessment

The sector's products normally have a low turnover rate, and the products often have provisos attached that prevent or make early repurchases impossible. Threat actors need to have knowledge of the products and the ability to remain anonymous in the sector is limited. It is assessed that money laundering does not occur to a large extent, but the amount of money that can potentially be laundered is large.

In summary, the threat of money laundering in the sector is considered to be moderate (2).

Vulnerability

Ability to detect money laundering

The transaction speed in the sector is relatively slow, and the sector is not exposed to cash. The transactions are mainly domestic in character, and the distribution of foreign endowment insurance to Swedish consumers only occurs to a limited extent. Traceability is generally considered to be good. As a whole, the exposure to the risk of money laundering in the life insurance sector is primarily linked to deposits, savings and repurchases of the sector's savings products via custody account insurance – risks that are not generally managed by the insurance distributors. The distributors' exposure to risk is primarily linked to the initial customer due diligence measures.

The risks for money laundering in the life insurance sector are mainly linked to deposits, savings and repurchases of the sector's savings products via custody

account insurance. These risks are not generally managed by the insurance distributors. The distributors' exposure to risk is primarily linked to the initial customer due diligence measures.

Regulatory compliance

Risk awareness and organisational conditions vary widely between different insurance distributors. In the case of smaller brokers in the sector, conditions are considered to be poor when it comes to the level of risk awareness and adequate system support. In the case of independent brokers, the conditions are deemed to be significantly worse. Some of the independent brokers receive some support from partners, which reduces the risks to a certain extent. Larger actors in the sector usually have stronger control functions and better understanding of the regulations than smaller actors. This is also reflected in the quality of money laundering risk management. In the case of InsureSec licensing or certification of insurance brokers, for example, knowledge requirements are set for parts of the money laundering regulations.[77]

There are inherent conflicts of interest linked to the sector's remuneration models. This could lower the incentives to strengthen the conditions for the distributor's risk management.

The number of money laundering reports submitted to the Financial Intelligence Unit of Sweden (Fipo) for the years 2018/2019 may indicate a certain degree of under-reporting.

Overall assessment

The transaction speed in the sector is relatively slow. The sector is not exposed to cash. Transactions in the sector are mainly domestic in character, and traceability is generally deemed to be good. Risk awareness differs between operators.

In summary, vulnerability to money laundering in the sector is assessed as moderate (2).

Risk – financing of terrorism

There are currently no known scenarios in which the sector is used to finance terrorism within the framework of the national risk assessment. Therefore, the risk of terrorist financing in the sector has not been assessed.

[77] Through regulations, disciplinary boards and criteria for knowledge and competence, InsureSec aims to increase the quality and customer value of the advisory services offered and insurance distributed in Sweden.

7.6 Issuance of electronic money

Overall sector risk:

Sector

Electronic money is an electronic store of monetary value as represented by a claim on the issuer. These monetary values are issued in exchange for funds for the purpose of carrying out payment transactions in accordance with the Payment Services Directive (2010:751) and are accepted as a means of payment by entities other than the issuer.

General description of the sector and related products or activities

In order to issue electronic money, authorisation from the Swedish Financial Supervisory Authority is usually required in accordance with the Electronic Money Act (2011:755). Banks and credit market companies are permitted to issue electronic money under their existing licenses.

The Electronic Money Act does not apply to certain electronically stored funds. This concerns funds that can only be used among a limited network of suppliers, in a supplier's place of business or when it concerns a limited range of goods or services, i.e. gift cards and similar products.

The law also does not apply to funds used for certain payment transactions. These are transactions carried out using equipment for telecommunications, digital technology or information technology, when the goods or services to be purchased are delivered and intended to be used with such equipment. This applies provided that the operator of the equipment does not act solely as an intermediary for the payment service user and the supplier of the goods or services.

If the average amount of electronic money issued exceeds EUR 5 million or the equivalent, authorisation is required to act as an electronic money institution (EMI). If the value issued is less than EUR 5 million, the issuer can apply for an exemption from the authorisation obligation and act as a registered issuer. An institution for electronic money or a registered issuer may also provide payment services in accordance with the Payment Services Act (2010:751). The prerequisites for the Swedish Financial Supervisory Authority to grant authorisation or an exemption from the authorisation obligation to issue electronic money are set out in the Electronic Money Act and the Electronic Money Ordinance (2011:776).

Electronic money is primarily issued in two forms: hardware-based products and software-based products.[78] Hardware-based electronic money is stored on a physical product (such as a card) and is transferred from sender to receiver through

[78] www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html (retrieved 14/02/2021).

a device reader, such as a card reader. An internet connection is generally not required to transfer this money. Software-based electronic money, on the other hand, is stored on a personal device such as a computer or a smartphone, and an internet connection is therefore required to transfer these funds.

Unlike payment services, for example, an issuer of electronic money may store received funds. This can be prepaid cards (sometimes called electronic purses), for example, where funds are stored to make purchases at a later date.

The majority of electronic money institutions in the EU are based in a few countries (UK, Belgium, Czech Republic, Denmark, Latvia and the Netherlands).[79] Sweden is home to three electronic money institutions. However, electronic money institutions can also conduct cross-border activities in Sweden. This is comparable to payment institutions and registered payment service providers.

Foreign companies within the EEA that are authorised to issue electronic money in their home country do not need authorisation from the Swedish Financial Supervisory Authority to issue e-money or offer payment services in Sweden. On the other hand, actors who conduct cross-border activities in Sweden without having a branch or agent in the country must be registered in the Swedish Financial Supervisory Authority's register. This can occur once the Swedish Financial Supervisory Authority has received a notification from the actor's home country. There are currently about 200 foreign electronic money institutions – with cross-border activities – in the Swedish Financial Supervisory Authority's register. The sector in Sweden consists almost exclusively of one company. This company accounts for the majority of the key figures presented below.

Key figures*	**Total for entire sector**
Number of companies	6
Companies' turnover	SEK 13,724,655,409
Companies' balance sheet total	SEK 24,247,492,843
Number of employees	2,187
Number of established business relationships	994,978
Total Number of natural customers	**638,995**
Total number of legal customers	**355,974**

* All data in the table were obtained from the Swedish Financial Supervisory Authority's periodic reporting for money laundering, report F880, with a reference date of 31/12/2019. The table may therefore contain data that differ to some extent from the current situation.

* * The number of authorised legal entities will soon increase due to the restructuring of one of the largest brokerage firms. The number of licenses for natural persons will decrease for the same reason.

[79] SWD 2019(650), p 72.

Money laundering – description of risk scenario including known approaches (modus operandi)

- Several foreign electronic money institutions that target Swedish customers offer customers the ability to transfer funds through web-based or mobile applications. This can, for example, be a transfer from a bank account to a holder of reloadable debit cards and issued by the institution or a third party. This allows criminally acquired money to be transferred between different individuals and companies and then used, for example, for card payments and ATM withdrawals. Cross-border transactions and currency exchanges are also possible with these services. Some agents also offer transfers, trading and purchases with cryptocurrencies.
- Taken together, this decreases traceability and thus entails an increased risk of money laundering. There are also foreign electronic money institutions that provide anonymous, prepaid cards. The prepaid cards can be bought at stores in Sweden and can be paid for using cash. They can also be used for gambling and thus constitute a potential tool for money laundering.

Threat – money laundering

Scope

In Sweden, there are only a few companies that are authorised to issue electronic money. For larger companies with authorisation, some form of business activity is often required to use the service. The accessibility of the sector for threat actors therefore reduces the risk that it will be exploited for money laundering. For other issuers of electronic money (e.g. foreign institutions that offer prepaid cards or institutions that provide virtual online currencies), the accessibility is slightly higher. This also increases the threat of money laundering.

Capacity of threat actors

Threat actors and traders who wish to make payments to other connected traders with e-money need to have some type of established business. Threat actors also need to have a certain capacity to start a business for the purpose of laundering money. No special ability is required to use prepaid cards from foreign institutions.

Anonymity

The use of cash is very limited in the sector, which reduces the threat. The ability to remain anonymous is therefore considered to be low, which reduces the threat profile. In the case of prepaid cards offered by foreign institutions, there is an opportunity for threat actors to remain anonymous and conceal assets. Prepaid cards can be loaded with a monetary value that can then be used with more limited opportunities to trace the funds than with traditional bank accounts. Transactions with these cards take place immediately and the level of anonymity is very high. This increases the threat of money laundering in the sector.

Overall assessment

Companies that conduct cross-border activities in Sweden and offer prepaid cards can increase the threat to the sector. Prepaid cards offer fast transactions and a high degree of anonymity.

In summary, the threat of money laundering in the sector is assessed as significant (3).

Vulnerability – money laundering

Ability to detect money laundering

Card transactions to and from the sector are usually completed in one or two days and cash is used to a very limited extent. These conditions, in combination with the traceability of card transactions, means that traceability is generally good in the sector. However, the ability to repurchase and send funds to an unknown account or card creates lower traceability than other types of transactions. The low traceability of prepaid cards from foreign electronic money institutions can also create a certain degree of vulnerability in the sector. As the e-money sector is fintech-intensive, there is a risk that new products and approaches can quickly develop that are suitable for money laundering.

Regulatory compliance

In Sweden, the sector consists of companies with a relatively high degree of maturity and smaller companies. Companies in the sector generally carry out good controls, set relevant variables in monitoring systems and have high data quality.

Overall assessment

The sector accounts for only a small part of the Swedish financial system, and the number of authorised or registered operators with the Swedish Financial Supervisory Authority is low. Vulnerability in the sector is increased by the presence of foreign companies that conduct cross-border activities in Sweden.

In summary, vulnerability to money laundering in the sector is assessed as significant (3).

Description of risk scenario including known approaches (modus operandi) to terrorist financing

- Foreign electronic money institutions can be used for the purpose of moving money further along in a terrorist financing chain, for example, from bank accounts to anonymous alternatives outside Sweden. The services are also used for transactions and consumption in Sweden as an option that provides a higher degree of anonymity than transactions made through a traditional bank account. The services enable transfers and consumption in an environment characterised by significantly reduced transparency than transactions made through a Swedish bank account.
- The sector is used in the same way as described for money laundering, however,

the amounts handled in this context are usually small. Nor do the threat actors primarily target operators who are primarily active in business. It is primarily operators who do not have their registered office in Sweden, but who offer their services on the Swedish market, who are targeted.

Threat – financing of terrorism

Scope, capacity and anonymity

The increased supply of e-money in the Swedish market and the availability via mobile services has increased the scope in the sector. As described above for money laundering, the services do not provide total anonymity, but are likely to provide increased anonymity compared to using a Swedish bank account. The user needs to be familiar with the use of mobile services, but beyond that, no special skills are required to use the financial solutions offered in the sector.

Vulnerability – financing of terrorism

Opportunity to detect terrorist financing

The fact that foreign operators do not take adequate customer due diligence measures with respect to Swedish customers reduces the ability to detect abnormal behaviour. The opportunity to collaborate with Swedish law enforcement authorities is also made more difficult by this situation.

The same factors that make it difficult to detect terrorist financing in other sectors also apply here as well. That is, the sector often involves individual transactions with smaller amounts of money.

7.7 Fund operations

Overall sector risk:

Sector

Fund management can be divided into two types of activities: management of mutual funds and management of alternative investment funds (AIFs). The two types are governed by an interconnected set of regulations, as the financial instruments are similar to a certain extent, and a large proportion of the fund managers have authorisation for both types. As the risks are also considered to be similar for both instruments, the two types of business are jointly reviewed in this section.

General description of the sector and related products or activities

Fund management can be divided into the management of mutual funds and management of alternative investment funds (AIFs). Special funds are separately regulated AIFs, which are generally marketed to non-professional investors.

Unlike special funds, other AIFs are primarily marketed to professional investors. However, under certain conditions, these instruments can also be marketed to non-professional investors (e.g. if the units or shares in the fund are admitted to trading on a regulated market). Examples of other alternative investment funds are venture capital funds, real estate funds and credit funds.

Unlike the management of mutual funds, which always requires a license, the management of an AIF can be subject to a registration requirement or authorisation obligation. Whether the activity requires registration or authorisation depends on how much capital the manager has under management. The regulations set out in the Alternative Investment Fund Managers Act (2013:561 – LAIF) only apply to registered managers of AIFs to a limited extent.

The fund manager's responsibilities include portfolio management and risk management. A custodian is required for both mutual funds and AIFs. The custodian shall, among other things, hold the fund's assets and monitor cash flows.

Fund management is governed by the Swedish Mutual Funds Act (2004:46) and the Alternative Investment Fund Managers Act (2013:561 – LAIF). While managers of mutual funds and special funds have long been subject to supervision in Sweden, the regulations for the management of AIFs are relatively new.

Fund activities are largely cross-border in character, particularly within the EU/EEA. A large number of funds that are marketed and sold in Sweden are based in other member states. The major managers of mutual funds and special funds – in terms of capital under management – include bank-owned fund managers. Bank-owned fund managers often manage both securities and special funds. These funds

are often distributed through banking activities. Funds can also be distributed via fund platforms. Funds are also sold via insurance companies, for example, within the framework of unit-linked/custody account insurance and through the premium pension system. Fund units can be nominee-registered, whereby the nominee is entered in the unit-holder register instead of the unit-holder.

Key figures*	**Total for entire sector**
Number of companies	230
Companies' turnover	SEK 37,368,747,773
Companies' assets under management	SEK 4,202,357,415,758
Number of employees	2,316
Number of established business relationships	1,624,410
Total Number of natural customers	**1,605,167**
Total number of legal customers	**36,204**

* The figures are a combination of mutual funds and AIFs. All data in the table were obtained from the Swedish Financial Supervisory Authority's periodic reporting for money laundering, report F880, with a reference date of 31/12/2019. The table may therefore contain data that differ to some extent from the current situation.

The table includes both AIF managers and mutual fund managers.

Money laundering – description of risk scenario including known approaches (modus operandi)

- Mutual fund managers and AIF managers fit the profile of most common risk scenarios. For example, different types of funds can be used for money laundering in situations where illegal money is layered and integrated into the financial systems. Given the fact that investment funds often handle large capital flows, these instruments can be an attractive channel for money laundering, including large-scale schemes.
- Threat actors can exploit the sector's legitimate products. For example, a threat actor may buy or sell fund units for the purpose of layering or integrating funds originating from criminal activities. If payment is then made to an account other than the account where the funds were originally deposited, funds can be used in the layering phase of a scheme. In this way, the recipient can create the appearance that the money received originated from accumulated capital gains.
- Fund transactions can also be largely cross-border in nature. This makes it very easy to invest money abroad and can make it very difficult to trace the money as well as to identify ownership structures. In cases where a fund manager and/or a fund are based outside the EEA – but has been granted authorisation to be marketed in Sweden – there may be an elevated risk of insufficient customer due diligence measures, which in turn opens the door to money laundering.

Threat – money laundering

Scope

It is assessed that money laundering does not occur to a large extent, but the volume of money that can potentially be laundered is high. Smaller funds can be at risk of money laundering. This has also been confirmed in some international risk analyses in the area (cf. family office structures as a risk factor).[80]

Ability of threat actors

In order use the sector for money laundering, certain specialised skills are required as well as access to capital. These factors reduce the risk of money laundering and make the sector less attractive to threat actors. But the same factors also contribute to higher risk, as larger volumes of money can potentially be laundered through the sector.

Anonymity

If a new fund is created explicitly to launder money, anonymity can be built in to the fund's structure as part of the scheme. However, these schemes are considered to be less common, and the overall amount laundered through the sector is therefore considered to be limited.

Overall assessment

The sector is considered to be the most attractive sector for threat actors with large amounts of capital and high levels of competence, as well as those who use complex schemes. But simpler schemes can also be carried out in the sector. Therefore, even though volumes may be high in individual cases, the overall threat profile in the sector is relatively limited.

In summary, the threat of money laundering in the sector is deemed to be significant (3).

Vulnerability – money laundering

Ability to detect money laundering

Several funds are marketed across borders, which mean that money can be easily invested abroad through the purchase of fund units. In these cases, the vulnerability is linked to foreign ownership structures with hidden beneficial owners. In addition, there are ownership structures in the sector that are complex and lack transparency. For example, the sector includes foreign trusts, which increases vulnerability to money laundering.

The use of cash is extremely rare in the sector, which contributes to good traceability. Overall, transactions in the sector are considered to be largely traceable, and that the identities of users of products and services are largely verified. However, there is a certain level of risk linked to the international part of

[80] JC 2017/37 Guidelines and Risk Factors, p 71.

the sector.

Fund-related transactions in the sector take just a few days to complete and are considered relatively easy to trace. But transactions in the more complex schemes can take longer to complete. These transactions also have reduced traceability by design, and it is therefore more difficult to trace completed transactions.

Regulatory compliance

The level of risk awareness varies within the sector. With the exception of special funds, managers of AIFs have only been subject to supervision since 2013, and this likely means that many companies in the sector have not had the opportunity to mature compared to, for example, managers of mutual funds. Reports on regulatory compliance in the sector indicate that institutions see shortcomings that are linked to companies' level of compliance. Smaller companies in the sector are not deemed to have sufficient resources to guarantee an effective control system and face the same challenges seen in other sectors in relation to poor organisational conditions (compare international risk analyses for the sector[81]). However, the bank-owned fund companies are deemed to have established risk control functions and are able to apply the systems and tools that they already use in their banking activities.

Smaller companies in the sector often rely on the banks to take customer due diligence measures for the customers with accounts in the bank who trade in the fund. As a result of this assumption, fund companies dedicate less resource to adequate customer due diligence measures.[82] There is also a risk of significant conflicts of interest, mainly among the smaller companies. The sector is dependent on invested capital, and financial interests may take precedence over regulatory compliance.

Overall assessment

A significant part of the sector consists of bank-owned fund companies, and these are considered to have adequate control systems in place. There are risks of conflict of interest in the smaller companies within the sector, and the organisational conditions to maintain an effective control function and ensure regulatory compliance are deemed to be less robust.

In summary, vulnerability in the sector is assessed as moderate (2).

Risk – financing of terrorism

There are currently no known scenarios in which the sector is used to finance terrorism within the framework of the national risk assessment. Therefore, the risk of terrorist financing in the sector has not been assessed.

81 EU SNRA, Annex, SWD (650), p 45.

82 This reasoning is also taken in the EU's Supranational Risk Assessment, see aa p. 45.

7.8 Payment institutions

Overall sector risk:

Sector

Payment institutions are operators that offer payment service activities that are subject to an authorisation obligation.

General description of the category and related products or activities

Several company types are defined as payment service providers across different sectors.[83] This section only deals with payment institutions. A payment institution is a limited liability company or an economic association that has been granted authorisation to offer payment services under the Payment Services Directive (2010:751) (LBT). In its most basic form, the core business of a payment institution is offering a variety of ways to make payments.[84]

Companies that offer payment services totalling the equivalent of more than EUR 3 million per month must have authorisation to carry out operations and are known as payment institutions in the Payment Services Act.[85] Companies with authorisation to provide payment initiation services are always considered payment institutions, regardless of their turnover.

The primary activity of a payment institution is to implement payment transactions from sender to recipient through a variety of methods. In principle, this can include everything from cash payment transfers to transfers via various forms of Internet-based services (e.g. apps). There are also related services, such as account information services.[86] Payment service providers – regardless of whether it is a bank or other payment service provider – thus provide an essential service and are necessary for the implementation of transactions. Payment service providers often offer a combination of several services that are listed in Chapter 1, Section 2 of the Payment Services Directive. For example, there is a large market for account information services and payment initiation services (often referred to as Third Party Providers (TPPs)). In addition, payment institutions and registered payment service providers can have different specialisations (e.g. the gambling industry).

A payment institution is never permitted to hold its customers' funds for an extended period of time. It is therefore not possible to deposit funds for a payment

---

[83] Ch. 1, Section 3 of the Payment Services Directive.

[84] The exception is account information services. However, only account information service providers are excluded from the scope of the Payment Services Directive.

[85] This chapter does not cover activities that involve money transfer.

[86] Operations that exclusively offer account information services are not covered under the scope of the Payment Services Directive.

institution to hold for future payments or otherwise dispose of funds.

Swedish payment institutions include a number of fintech companies. There are also a large number of foreign actors who are permitted to provide payment services in Sweden. These are regulated and are under the supervision of the Swedish Financial Supervisory Authority.

Payment institutions must have an individual authorisation for the various payment services. This means that a supplier of these services must apply for a new authorisation if they wish to add a new service.

The biggest difference between registered payment service providers and payment institutions is the size. Payment service providers are usually smaller companies that offer a specialised service. Payment institutions that have been granted authorisation by the Swedish Financial Supervisory Authority are often larger companies with a broader focus and typically offer a larger number of payment services.

Special considerations for money transfer

In a money transfer, money is transferred from a payer without opening a payment account, either in the payer's name or the recipient's name. The transfer is made solely for the purpose of transferring a fixed sum, either to a recipient or to a payment service provider acting on behalf of the recipient. Alternatively, the funds are received on behalf of the recipient and made available to the recipient. Money transfers are often used to send money abroad.

Money transfer is considered a payment service and can thus be offered by a number of different types of institutions. However, this section refers to money transfer made through payment institutions. The payment institutions that offer money transfer services in Sweden are largely foreign payment institutions that are established in the country through agents. There are four main actors who are established in Sweden through agents. There are also alternative forms of money transfer offered in the sector, such as Hawaladars.[87]

Key figures*	**Total for entire sector**
Number of companies	39
Companies' turnover	SEK 7,592,185,639
Companies' balance sheet total	SEK 15,827,000,812
Number of employees	2,620
Number of established business relationships	2,532,187
Total Number of natural customers	**2,562,613**
Total number of legal customers	**128,112**

[87] See, e.g. FATF (2016), Guidance for a Risk-Based Approach for Money or Value Transfer Services, FATF, Paris. www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-money-or-value-transfer.html, p. 11. The FATF describes money transfer as a service that sometimes has ties to geographic regions, and which can take various forms depending on the geographic location, for example through Hawala (p. 7).

* All data in the table were obtained from the Swedish Financial Supervisory Authority's periodic reporting for money laundering, report F880, with a reference date of 31/12/2019.The table may therefore contain data that differ to some extent from the current situation.

Money laundering – description of risk scenario including known approaches (modus operandi)

- Placement takes place by paying for illegal goods or services through payment service providers. The payments sometimes go to frontmen, who then transfer the money or withdraw the money so it can be handed over in cash to the UBO or other party in the transaction chain (layering).
- In addition to decreasing traceability, the products can also be part of the layering process through other applications or services. One scenario is that a threat actor uses a payment service to move money to and from online casinos, where money is won or lost between parties working in collaboration.

Special considerations for money transfer

- Criminally acquired money is laundered through payment systems in third countries. The individual sending funds channels the money to Sweden using complex payment chains that involve a large number of intermediaries and jurisdictions. This reduces the ability to trace the origin of the funds. Often, the transfer service provider involved in the payment chain also establishes formal and/or informal payment systems that further weaken traceability.
- Cash from sales in illegal activities is deposited in an individual's bank account through money transfer.
- Cash withdrawals from money transfer providers, card payments or transfers from bank accounts can be made to pay wages while avoiding paying taxes. Criminally acquired funds are placed in the financial system through the regulated money transfer providers. Cash deposits of criminally acquired funds can, for example, be sent to bank accounts with recipients in Sweden or abroad. Threat actors can also use regulated money transfer providers to channel their funds and place and/or transfer money through money transfer services. The risk of money laundering can be especially high when transferred funds are received in cash.
- When money is able to be deposited, it becomes more difficult to trace. This is either done by frontmen or by making structured deposits. In these cases, the deposits are kept within certain amount limits to avoid the need for stricter identity verification.

Threat – money laundering

Scope

Payment services are used to a relatively large extent, partly for providing payment for illegal goods or services and partly for layering.

The sector is frequently used for the purpose of money laundering, and organised crime networks are known to use money transfer services as a part of a larger

scheme. The risk of money laundering is increased as part of the modus operandi is to carry out multiple, smaller transactions and to send money to several recipients. Given the high frequency, the volume of money laundered is also considered to be high.

Ability of the threat actor

The payment services themselves are often developed by fintech companies and are specifically developed to be easy to use. Therefore, users do not need to have any special prior knowledge. In addition, payments and transfers are often completed very quickly, which makes the sector more attractive for money laundering.

In terms of money transfer, it is easy to use the sector as part of a money laundering scheme (layering). No special knowledge is required. Transfers can be made almost immediately.

Anonymity

The opportunity for users to remain anonymous is relatively low. Due to the difficulty remaining anonymous, threat actors therefore often use strawmen to carry out transactions in one or more stages. This complicates the ability to trace the origin of the funds.

Regarding money transfers; there are indications that threat actors use fake identification documents. At the same time, some money transfer agents lack the ability or willingness to carry out accurate identification verification. This increases the ability of threat actors to remain anonymous in the sector. In addition, operators only need to take customer due diligence measures for transactions that individually or collectively exceed EUR 15,000 (unless it is a business relationship). Threat actors can therefore make structured money transfers within certain amounts to reduce the risk of detection and reporting. This opportunity is deemed to increase the threat of money laundering in the sector.

Overall assessment

The sector's exposure to criminal actors is considered to be relatively high. This occurs, for example, when companies offer payment service solutions over a broad area. In several cases, the business is focused on specific, high-risk industries, such as online casinos. The sector also includes money transfers, which are frequently used as part of money laundering schemes.

In summary, the threat of money laundering in the sector is assessed as significant (3).

Vulnerability – money laundering

Ability to detect money laundering

The volume and share of international flows in the sector differ significantly between different payment service providers. In the case of companies that have collaborations with, for example, online casinos, the proportion of international flows is considered to be high. But for other companies in the sector, international

flows only occur on a smaller scale.

Due to the use of digital business models in the majority of companies, cash is used to a minimal extent. Considering the use of digital solutions and identification requirements, the traceability of transactions is deemed to be good.

For certain services, it is more difficult for the institution receiving the payment (e.g. a bank) to obtain information about who initiated the payment. Such a risk may arise when the payment has been initiated by a representative of the TPP who delivers the payment file. In this example, the bank can see that the payment is coming from the TPP. However, the bank is unable to see if the payment has been initiated by an agent, which would mean that the payment should be treated as high risk. In this way, the receiving party's risk exposure can be minimised, and customer due diligence measures and transaction monitoring become more difficult.

In addition, some companies in the sector have a cash-intensive business. This primarily applies to secure logistics suppliers, which increases the vulnerability to money laundering. For several of the payment services, transactions can be implemented immediately, while for other solutions (e.g. international payment transactions), it can take one or more days before the transaction is completed.

Another factor that increases the vulnerability to money laundering is that a number of payment institutions offer their products and services through agents or collaborative business applications. The payment institutions are the party that needs to ensure (through their handling of third-party risks) that the agents comply with the payment institution's AML requirements and the regulations for money laundering. The fact that this does not happen to a sufficient extent is considered to be a risk.

In the case of money transfers, these transactions include a high volume of cross-border transactions that often go outside the EEA. It is common for customers to use cash, and traceability is limited. The threshold provision in the Anti-Money Laundering Act also means that the likelihood of identifying the UBO is low.

Hawala transfers are completed very quickly, as no actual transactions are made when the order is placed. The transfer instead takes place between the actors within the Hawala network. The traceability within these networks is therefore poor.

Regulatory compliance

Risk awareness varies significantly between companies in the sector. Some companies in the sector have operational risk analyses and good documentation, which indicates good awareness and knowledge of the regulations. Most of the other actors use more generic documentation. Here, there is a high degree of uncertainty in the practical implementation, which indicates poorer awareness or knowledge. The general risk assessments of companies in the sector often do little to address the risks associated with money laundering and terrorist financing.

There are several companies in the sector that can be considered fintech companies. These companies usually have a strong focus on growth, digital solutions and low costs. There is therefore an inherent risk that these companies

have not allocated the resources necessary to put adequate control functions and processes into practice.

In their periodic reporting to the Swedish Financial Supervisory Authority, the operators report that only a small proportion of their customers are legal entities.[88] However, it has been discovered during supervision that payment service providers had a higher proportion of legal entities than what the operators reported. The discrepancy is believed to be the result of the way cooperation agreements with legal customers are counted regarding payment initiation solutions. In these cases, a natural customer is usually the end user. Payment services are mainly used by natural customers. However, a number of companies in the sector have not done a thorough analysis of who their customers are. If the companies do not know who their users are, there is a risk that customer due diligence and transaction monitoring will also fall short.

There are deficiencies in the management of AML risks in the sector. For example, it has been noted that companies in the sector have used generic risk analyses and process documents, often based on templates through the Swedish Anti-Money Laundering Institute (Svenska institutet mot penningtvätt – SIMPT). Furthermore, there are also indications that for some operators, AML processes are not fully implemented in their operations, or that the processes are difficult to implement in practice.

Risks and control systems vary significantly between companies. The companies that can be classified as fintech companies usually have automated business models with low or no reliance on manual processes and decision-making for individual transactions.

Money transfer services include agents working on behalf of foreign payment institutions. Often, companies have policies and IT systems in place at the group level, but the agents may not have sufficient knowledge of risks and the necessary customer due diligence measures. When a company's business activities are conducted through agents, it also becomes more difficult to maintain an effective control function, which also applies to facilitators.

Many agents are small and often locally based, and the reporting of suspicious transactions to the payment institutions or the Financial Intelligence Unit of Sweden (Fipo) is done by staffs that come in direct contact with customers. Given that there are customers in the sector with a high capacity for violence, there is a risk that operators will fail to report suspicious transactions due to fear of retaliation. Taken as a whole, this increases the vulnerability to money laundering. There are also many smaller actors in the sector who are more likely to depend on recurring transactions.

Overall assessment

The vulnerability to money laundering in the sector differs depending on the type of activity. Parts of the sector are cashless, and the traceability of transactions is

[88] Self-reported data, periodic reporting F880, 2018

assessed as good due to the use of digital systems and identification requirements. However, the sector is also characterised by cross-border transactions and exposure to high-risk sectors, such as online casinos. The sector also includes operators that provide money transfer services, which is deemed to increase vulnerability to money laundering in the sector.

In summary, vulnerability to money laundering in the sector assessed as significant (3).

Description of risk scenario including known approaches (modus operandi) to terrorist financing

A known approach for money transfer is to use a large payment institution for funds that may later be suspected of financing terrorism. The entire terrorist financing chain is rarely completed in the sector, but the crucial link – getting money out of Sweden and to or near a conflict zone – can be made through payment institutions. It is usually possible to carry out cash transactions, which do occur to a certain extent in the sector and create difficulties for authorities when they attempt to trace the transaction chains. It is also common that the money that is transferred in the sector is withdrawn from an account via a card purchase.

Hawaladalars also operate in the sector, which are well suited to exploitation for the financing of terrorism. The sector also provides good opportunities to carry out transactions anonymously and to send money to conflict zones. Hawaladalars also make it possible to transfer money to jurisdictions that are subject to sanctions and do not have agents for the larger payment institutions, as well as to war zones with a lack of electrical and technical infrastructure.

Threat – financing of terrorism

Scope and capacity of the threat actor

The payment institutions' services are easily accessible, and the sector includes a large number of agents with a wide geographical spread. The services offered can be accessed via the internet, but this requires the use of some form of payment solution, which increases traceability to varying degrees. The services are considered to be reliable and easy to use with broad geographical reach across the world. Therefore, it is possible to send money to a large number of countries, many of which are in war zones. Since the services offered by large payment institutions essentially operate according to the same principles throughout the world, they are perceived to be easily accessible even when travelling between countries. This is also a characteristic that can potentially be exploited in terrorist financing scenarios. Similar to money laundering, no special abilities are required to use the sector's services.

Anonymity

Recipients are largely able to remain anonymous, as it is not possible to verify the identity of the person who collects the money, and in the context of terrorist

financing, it is the recipient that is the crucial party. False identification information is often provided when the money is sent so that the transaction cannot be traced to the right person. The local representative is ultimately responsible for carrying out proper identity verification, but this does not always happen for a number of reasons. The ability to send cash and settle accounts without thorough identity verification creates opportunities for anonymity.

Vulnerability – financing of terrorism

Ability to detect terrorist financing and regulatory compliance

The problems that apply to the sector described in the money laundering section are also relevant for terrorist financing. As many payment institutions conduct operations across the globe, they generally have a good overview of international transaction flows and the ability to detect abnormal flows or flows that match the modus operandi in a terrorist financing scheme. These institutes can help identify recipients of international significance that national authorities cannot identify based on the information they have access to. This is because the information only relates to transactions to and from the relevant jurisdiction. However, payment institutions currently understand their reporting obligation to mean that they can only report transactions to and from the relevant jurisdiction and not take responsibility for the entire intelligence picture.

In the case of money transfers, the difficulty is largely about distinguishing between suspicious transactions and legal transactions sent to relatives and families in conflict zones, as these may fit the profile of terrorist financing in terms of the recipient country and amount. The ability of large payment institutions to get an overview of global patterns should make it somewhat easier to make this distinction.

7.9 Registered payment service providers

Overall sector risk:

Sector

Registered payment service providers are institutions that offer payment services according to the definition in Chapter 1, Section 3, third paragraph of the Payment Services Directive (2010:751) (LBT), but which have been granted an exemption from the authorisation obligation pursuant to Chapter 2, Section 3 of the same directive.

General description of the sector and related products or activities

An entity that conducts payment services with a turnover exceeding the equivalent of EUR 3 million per month must hold authorisation to conduct payment service operations and is referred to in the Payment Services Directive (2010:751) as a payment institution. An entity with a turnover less than this amount may apply for an exemption from the authorisation obligation and is referred to as a registered payment service provider.[89] The same applies to entities that exclusively offer account information services. An entity that provides payment initiation services must always be authorised as a payment institution, regardless of turnover. The rules laid out in the Payment Services Directive apply to registered payment service providers, but only to a limited extent.

A registered payment service provider is largely similar to a payment institution. The difference between the two is partly the turnover and applicable regulations (as mentioned above), and partly that a registered payment service provider is not permitted to provide payment initiation services.[90]

Money transfer is also a payment service covered under the scope of the Payment Services Directive. The description given in the *Payment Institutions* section also generally applies to money transfer providers who are registered payment service providers. There are also alternative forms of money transfer offered in this category, such as Hawaladars. Currency exchange companies offering card payments also fall into this category.

[89] CHAPTER 2, Section 3 of the Payment Services Directive (2010:751 – LBT).
[90] Ibid.

Key figures*	Total for entire sector
Number of companies	40
Companies' turnover	SEK 797,954,111
Companies' balance sheet total	SEK 203,133,396
Number of employees	206
Number of established business relationships	219,250
Total Number of natural customers	**209,805**
Total number of legal customers	**2,693**

* All data in the table were obtained from the Swedish Financial Supervisory Authority's periodic reporting for money laundering, report F880, with a reference date of 31/12/2019. The table may therefore contain data that differ to some extent from the current situation.

Money laundering – description of risk scenario including known approaches (modus operandi)

- Risk scenarios for this sector are largely similar to the risk scenarios described in the analysis for *Payment institutions.*

Threat – money laundering

The threat analysis generally corresponds to the threat analysis for the *Payment Institutions* sector. For a detailed explanation of the reasoning behind the assessment, please refer to this section.

In summary, the threat of money laundering in the sector is assessed as significant (3).

Vulnerability – money laundering

This sector describes only the sector-specific vulnerabilities that differ from the Payment Institutions sector. For a more detailed explanation of the reasoning behind the assessment, please refer to the vulnerability analysis in this section.

Special considerations for money transfer

Money transfer companies are relatively small, and they often offer money transfers only as an ancillary service. This means that knowledge of money laundering regulations is lacking in the sector. A large proportion of actors in the sector provide services without being registered. This creates a significant degree of vulnerability for the sector to be exploited for money laundering.

Overall assessment

The sector is characterised by a lack of traceability and includes unregistered actors who offer money transfer services.

In summary, vulnerability to money laundering in the sector is assessed as significant (3).

Description of risk scenario including known approaches (modus operandi) to terrorist financing

With a few additions, the same risk scenarios that apply for payment institutions also apply for payment service providers. The factors described in the threat analysis are also likely to affect the scope.

One additional risk scenario concerns payment service providers, both registered and unregistered. Some of these deficiencies result from a deliberate lack of reporting and insufficient customer due diligence measures, which contribute to the failure to systematically examine and detect suspected terrorist financing. This tends to occur among individual registered payment service providers but is not believed to be systemic.

Another risk scenario is the use of Hawala transactions for the purpose of financing terrorism. For example, Hawala offers the opportunity to transfer money to jurisdictions that are subject to sanctions, where the larger payment institutions have no agents for this very reason. Hawala can also be used to transfer money to war zones with a lack of electrical and technical infrastructure. These factors make the Hawala system the only option when transferring funds to certain regions. The Hawala system is described in more detail in section three.

There are both registered and unregistered Hawaladalars active in the sector, and these services are used for the purpose of financing terrorism for the same reason as described for payment institutions.

Threat – financing of terrorism

Scope, ability and anonymity

The same factors that apply for payment institutions also apply for payment service providers, to a certain extent. However, a crucial difference is that the smaller payment service providers do not have the same global accessibility and coverage, which affects the scope in terms of the lower number of transactions in the sector. On the other hand, the scope of unregistered payment service providers, or those who do not report in accordance with their statutory obligations, is considered to be greater for registered payment service providers than for payment institutions.

In order for threat actors to be able to exploit the smaller payment service providers who deliberately fail to report, they need to have knowledge and established trust capital. In other respects, the capacity needed for threat actors to carry out transactions is the same for payment institutions. It is known that certain payment service providers are deliberately targeted in the sector. These providers are perceived to be safe targets in terms of not reporting transactions, which also affects the ability to remain anonymous.

Vulnerability – financing of terrorism

Ability to detect terrorist financing and regulatory compliance

Vulnerability is assessed to be equivalent to the vulnerability for money laundering.

7.10 Consumer credit operations

Overall sector risk:

Sector

Consumer credit businesses that issue or broker loans or lines of credit to consumers.

General description of the sector and related products or activities

The sector can be divided into two main categories: companies that issue loans or lines of credit to consumers and brokers of these products.

The first category offers loans where collateral is normally not required for the loan (unsecured loans). The loan application is often done through the company's sales channel over the internet. It is usually a fast process to apply for a loan and get funds paid out. Payment-free months and the option to extend existing loans are sometimes offered. In recent years, a number of regulations have entered into force, which aims to strengthen consumer protection. For example, certain requirements have been increased in relation to the companies' credit assessment process.

The second category consists of operators who broker the above-mentioned products to consumers. Some of the companies offer a service where the customer's loan application is forwarded to a number of different lenders. The customer is then able to choose from the lenders that have approved the application and offered loans. Brokers often do not charge a fee for their services, but instead receive a commission from the creditor. Some companies only serve as brokers for a single lender. There are also companies with another primary business activity (e.g. sales of consumer products) that also broker unsecured loans.

In order to issue or broker loans to consumers, an entity must obtain authorisation from the Swedish Financial Supervisory Authority in accordance with the Certain Consumer Credit-related Operations Act (2014:275).[91] In order issue and mediate loans, a company must have authorisation for consumer lending and consumer credit brokerage.

[91] Licenses are not required for companies that already hold a license under the scope of a) the Banking and Financing Business Act (2004:297 – LBF), b) the Payment Services Directive (2010:751 – LBT), c) the Electronic Money Act (2011:755) or d) the Mortgage Business Act (2016:1024).

Key figures*	Total for entire sector
Number of companies	74
Companies' turnover	SEK 6,129,206,691
Companies' balance sheet total	SEK 12,827,629,774
Number of employees	1,812
Number of established business relationships	1,274,507
Total Number of natural customers	**1,910,447**
Total number of legal customers	**98,822**

* All data in the table were obtained from the Swedish Financial Supervisory Authority's periodic reporting for money laundering, report F880, with a reference date of 31/12/2019. The table may therefore contain data that differ to some extent from the current situation.

Money laundering – description of risk scenario including known approaches (modus operandi)

- A private individual is very likely to be able to get unsecured loans paid into their account in a short period of time. The money paid into the account can then be used for the purchase of capital goods or for other types of investments. By paying off loans with money from criminal activities (integration), the money can be laundered. Loans can be taken out from several different lenders at the same time, and in some cases, loans may be repaid by persons other than the borrower. The purpose of using different lenders may be to increase the amount of money that is integrated, but it may also reduce the risk of detection, as this strategy avoids large payment flows with one and the same lender or via the bank where the borrower has his/her main accounts. Loan disbursement documentation can also be used to show that the origins of larger amounts of transferred money are legitimate (legitimisation of money holdings).
- Typically, a private individual is granted an unsecured loan and has the amount paid into his or her bank account, or the person is granted a line of credit and transfers the credit amount to his or her bank account. Here, the money laundering strategy is the same as the previous modus operandi. Laundering occurs partly through monthly repayment of the loan with money acquired through criminal activities, and partly through the use of the borrowed funds to purchase durable goods (e.g. cars, watches, motorcycles). The goods are subsequently sold, and the purchase thus gains the appearance of legitimacy in the threat actor's bank account, as he or she can show that the money originated from a sale.

Threat – money laundering

Scope

Products in the sector are considered to be easily accessible. It is often a quick process to secure a line of credit or a loan, as applications are completed via the internet and signatures can be provided through BankID. Transfers and

withdrawals can sometimes be made immediately, which attracts threat actors who want to transfer money quickly. The volume of money that can be laundered in the sector is not significant, as credit institutions apply a certain loan-to-value ratio. This means that many threat actors are likely to choose another sector to implement the actual money laundering stage of the scheme.

Capacity of threat actors

No special capacity is required to conduct money laundering in the sector. However, one obstacle can be the credit assessment that credit institutions must perform before loans or credit can be granted. Even if a threat actor's own financial situation is not adequate to pass a credit check, there is a risk that false documents will be used to improve the chances of passing the credit check. Information in public registers (e.g. the statement of income and tax deductions from the Swedish Tax Agency) can also contain false information and make it easier to secure loans based on this information. Another approach is to use a strawman with a good credit rating to take out the loan, after which the threat actor repays the loan to the strawman.

Anonymity

Threat actors can remain anonymous by using strawmen and hijacked identities. Since identity verification and the signing of loan and credit agreements can be done using BankID, there are good opportunities for the threat actor to conceal his or her identity by using another person as a strawman.

Overall assessment

The products offered in the sector are easily accessible and threat actors do not need special capacity to conduct money laundering in the sector. Threat actors also have opportunities to remain anonymous. However, the volume of money that can be laundered in the sector is not significant, and there are no indications that the sector is being used to a significant extent to launder money.

In summary, the threat of money laundering in the sector is considered to be moderate (2).

Vulnerability – money laundering

Ability to detect money laundering

The sector offers digital services, which means, in practice, that cash is not handled in the sector. Applications are normally submitted using BankID, and the funds from of an unsecured loan are deposited into the customer's bank account. Based on this, the products are considered to have a high degree of traceability. Quick loans are an exception, which are loans that can also come with a certain degree of increased risk in terms of traceability.

The ability to offer a quick and easy loan process is part of the business model for both quick loans and unsecured loans. This service is often offered through credit brokers who serve as intermediaries in the loan application process on behalf of a

large number of lenders. The use of credit brokers forces lenders to process applications within a relatively short time frame. This creates incentives for lenders to adopt a lending model that uses automated processes as much as possible. This, in turn, reduces the ability to do a more through, risk-based credit check.

Regulatory compliance

The level of risk awareness varies between the larger and smaller operators. The larger lenders that provide unsecured loans and credit have a higher degree of awareness and knowledge of the risk of money laundering. The awareness level is lower among the smaller companies that offer quick loans. A number of smaller operators also tend to lack the organisational prerequisites and resources needed to ensure adequate awareness and knowledge in relation to money laundering risks.

It has also been noted that there are companies in the sector that offer consumer credit and consumer credit brokerage services without authorisation from the Swedish Financial Supervisory Authority.

Overall assessment

The traceability of transactions is generally considered to be high in the sector, with certain exceptions. As the dominant business model in the sector is to offer quick loans and access to lines of credit, the conditions for performing thorough customer checks can be reduced. Larger lenders are deemed to have a higher degree of awareness and knowledge of money laundering risks than smaller lenders that offer quick loans and credit.

In summary, vulnerability to money laundering in the sector is assessed as moderate (2).

Description of risk scenario including known approaches (modus operandi) to terrorist financing

One scenario includes the use of credit to purchase vehicles, which are subsequently driven to conflict areas, without the loan being repaid. This was a common scenario when IS was still engaged in the war in Syria.

Much the same way that credit through the banking sector can be misused for terrorist financing, consumer credit can also be misused. When purchasing an item using credit, a higher line of credit is often granted for credit cards. Credit cards make it possible to make cash withdrawals in Sweden or abroad, with no intention of repaying the borrowed amount.

Consumer credit can also be taken out in one's own name or someone else's (related party) name to finance travel to countries in or near conflict zones. Since it is possible to borrow from multiple lenders, the amounts that are borrowed can be large in comparison with the low transaction amounts that are otherwise typical in terrorist financing. Threat actors are known to then use the line of credit to leave the country with no intention of returning.

Threat – financing of terrorism

Scope, capacity and anonymity

The purchase of capital goods with the intention of bringing them out of the country to finance terrorist activities is considered to be relatively uncommon. On the other hand, the sector is known to be used, to a certain extent, to secure credit where the money that is borrowed is withdrawn abroad in cash using a credit card.

Although this scenario is uncommon, relatively large amounts of money can be withdrawn by an individual borrower, given the fact that even small amounts can go a long way to finance terrorist activities. If an individual applies for credit in his or her own name, the individual will be in debt, the case will be handed over to the Swedish Enforcement Authority and the individual will likely be reported for a crime. This reduces the attractiveness of this type of terrorist financing scheme. But legal entities are used in this type of scheme as well as different types of false identities.

Vulnerability – financing of terrorism

Ability to detect terrorist financing and regulatory compliance

As with loans secured through the banking sector, the lack of intention to repay is difficult to predict with the current system. Otherwise, the same conditions apply to vulnerability as described for money laundering.

7.11 Mortgage lending business

Overall sector risk:

Sector

Services provided by mortgage business operators include lending, credit intermediation and advisory services for consumer lenders.

General description of the sector and related products or activities

The sector can be divided into two main business categories: companies that provide loans for houses or condominiums (tenant-owner properties) to consumers and mortgage brokers. The sector mainly consists of smaller operators in the Swedish mortgage market rather than credit institutions and banks.

The first category of companies provides loans to consumers. The customer typically applies for a new loan or transfers an existing loan through the company's own sales channels or a partners' sales channels via the Internet. A number of companies in the sector have adopted a business model to challenge the major actors in the market by offering mortgages at competitive interest rates and low fees. This model is based in part on the fact that these companies can keep costs down in comparison with traditional players through streamlined organisations with fewer employees and digitised processes. The companies finance their lending in a variety of ways. For example, companies can establish mortgage funds or similar structures where financing is carried out through investors outside the banking sector, for example, insurance companies or pension funds.

The second category is mortgage brokers. Some of the companies offer a service where the customer's loan application is forwarded to a number of different players in the mortgage business. The customer is then able to choose from the creditors who have approved a loan for the customer, and the broker receives a commission from the creditor. There are also credit institutions that offer mortgages through partnerships with mortgage companies.

In order to grant or broker mortgages or advise consumers, operators must be granted authorisation from the Swedish Financial Supervisory Authority in accordance with the Mortgage Business Act (2016:1024). Separate authorisations are required for providing mortgages and brokerage services. With either of the authorisations, the company may also offer advisory services to consumers.

Key figures*	Total for entire sector
Number of companies	18
Companies' turnover	SEK 760,820,667
Companies' balance sheet total	SEK 2,529,868,921
Number of employees	630
Number of established business relationships	404,699
Total Number of natural customers	**534,818**
Total number of legal customers	**5**

* All data in the table were obtained from the Swedish Financial Supervisory Authority's periodic reporting for money laundering, report F880, with a reference date of 31/12/2019. The table may therefore contain data that differ to some extent from the current situation.

Money laundering – description of risk scenario including known approaches (modus operandi)

- Threat actors can conceal their activities and invest criminal proceeds through real estate investments. Criminal proceeds are used for deposit, repayment or early repayment in relation to the asset. A typical scenario is that the mortgage is repaid quickly and the net gain from the sale is cleaned (integration).
- Money laundering through mortgages and false certificates. In these schemes, the individuals have low taxable income that makes them ineligible for a mortgage. In the loan applications, the individual indicates that they have started a permanent job during the current year and submits an employer certificate as evidence. The companies involved can then be used to bolster the creditworthiness of people who, for example, work illegally or make their living from criminal activities. In many cases, these borrowers have relatively weak ties to Sweden. In this scenario, the companies that are indicated as employers are few in number, and many borrowers indicate the same company as their place of employment. In most cases, a home has been acquired. Interest payments and mortgage repayments have subsequently been made without a record of non-payment. The overlap with the legal sector takes place, for example, when mortgages are repaid with criminal proceeds. Another possible scenario is that borrowers are registered for the purpose of using their identities in criminal schemes.
- Employees of mortgage lenders and banks grant mortgages to criminal actors under false pretences, which may also involve bribes. This approach is often linked to a money laundering scheme where the loan is repaid with criminal proceeds.

Threat – money laundering

Scope

The assessment here is that the sector is not used for money laundering to a significant extent. As property sales occur in a series of steps, the sector is not suitable for quick money laundering and is therefore less attractive. But the potential exists to launder significant amounts in the sector.

Capacity of threat actors

In order to exploit the sector for money laundering, threat actors need to have a certain capacity; for example, they need to have their finances in order or knowledge of the product. For some approaches, threat actors also need to be able to produce complex, falsified documentation, which often involves organised crime. Third parties (frontmen) may also be involved in the schemes.

Anonymity

The ability to remain anonymous when using the sector's products is very limited.

Overall assessment

The assessment here is that the sector is not used for money laundering to a significant extent and that the approaches used by threat actors are slow in speed.

In summary, the threat of money laundering in the sector is assessed as moderate (2).

Vulnerability – money laundering

Ability to detect money laundering

The sector mainly provides loans exclusively within the Swedish housing sector. This sometimes involves cross-border funds transfers.

Operators in the market are based on the Internet, and the use of cash is not an option. In addition, the sector is only aimed at private consumers. This means that the opportunity for anonymity in the sector is considered to be low. Both the repayment of mortgages and sale of properties in the sector mean that the approaches used by threat actors are slow in speed.

Regulatory compliance

Operators in the sector are generally assessed to be aware of the money laundering risks and the companies have recently been approved by the Swedish Financial Supervisory Authority.

The Financial Intelligence Unit of Sweden (Fipo) has received few reports from the sector during 2018/2019. The explanation for this may be that few threat actors use the sector for money laundering. There are no indications that there would be threats or retaliation against employees who work in the sector or that an individual would refrain from reporting for their own personal gain.

There have been new regulations in place for the sector since 2017. The sector includes many new actors, and only a few companies are currently active. These companies have recently been granted their authorisations, which mean that the documentation has recently been reviewed and approved by the Swedish Financial Supervisory Authority. High demands are placed for lending as part of the business model, which is considered to reduce vulnerability in the sector. However, the organisations are small, which can mean increased vulnerability to money laundering, as individual officers may have broad authority. At the same time, the risk functions that carry out subsequent manual reviews may be small in scale.

Overall assessment

Traceability is deemed to be high, speed is low and operators in the sector have recently had their documentation reviewed and approved.

In summary, vulnerability to money laundering in the sector is assessed as moderate (2).

Risk – financing of terrorism

There are currently no known scenarios in which the sector is used to finance terrorism within the framework of the national risk assessment. Therefore, the risk of terrorist financing in the sector has not been assessed.

7.12 Real estate agent – full registration

Overall sector risk:

Sector

Real estate agents provide services that include brokerage, drafting documentation and valuation assignments.

General description of the sector and related services or activities

A real estate agent is a natural person who provides professional brokerage services for properties, parts of properties, condominiums (tenant-owner properties), buildings on land owned by third parties, site leaseholds, condominium titles, leasehold titles or tenancies. Brokerage refers to an activity which, through an assignment agreement, assigns a counterparty with which the client can enter into an agreement on transfer or assignment.[92] Individuals wishing to use the title real estate agent are subject to a registration obligation, though this obligation does not apply to advocates. Furthermore, the registration obligation does not apply to real estate agents who only engage in the brokerage of rental objects that are specified in the Estate Agents Act (2011:666).[93]

The title *real estate agent* itself is not protected by law. This means that anyone can call themselves a real estate agent, without being subject to the registration obligation.[94]There are actors who serve as intermediaries for objects without being registered, even though they are subject to the registration obligation. Unauthorised real estate intermediation is regulated in the Real Estate Agents Act and can result in a fine or imprisonment for a maximum of six months.[95]

Provisions regulating real estate agents' activities are laid out in the Estate Agents Act. A real estate agent shall carry out his or her assignment with due cares and in all respects observes good practice. The agent must act in both the seller's and the buyer's interests. Within the framework of the requirements set by good real estate practice, the agent shall especially consider the client's (usually the seller's) financial interests.[96] The estate agent code of conduct means, among other things, that the agent is also obliged to comply with all other applicable legislation.

In addition to intermediation assignments, a real estate agent can also help with the preparation of transfer documents, a so-called drafting assignment. A real estate agent can also be hired for the valuation of various objects.

---

92 Section 1 of the Real Estate Agents Act (2011:666).

93 Section 5 of the Real Estate Agents Act.

94 Magnus Melin, the Real Estate Agents Act. A comment, pp. 19–20, u 4:1 2017 (the author and Wolters Kluwer Sverige AB).

95 Section 31 of the Real Estate Agents Act with reference to Section 5 in the same act.

96 Section 8 of the Real Estate Agents Act.

Every real estate agent must have a client funds account. The agents' client funds accounts are primarily used for the deposit of the down payment that the buyer pays in connection with the purchase of properties or condominiums (tenant-owner properties) for which the agents serve as intermediaries. It is very common for agents to take assignments that involve handling the down payment by depositing it in the agent's client funds account.[97]

Key figures	Total for entire sector
Turnover in the sector	SEK 10,763,000 thousand *
Number of registered real estate agents	7,027**
Sales (housing market)	SEK 440 billion***
Sales (commercial properties)	SEK 200 billion****

* Turnover in the sector, 2018. UC Industry Report Real Estate Agents 2019:2 Total operating income.

** The Swedish Estate Agents Inspectorate (FMI) real estate agent register as of 31 January 2020.

*** In 2018, approximately 164,000 changes of ownership occurred in the housing market. Agents were hired for 91% of all sales in 2018 (source: Association of Swedish Real Estate Agents Information and Key Figures 2019). According to the company Svensk Mäklarstatistik, the total sales value of the housing market in the country amounted to SEK 440 billion in 2018. www.maklarstatistik.se/pressmeddelanden/bostadspriserna-uppat-under-2019/.

**** The sales figure is an estimate (here, there is limited information on when the services of real estate agents have been used).

Money laundering – description of risk scenario including known approaches (modus operandi)

- The services provided by real estate agents can be part of a scheme used for the purposes of money laundering and terrorist financing. Threat actors can exploit real estate agents with or without their knowledge.
- Money is transferred via the real estate agent's client funds account. For example, schemes may include the repayment of an overpaid down payment to the same account the payment was made or to another account. A cancellation clause may be exploited for this purpose. In this scenario, the buyer backs out of the purchase and the down payment is paid back to another account.
- Property purchases may occur via a frontman to conceal the origin of the money or the identity of the beneficial owner.
- Property may be overvalued or undervalued. In cases of undervaluation, part of the purchase price can be provided separately with black money. Overvaluation, on the other hand, can allow the buyer to take out a larger mortgage, which is then paid for with criminal money.
- Agents may be engaged for drafting assignments where buyers and sellers have already made contact. The real estate agent then provides the appearance of legitimacy to the deal.

[97] Section 10 of the Real Estate Agents Act (2011:666).

Threat – money laundering

Extent

There is the potential to launder significant sums of money in the sector via the client funds account used for the transfer of the down payment. By transferring money via the real estate agent's client funds account, the account can be used to conceal the origin of the money. The down payment can amount to several million Swedish kronor for more expensive properties. Real estate transactions primarily offer an opportunity to layer or invest criminal proceeds that have already been introduced into the economic system. Cash payments are very unusual, but cash instalments can occur.

Capacity of threat actors

In order for threat actors to carry out a money laundering scheme with the knowing or unknowing assistance of real estate agents, a certain amount of knowledge is required. The reason is that the transactions generally involve large sums of money and documentation is needed for the banks to carry out the transactions.

Anonymity

Traceability in the sector is high, as all transactions take place via bank transfers. However, the real estate agent cannot see who the money is coming from, and some agents do not always check.

Cross-border transactions are very unusual in the sector, but international flows to the sector do occur. International flows of funds can facilitate the threat actor's ability to remain anonymous, as the real estate agent does not have insight into the origin of the money.[98]

The sector can be exploited for money laundering by both natural persons and legal entities, but the vast majority of customers are natural persons. It is possible to use strawmen or straw buyers so the true buyer can remain anonymous, but buyers typically want the asset – which is often long-term – in their own name.

Overall assessment

There is the potential to launder significant sums of money in the sector via the client funds account. There are indications that threat actors use real estate agents to layer or invest money that has already been introduced into the economic system.

In summary, the threat of money laundering in the sector is assessed as significant (3).

[98] This relates to the fact that the broker does not have insight into the origin of the money. This is because the banks require a Swedish bank account and the agents do not see that the funds originate from another country.

Vulnerability – money laundering

Ability to detect

Risk awareness and knowledge vary within the sector but are generally considered to be low. The number of reports submitted to the Financial Intelligence Unit of Sweden (Fipo) from real estate agents is very low. The reporting to FIPO that concerns real estate transactions comes almost exclusively from the banking sector. One factor that complicates detection is that agents do not always have insight into where or from whom the transaction originates.

Regulatory compliance

In a number of supervisory cases, the Swedish Real Estate Inspectorate has identified shortcomings related to anti-money laundering measures. The overall assessment is that risk awareness among agents needs to be increased.

The low rate of reporting and relatively high profit per transaction means that there is reason to suspect that agents deliberately fail to report. The low rate of reporting may also be due to the fact that the agents are not always aware of the low threshold for reporting suspicious transactions. The agent is not required to have actual evidence that money laundering has in fact occurred; it is enough that the agent has reasonable grounds to suspect that this is the case.

Overall assessment

Risk awareness and knowledge are generally deemed to be low in the sector, and real estate agents do not always know where or from whom a transaction originates.

In summary, vulnerability to money laundering in the sector is assessed as significant (3).

Risk – financing of terrorism

There are currently no known scenarios in which the sector is used to finance terrorism within the framework of the national risk assessment. Therefore, the risk of terrorist financing in the sector has not been assessed.

7.13 Merchants

Overall sector risk:

Sector

Merchant refers to legal entities and natural persons who engage in the professional trade in goods.

In a merchant's operations – or a part of a merchant's operations – transactions (individual or related) are carried out, or will be carried out, that will result in an amount being paid or received in cash that amounts to the equivalent of EUR 5,000 or more.

General description of the sector and related products or activities

Operators in the sector are active in a variety of industries, but the common denominator is that they often sell goods with a higher value, so-called rare goods. These activities can include the sale of motor vehicles, parts for motor vehicles, scrap and metal, jewellery, watches, coins and antiques.

Businesses in the sector include, for example, individual companies with no employees and large limited companies with several employees. The turnover for companies in the sector varies widely and depends on the conditions in the various operations; for example, turnover varies significantly when comparing a large car dealer versus a small jewellery shop.

On 31 December 2019, the Swedish Companies Registration Office's anti-money laundering register contained 616 companies registered as engaging in the trade in goods sector. There are likely a large number of operators who can be classified as merchants – and who should be covered under the scope of the Anti-Money Laundering Act – but are not registered in the Swedish Companies Registration Office's register.

It is difficult to reliably estimate how many operators conduct activities that are subject to the registration requirement but are not registered, as there is no comprehensive register of merchants.

Key figures	**Total for entire sector**
Number of companies	616
Companies' turnover	SEK 29,010,987* thousand
Companies' balance sheet total	No information
Number of employees	4516**
Number of established business relationships	No information
Total share of natural customers	**60 %**
Total share of legal customers	**35 %***

* Turnover is higher because the company form sole trader (18%) is not included.
** The number of employees is higher as the company form sole trader (18%) is not included.
*** 5% of customers are government agencies or similar.

Money laundering – known risk scenarios

- One approach a threat actor might use is to purchase goods with cash obtained through illegal activities then resell the goods. By using this approach, threat actors can show that they legitimately received the money through the sale of goods, thus explaining the origin of the money. There is also self-laundered money, where criminal funds are used for the consumption of goods for own use.
- Another approach threat actors might use is to purchase goods with cash, return the products and then ask to have the refunded money deposited into a bank account. Another example might be the purchase of gift cards with cash across several occasions. The purchase is made for an amount that is just below the limit for when operators are required to take customer due diligence measures. The threat actor can then buy an item with the gift cards without identifying himself/herself.

Threat – money laundering

Scope

Trade in goods is an easily accessible sector, which all threat actors can access. The purchase of goods with higher value, such as motor vehicles, boats and watches, can be made with cash. This allows a threat actor to illegally turn over his or her acquired funds and be able to show at a later date that the money came from a sale. Money laundering can also take place quickly in the sector, as transactions can be carried out with cash. Given the above, the extent of money laundering using the sector is assessed as high.

Ability of threat actors

Threat actors need no specialised knowledge to be able to launder money in the sector. In some extensive money laundering schemes, threat actors may need access to strawmen who buy and sell the goods.

Anonymity

Threat actors can carry out cash transactions anonymously; these transactions are therefore not traceable. In other words, threat actors can exploit the sector to launder money without a significant risk of detection. Threat actors can also use strawmen to remain anonymous.

Overall assessment

Trade in goods is an easily accessible sector that offers threat actors the opportunity to deal in cash. This means that transactions can take place very quickly while maintaining a high degree of anonymity.

In summary, the threat of money laundering in the sector is assessed as high (4).

Vulnerability – money laundering

Ability to detect money laundering

If an operator or seller reports suspected money laundering, the purchase may then be denied. This can lead to reduced income for the owner of the business or a seller who relies on a commission-based salary. This may also reduce the incentive to report suspected money laundering in the sector. Additionally, purchases and transactions in the sector usually take place through a physical meeting with the customer, which means that threat situations can arise that can make it difficult to refuse the purchase or report the customer to the Financial Intelligence Unit of Sweden (Fipo). The ability to detect money laundering in the sector is further limited by the fact that transactions are made in cash, which makes it difficult for the money to be traced to potential predicate offences.

Regulatory compliance

The awareness of risks and knowledge of the Anti-Money Laundering Act is assessed as low in the sector. The county administrative boards have discovered serious shortcomings in regulatory compliance in the course of supervision. There are a number of operators who do not complete a general risk assessment at all and have not considered all the risks that need to be assessed. It can therefore be stated that the operators generally do not understand what is required of them under the legislation regarding their obligation to assess their own operations. They also do not fully understand how their own business can be exploited for money laundering.

Overall assessment

The ability to detect money laundering in the sector is limited by the fact that it exclusively uses cash. There is also a risk that threat situations may arise in connection with the purchase of goods, as this often occurs in a physical encounter in a store. This means that out of fear, operators may refrain from taking the appropriate customer due diligence measures to minimise the risk of money laundering. The assessment also finds that operators generally do not understand the Anti-Money Laundering Act and the risks of money laundering within their own business.

In summary, vulnerability to money laundering in the sector is assessed as high (4).

Risk – financing of terrorism

There are currently no known scenarios in which the sector is used to finance terrorism within the framework of the national risk assessment. Therefore, the risk of terrorist financing in the sector has not been assessed.

7.14 Pawnbrokers

Overall sector risk:

Sector

A pawnbroker is a business that grants credit to consumers against a pledged asset that mainly consists of movable property.[99]

General description of the sector and related products or activities

Provisions on pawnbrokers are laid out in the Pawnbrokers Act (1995:100). The law contains requirements that pawn activities may only be conducted by a limited company. If a foreign company does not wish to form a Swedish subsidiary, but instead wishes to operate as a foreign legal entity, the business must be run as a branch in accordance with the Foreign Branch Offices Act (1992:160).[100] Permits may only be granted to a foreign company if it conducts operations as a pawnbroker and is under the supervision of the relevant authority in the country where it has its registered office.[101]

In order to be permitted to operate a pawn business, a permit is required from the relevant county administrative board (in accordance with the Pawnbrokers Act).[102] A permit is also required for the direct or indirect acquisition of shares in a pawnbroker, which means that the holding constitutes a qualifying holding.[103] Before a pawnbroker opens a new office, this must be reported to the county administrative boards. The county administrative boards are also responsible for examination and supervision.[104] Given the fact that pawnbrokers require a permit, the companies do not need to be registered in the Swedish Companies Registration Office's anti-money laundering register.

The activities that may be conducted by a pawnbroker are clearly defined, and it is forbidden to combine pawnbroker activities with other activities. Exceptions are made for the sale of overdue pledged pawns that have been repurchased by the pawnbroker. These pledged items may be resold by the pawnshop over the counter. There is also nothing to prevent a pawnbroker from whole or partial ownership of

---

[99] The legal definition of a pawnbroker does not exclude the traditional possibility of also pledging securities through the pawnbroker establishment. About 5% of the pawnbrokers pledged inventory comes from this type of pledging. However, this does not afford pawnbrokers the right to expand their business area into the area of the ordinary credit market companies, see Bill 1994/95:178 p. 27.

[100] Section 3, para. 2 of the Pawnbrokers Act.

[101] Section 4, para. 2 of the Pawnbrokers Act.

[102] Section 3, first paragraph of the Pawnbrokers Act.

[103] Section 23, first paragraph of the Pawnbrokers Act.

[104] Section 24 of the Pawnbrokers Act.

other companies that conduct business other than pawn activities.[105]

Key figures	Total for entire sector
Number of companies	18
Companies' turnover	SEK 535,505* thousand
Companies' balance sheet total	No information
Number of employees	216**
Number of established business relationships	No information
Total share of natural customers	**98.8 %**
Total share of legal customers	**1.2 %**

* Turnover is higher because the company form sole trader (6 %) is not included.

** The number of employees is higher as the company form sole trader (6 %) is not included.

Money laundering – description of risk scenario including known approaches (modus operandi)

- Criminal actors who have obtained objects (e.g. precious metals, precious gemstones and watches) through criminal activities can convert the objects into funds by pledging the items. An individual who pledges an item receives a pawn ticket and this is used to give the appearance that the funds were legally obtained.[106]
- Criminals can use cash – originating from criminal activities – to buy pledged goods with higher value goods, such as watches, jewellery and precious gemstones.

Threat – money laundering

Scope

The sector is considered to be relatively easily accessible to threat actors but the number of pawnbrokers is limited, and the amounts pledged in individual transactions are generally low. Therefore, money laundering is considered to be relatively uncommon and the number of reports submitted to the Financial Intelligence Unit of Sweden (Fipo) is low.

The speed of a transaction in the sector depends on the value of the goods and the amount of the pledge. The purchase of a pledged item is likely faster. It is generally considered a somewhat lengthy process to carry out money laundering in the sector. Since a permit is required to conduct activities as a pawnbroker, there are likely few actors who conduct pawn activities without a permit.

Capacity of threat actors

No special knowledge is required to pledge an item or to purchase a pledged item.

[105] Prop 1994/95:178 p. 27.

[106] Swedish National Council for Crime Prevention (Brå) p. 232.

Anonymity

It is difficult for a threat actor to remain anonymous when laundering money in the sector. It is possible to use a strawman, but the transaction can always be traced to someone. Operators come into contact with their customers in every transaction and are relatively thorough with customer due diligence measures as well as the identification of their customers, who are almost exclusively private individuals.

Overall assessment

Despite the fact that the sector is relatively easily accessible, money laundering is considered uncommon in the sector due to the level of regulation and generally low amounts of individual pledges.

In summary, the threat of money laundering in the sector is assessed as moderate (2).

Vulnerability – money laundering

Ability to detect money laundering

Risk awareness and knowledge vary within the sector but are generally considered to be good. Reporting to the Financial Intelligence Unit of Sweden (Fipo) is low, which may indicate that operators are unaware of their obligation to report suspected money laundering. Operators largely have a general risk assessment in place. They are aware that they are under the supervision of the county administrative boards and are generally responsive to the authorities' directives and orders.

Regulatory compliance

In the course of the county administrative boards' supervision, shortcomings in regulatory compliance have been noted, but no serious deviations were noted. One reason for the limited extent of reporting to Fipo may be that operators are accustomed to reporting to the police's stolen goods unit. The generally low average amount of the pledges in the sector can also be a reason for the low number of reports to the Financial Intelligence Unit of Sweden (Fipo), as there is no risk of large-scale money laundering.

In summary, vulnerability to money laundering in the sector is assessed as moderate (2).

Risk – financing of terrorism

There are currently no known scenarios in which the sector is used to finance terrorism within the framework of the national risk assessment. Therefore, the risk of terrorist financing in the sector has not been assessed.

7.15 Accounting and auditing services

Overall sector risk:

Sector

Natural persons and legal entities that professionally provide accounting and auditing services.[107]

General description of the sector and related products or activities

Accounting and auditing services include regularly recording transactions, preparing annual accounts or annual reports, preparing tax returns and serving as a tax return representative.

The titles accounting consultant and bookkeeping consultant are not protected. This means that the law does not regulate who may call themselves an accounting consultant or bookkeeping consultant. The work performed by someone with these titles is not subject to any form of supervision other than the supervision of the county administrative boards in accordance with the Money Laundering and the Financing of Terrorism (Prevention) Act (2017:630).

There are two leading industry organisations serving companies in the accounting and auditing sector: The FAR and Srf Consultants (formerly Sveriges Redovisningskonsulters Förbund (the Swedish Association of Accounting Consultants, SRF). An accounting consultant or bookkeeping consultant can choose to seek authorisation through one or both industry organisations and adhere to their guidelines. Authorisation requires certain theoretical competence, professional experience, continuing education, liability insurance, and approval of quality controls. Furthermore, operators in the sector are required to follow the Swedish standard for accounting and payroll services and the Swedish standard for accounting services.

Bookkeeping and accounting consultants have a unique insight into their customers' transactions and have the opportunity to detect suspicious transactions. These may be either transactions the customers make themselves or suspicious behaviour on the part of the customers' customers.

On 31 December 2019, the Swedish Companies Registration Office's anti-money laundering register contained 11,232 companies registered as engaging in accounting and auditing services. Among these companies, many engage in mixed business activities, which mean that accounting and auditing services only represent part of their business.

---

[107] Not covered under Chapter 1, Section 2 first paragraph of the Money Laundering and the Financing of Terrorism (Prevention) Act (017:630).

Key figures	Total for entire sector
Number of companies	8,263*
Companies' turnover	SEK 13,437,547,000**
Companies' balance sheet total	No information
Number of employees	13,685***
Number of established business relationships	No information
Total share of natural customers	**6 %**
Total share of legal customers	**93 %**

* The figure represents businesses that have stated that they exclusively engage in accounting and auditing.

Another 2,969 are engaged in bookkeeping and accounting and other activities, for example, tax advisory activities.

** Turnover is higher because the company form sole trader (33%) is not included.

*** The number of employees is higher as the company form sole trader (33%) is not included.

Money laundering – description of risk scenario including known approaches (modus operandi)

- Threat actors can exploit auditing and accounting services when they are seeking to convert illegally acquired funds into legitimate funds. Threat actors can achieve the appearance of legitimacy for illegal transactions and get false documents and invoices to appear to be legitimate by seeking the services of an operator in the sector.
- Insufficient customer due diligence measures or a lack of understanding of the customer's operations can cause operators to fail to detect transactions that should arouse suspicion for reporting to the Financial Intelligence Unit of Sweden (Fipo). Such activities include:
- Money from criminal activities is recorded as a sale and then converted into legal funds in the form of salaries and dividends.
- Legally obtained money is paid as wages for undeclared work or for private consumption.
- Money enters the company account for no reason, the company owner is asked to repay the money (the payer cites payment error) but pays to an account other than the account where the money came from.
- The operator notes a larger transaction coming into a customer's account without documentation showing where the money came from.
- Get false documents and invoices to appear to be legitimate Cross-border payments.

Threat – money laundering

Scope

The sector is the largest under the supervision of the county administrative boards.

Given that accounting consultant is not a protected title, there is a wide range of operators engaged in accounting and auditing activities, and there is a risk that unscrupulous actors will also conduct such activities. It is common for operators in the sector to have customers in sectors that are known to be more exposed to financial crime than others, for example, the construction and restaurant industries.[108]

Overall, the ability to conduct money laundering in the sector is considered high, as bookkeeping and accounting services can be an important part of a money laundering scheme. There is also a large number operators who are not represented in the figures since they are not registered in the Swedish Companies Registration Office's anti-money laundering register.

Capacity of threat actors

Some knowledge and capacity are required to be able to exploit the sector for money laundering. Threat actors are required to enter into agreements and cooperate with the accounting consultant.

Anonymity

Operators in the sector collect certain information about their customers when entering into agreements between the operator and the customer. Individual transactions can be traced, which makes it difficult to remain anonymous. Although most operators report that they carry out customer due diligence measures, a large number do not. This increases the risk that threat actors will be able to remain anonymous.

Overall assessment

Operators do not need authorisation to carry out activities in the sector, and the sector is not subject to any supervision other than that of the county administrative boards which is based on money laundering regulations. In addition, there are a large number of operators with accounting and auditing firms.

In summary, the threat of money laundering in the sector is assessed as significant (3).

Vulnerability – money laundering

Ability to detect

There are many large companies in the sector, but smaller firms and individual companies are also common. A number of operators have established long-term customer relationships and monthly contact with their customers.

At the same time, risk awareness and knowledge of the money laundering regulations are low in the sector. In 2019, only 34 reports were made to the Financial Intelligence Unit of Sweden (Fipo). This is a low figure, and reporting should occur at a higher rate than it does today. This assessment is based on the

[108] EBM 2019:690 Återrapportering Tillsammans mot brott [Feedback – Fighting Crime Together], p. 4.

fact that the sector is the largest sector under the supervision of the county administrative boards and that a large number of businesses use the services of operators in the sector.

A number of operators are unaware that they are subject to the provisions of the Anti-Money Laundering Act. This shows that in a number of cases, operators are simply not aware of the risks in the sector and how the company can be exploited in money laundering schemes.

Regulatory compliance

The county administrative boards identify deficiencies in regulatory compliance in the course of their supervisory activities. But the scope of the county administrative boards' supervision has been low in relation to the size of the sector.

Just under half of all operators in the sector report that they have performed a risk assessment of their operations. Based on the county administrative boards' observations during supervision, few operators have taken all factors into account in their risk assessments, and they do not fully comply with the legal requirements.

Overall assessment

The sector is characterised by a low level of awareness of the risk of money laundering and low awareness of money laundering regulations. The low number of reports made to the Financial Intelligence Unit of Sweden (Fipo) confirms this characterisation. It has also become evident that many operators do not take adequate or comprehensive customer due diligence measures, which increases the risk of exploitation for the purpose of money laundering. Furthermore, there are a large number of operators who are not registered in the Swedish Companies Registration Office's register and who therefore have low awareness of their obligations under the regulations and how they might be exploited in money laundering schemes.

In summary, vulnerability to money laundering in the sector is assessed as significant (3).

Risk – financing of terrorism

There are currently no known scenarios in which the sector is used to finance terrorism within the framework of the national risk assessment. The risk of terrorist financing in the sector has therefore not been assessed. However, it should be noted that there is a potential risk that false invoices could be used in a terrorist financing scheme.

7.16 Tax Consultants

Overall sector risk:

Sector

Natural persons and legal entities that professionally provide advisory services regarding taxes and fees.[109]

General description of the sector and related products or activities

The provision of advisory services on taxes and fees involves, for example, calculating and reporting taxes that affect companies, owners and private individuals as well as offering analysis, interpretation and advice regarding applicable tax rules.

FAR is an industry association for tax consultants. A tax consultant can choose to seek authorisation through FAR and thus adhere to their guidelines. The title certified tax consultant is protected. The work performed by someone with this title is not subject to any form of supervision other than the supervision of the county administrative boards in accordance with the Money Laundering and the Financing of Terrorism (Prevention) Act (2017:630).

Tax consultants have the opportunity to gain a unique insight into customers' transactions and their company structure and should have the ability and opportunity to detect suspicious transactions or suspicious ownership structures.

Key figures	Total for entire sector
Number of companies	64*
Companies' turnover	SEK 108,148,000**
Companies' balance sheet total	No information
Number of employees	82***
Number of established business relationships	No information
Total share of natural customers	**21.4 %**
Total share of legal customers	**75.1 %****

* The figure represents businesses that have stated that they exclusively engage in tax advisory activities. Another 2,817 offer tax advice and other activities, such as bookkeeping and accounting services.

** Turnover is higher because the company form sole trader (34 %) is not included.

*** The number of employees is higher as the company form sole trader (34 %) is not included.

**** Approximately 4 % of customers are government agencies or similar.

[109] Chapter1, Section 2, first paragraph (19) of the Money Laundering and the Financing of Terrorism (Prevention) Act (2017:630).

Money laundering – description of risk scenario including known approaches (modus operandi)

- Tax crime to seek taxation in low-tax countries or to avoid taxation altogether.
- Operators can be exploited to carry out tax schemes where money from criminal activities is introduced into the legitimate financial system.

Threat – money laundering

Extent

The amounts that are laundered are likely to be high on occasion. Laundering smaller sums of money through tax consultants is not profitable, as the services are relatively expensive. A tax consultant needs to have specialised knowledge of tax laws, awareness of how the Swedish Tax Agency's controls function, and which countries are strategically beneficial to move the money to. Large sums of money can be laundered through complex cross-border schemes that are difficult for authorities to investigate. However, the speed of money laundering in the sector is assessed as low. The extent of money laundering can therefore be reduced, as threat actors are likely to choose other sectors where transactions happen more quickly.

Capacity of threat actors

Threat actors who carry out money laundering in the sector likely are natural persons or legal entities with capital that they wish to have taxed favourably or not at all. Threat actors may need some knowledge of bookkeeping and the ability to create various false documents to give the impression that the money was earned legally.

Anonymity

Customer due diligence measures must be taken before a business relationship is established, but this does not always occur.
In these cases, threat actors can operate anonymously through legal entities with complex ownership structures that make it difficult for operators to identify the beneficial owner.

Overall assessment

Threat actors are likely to be individuals with large sums of money. These individuals have funds that need to be introduced into the legitimate financial system at a low rate of taxation or no taxation at all. Furthermore, threat actors likely have some competence in bookkeeping, tax law and complex ownership structures, which allows the beneficial owner to operate and remain anonymous. The sector is also considered to be susceptible to the use of facilitators, i.e. operators who are exploited by threat actors to carry out money laundering schemes.

In summary, the threat of money laundering in the sector is assessed as moderate (2).

Vulnerability – money laundering

Ability to detect money laundering

Just over half of the operators report that they take customer due diligence measures. The fact that customer due diligence and checks of customers' financial situation are not carried out on all customers increases the risk of money laundering in the sector.

Regulatory compliance

In an analysis of the sector, the county administrative boards have found that a large proportion of the operators do not implement any customer due diligence measures. This may indicate that the operators do not understand what is required of them under the law. The operators' lack of understanding of the legislation increases the risk that the sector will be used for money laundering. It may also mean that operators will not report suspected money laundering.

Overall assessment

There is a certain lack of awareness about what the law requires. This can increase the risk that the operators will be exploited for the purpose of money laundering and that they will fail to report suspected money laundering.

In summary, vulnerability to money laundering in the sector is assessed as significant (3).

Risk – financing of terrorism

There are currently no known scenarios in which the sector is used to finance terrorism within the framework of the national risk assessment. Therefore, the risk of terrorist financing in the sector has not been assessed. However, it should be noted that there is a potential risk that false invoices could be used as part of a scheme to finance terrorism.

7.17 Independent lawyers

Overall sector risk:

Sector

Professional business with an independent lawyer who is not an advocate (i.e. not a member of the Swedish Bar Association) and is not associated with a law firm.[110] An independent lawyer acts on behalf of the client and assists and plans in the execution of financial transactions.[111]

General description of the sector and related products or activities

The title oberoende jurist (independent lawyer) is not protected. This means that the law does not regulate who may call themselves an independent lawyer. The activities of an independent lawyer primarily consist of services that involve acting on the client's behalf in connection with financial transactions or real estate transactions. These services may also include assistance in planning or executing transactions (on behalf of clients) in the purchase and sale of real estate or companies. Other services may include the management of a client's money, securities or other assets; opening or managing bank, savings or securities accounts; raising the capital needed for the formation, operation or management of companies, associations, foundations or trusts and similar legal structures.

Key figures	Total for entire sector
Number of companies	187*
Companies' turnover	SEK 441,606 thousand**
Companies' balance sheet total	No information
Number of employees	375***
Number of established business relationships	No information
Total share of natural customers	**43.4 %**
Total share of legal customers	**47.6 %**

* The figure represents businesses that have stated that they exclusively engage in activities as independent lawyers. There are another 616 businesses active in the area independent lawyers and other activities, such as bookkeeping and accounting services.

** Turnover is higher because the company form sole trader (28 %) is not included.

*** The number of employees is higher as the company form sole trader (28 %) is not included.

[110] Chapter 1, Section 2, first paragraph (21) of the Money Laundering and the Financing of Terrorism (Prevention) Act (2017:630).

[111] Chapter 1, Section 4 of the Money Laundering and the Financing of Terrorism (Prevention) Act (017:630).

Money laundering – description of risk scenario including known approaches (modus operandi)

- By assisting with financial transactions, an independent lawyer may contribute to money laundering by moving illegal funds and making them appear legitimate. This can involve a number of money laundering schemes with varying degrees of complexity.

Threat – money laundering

Extent

The scope of the sector is small as it has a low number of operators. Companies are often small with only a few employees. Many of the operators also offer other services. These can include accounting and bookkeeping services as well as tax advice or company formation services. Reporting from the sector to the Financial Intelligence Unit of Sweden (Fipo) is low, both in terms of the number of reports and the amount compared to other sectors. Authorities generally have a low level of information about the sector, and it is therefore difficult to estimate the extent to which it is used for money laundering schemes.

Capacity of threat actors

A certain level of knowledge and capacity is required to be able to use the sector for money laundering, as threat actors must risk hiring an independent lawyer. The services of an independent lawyer are often less expensive than an advocate. This means that operators are either exploited or choose to help the threat actor carry out the money laundering scheme (facilitators).

Anonymity

Operators in the sector collect certain information about their customers when entering into agreements between the operator and the customer. Although most operators report that they carry out customer due diligence measures, a large number do not. This increases the risk that threat actors will be able to remain anonymous.

Overall assessment

An independent lawyer is not a protected title, and the sector is only supervised by the county administrative boards. There is also little information available about the sector as a whole. The threat level is therefore assessed as significant.

In summary, the threat of money laundering in the sector is assessed as significant (3).

Vulnerability – money laundering

Ability to detect

The awareness of risks and knowledge of money laundering regulations are assessed as low in the sector. For example, few operators report that they collect information about their customers' financial situation. This means that a significant

proportion of operators do not investigate to determine where their customers' money comes from.

Overall, operators in the sector have not taken all factors (product/service, customers, distribution channels, geographical location and other business-specific circumstances) into account in their general risk assessment. Therefore, it is assessed that many operators do not fully understand their requirements and obligations under applicable legislation.

Regulatory compliance

In all supervisory cases, the county administrative boards have discovered deficiencies in regulatory compliance. However, the scope of supervision has been low , and the number of operators who are not registered in the Swedish Companies Registration Office's anti-money laundering register is deemed to be high.

Operators report that the reason for that few reports are submitted to the Financial Intelligence Unit of Sweden (Fipo) is that there is uncertainty regarding whether suspicious transactions are in fact cases of money laundering. This shows that awareness of the threshold for reporting is generally low.

There may also be a significant number of operators who offer legal services but do not believe that they are subject to the Anti-Money Laundering Act or who do not know that they are subject to applicable laws.

Overall assessment

The sector is characterised by a low level of awareness of the risk of money laundering and low awareness of money laundering regulations. A number of operators fail to perform comprehensive general risk assessments of their operations and do not take adequate or comprehensive customer due diligence measures. Therefore, the risk that the sector will be exploited for money laundering is significant.

In summary, vulnerability to money laundering in the sector is assessed as significant (3).

Risk – financing of terrorism

There are currently no known scenarios in which the sector is used to finance terrorism within the framework of the national risk assessment. The risk of terrorist financing in the sector has therefore not been assessed.

7.18 Company formation agents and business brokers

Overall sector risk:

Sector

The sector includes natural persons and legal entities who offer services such as the formation of legal entities, the sale of newly formed limited companies and serving as intermediaries for Swedish or foreign legal entities.

General description of the sector and related products or activities

Company formation agents and business brokers offer services such as the formation of legal entities, selling ready-made companies (companies that have been started with the aim of being resold) and assignments for the purchase or sale of Swedish or foreign legal entities.

A business broker may be involved throughout the purchase or sales process, from company analysis and valuation to the preparation of a transfer agreement.[112]

The trade association Sveriges Företagsmäklares Riksförbund (SFR) serves business brokers in Sweden. A business broker can seek authorisation through SFR. For authorisation, a business broker must have a basic education in economics at the university level or equivalent education, including business administration and civil law. Business brokers must have also completed SFR's specialist training, worked as a business broker as a primary occupation for at least three years, have successfully carried out a number of company transfers and must be creditworthy.

On 31 December 2019, the Swedish Companies Registration Office's anti-money laundering register contained 906 companies registered as engaging in company formation activities.[113] However, several of these companies carry out mixed business activities. In these cases, business brokerage constitutes only a part of their operations.

[112] Company brokers also needs to comply with a variety of laws and regulations, including the Prohibition against Supply of Legal or Financial Services in Certain Cases Act (1985:354).

[113] The vast majority of the 906 companies also engage in other business. Only 1 company indicated that they exclusively engage in business brokerage and company formation. In the county administrative boards' survey, 14 companies indicated that their main business activities are business brokerage and company formation.

Key figures	Total for entire sector
Number of companies	1(905)*
Companies' turnover	SEK 326,486,000**
Companies' balance sheet total	No information
Number of employees	53***
Number of established business relationships	No information
Total share of natural customers	**52 %**
Total share of legal customers	**48 %**

* The figure represents businesses that have stated that they exclusively engage in company formation and business brokerage. An additional 905 are engaged in business brokerage and company formation and other activities.

** The figure represents the total turnover for the 14 operators who have indicated business brokerage and company formation as their main business.

*** The figure represents the total number of employees for the 14 operators who have indicated business brokerage and company formation as their main business.

Money laundering – description of risk scenario including known approaches (modus operandi)

- When transferring. Companies engaged in criminal activities are integrated into legal businesses through the purchase of established companies. This allows them to gain access to attractive customers and markets, to operate anonymously and to act through established companies with a good reputation. In the case of acquisition, money from criminal activities can be laundered and used as payment.
- In the case of company formation. Share capital comes from criminal activities. In the case of acquisition from the company founder, money is laundered by financing the purchase with money obtained from criminal activities.

Threat – money laundering

Extent

Even though there are only a few registered operators in the anti-money laundering register, it is possible to turn over large amounts of money in the sector. The purchase itself can be done through a single transaction, which means that money laundering can take place relatively quickly.

Capacity of the threat actor

The threat actor needs to have good knowledge of methods to transfer money without operators detecting abnormal or suspicious transactions. The threat actor also needs to have knowledge about company acquisitions and business valuation.

Anonymity

The business relationships are generally short-term and only occur occasionally. Cash is not handled in the sector, but there is a risk of money laundering when transferring the purchase price. If small amounts are transferred from several different bank accounts, it can be difficult to detect the origin of the money.

To reduce the risk of money laundering, operators are required to take adequate customer due diligence measures. But the majority of operators do not collect information about the customer's financial situation or information about where the money comes from. This means that there is low compliance with the Anti-Money Laundering Act in the sector.

Overall assessment

Money laundering can occur very quickly and involve large amounts of money. For more advanced money laundering schemes, the threat actor needs capabilities in several areas. The sector is deemed to be attractive to threat actors, who are able to operate anonymously through acquired businesses.

In summary, the threat of money laundering in the sector is assessed as high (4).

Vulnerability – money laundering

Ability to detect

A large number of operators carry out customer due diligence measures only occasionally, and several operators indicate that they do not always know where the money is coming from.

Most of the operators report that they have performed a risk assessment of whether the business can be exploited for money laundering and terrorist financing. In an analysis of the sector, the county administrative boards report that the risk assessments carried out by the operators in the sector do not fully comply with the legal requirements.

The Financial Intelligence Unit of Sweden (Fipo) has not received any reports from the sector. This may be partly due to the fact that company formation agents indicated another main activity, as most of them conduct business in several different areas. Many do not believe that there is anything to report. One explanation for this may be that operators are unaware of the approaches threat actors use and therefore do not recognise the risks.

Regulatory compliance

In the county administrative boards' assessment, many operators in the sector do not have adequate knowledge of the Anti-Money Laundering Act and their own obligations as operators. This assessment is based on the fact that many operators do not take adequate customer due diligence measures, do not request information about the origin of the money, or do not take into account all the relevant factors when performing a risk assessment of their activities.

Overall assessment

In the assessment of the county administrative boards, many operators do not fully understand their obligations under the Anti-Money Laundering Act. This results in an increased risk that the operators may be exploited and unknowingly contributes to money laundering.

In summary, vulnerability to money laundering in the sector is assessed as significant (3).

Risk – financing of terrorism

There are currently no known scenarios in which the sector is used to finance terrorism within the framework of the national risk assessment. The risk of terrorist financing in the sector has therefore not been assessed.

7.19 Business centres and postbox service companies

Overall sector risk:

Sector

Natural persons and legal entities who conduct businesses and offer a registered office or postal address and related services to natural or legal persons.

General description of the sector and related products or activities

The sector includes operators who offer a business address, with or without a physical office, in return for payment. Customers are usually small businesses and employees at, for example, branches without their own office.

Postbox service companies can offer "digital postboxes". This service means that incoming mail is scanned and sent to an e-mail address specified by the customer. A postbox can provide a certain level of anonymity, which is something many postbox companies promote in their marketing. Postbox companies are not subject to any form of supervision other than the supervision of the county administrative boards in accordance with the Money Laundering and the Financing of Terrorism (Prevention) Act (2017:630). As of 31 December 2019, the Swedish Companies Registration Office's anti-money laundering register contained 61 registered companies which, when registering, indicated that they operate business centres and postbox companies. Among these companies, many engage in mixed business activities, which means that the business centres and/or the postbox business only represents part of their business.

Key figures	**Total for entire sector**
Number of companies	Business centres 40 Postbox 40*
Companies' turnover	SEK 188,861,000**
Companies' balance sheet total	No information
Number of employees	114***
Number of established business relationships	No information
Total share of natural customers	**Business centres: 1.5%** **Postbox: 45 %**
Total share of legal customers	**Business centres: 96 %** **Postbox: 53,5 %****

* The figures overlap slightly as business can be conducted with both a postbox business and business centre, or just one of the two.

** Turnover is higher because the company form sole trader (21%) is not included.

*** The number of employees is higher as the company form sole trader (21%) is not included.

**** Other customers are government agencies or similar.

Money laundering – description of risk scenario including known approaches (modus operandi)

- When threat actors wish to operate anonymously, they need access to an office and post addresses that cannot be linked to them.[114] Threat actors use these in order to give the appearance that their activities are legal.[115] Therefore, there is a risk that operators who provide mailboxes and business centres can be exploited as part of money laundering schemes by threat actors seeking to operate anonymously.

Threat – money laundering

Extent

Postbox companies and business centres often appear in reports and can play a role in complex money laundering schemes. Operators in this sector are attractive and useful to threat actors. The reason for this may be that threat actors need an address in Sweden to register companies, to receive certain benefits from the state or to obtain a bank account.

Capacity of the threat actor

The threat actor does not need specialised knowledge. The threat actor can also hire a strawman who is responsible for the address.

Anonymity

The level of anonymity the threat actor can achieve depends on how thorough the operator is in his or her customer due diligence measures when evaluating the person who hires the postbox or office. The county administrative boards report that many operators do not obtain any information about the customer's financial situation. They also fail to collect information about where the customers' money comes from. False identities linked to coordinated addresses make the scheme difficult to detect.

Business relationships are mostly reported to be long-term and recurring. Contact with customers is usually reported to take place through in-person meetings, which makes it difficult to remain anonymous. Long-term relationships can also mean that money laundering is enabled for an extended period.

Overall assessment

Operators in the sector are attractive to threat actors and can be used as facilitators. This means that the operators can be part of a money laundering scheme.

---

[114] Swedish National Council for Crime Prevention (Brå) 2011:7, p. 66.

[115] Swedish National Council for Crime Prevention (Brå) 2015:22 p. 276, 2011:7, p. 133.

In summary, the threat of money laundering in the sector is assessed as significant (3).

Vulnerability – money laundering

Ability to detect

A majority of the operators claim that they have performed a risk assessment of their operations. However, the county administrative boards report that few operators have performed a risk assessment that fully complies with the legal requirements. Many operators state that they seek out information and train employees in money laundering regulations. However, as there is a general lack of knowledge of money laundering, the county administrative boards contend that the training measures are insufficient.

The Financial Intelligence Unit of Sweden (Fipo) has not received any reports from the sector.

The vast majority of operators do not believe that there is anything to report. This may be due to a lack of knowledge of the approach threat actors use, thus preventing operators from recognising the risks.

Regulatory compliance

Half of the operators indicate that they are aware of their obligations under the Anti-Money Laundering Act. At the same time, there are a number of operators who do not take the necessary customer due diligence measures, do not ask about the origin of the money, train their staff or take all risk factors into account when performing the risk assessment. This indicates that the operators do not understand what is the law requires from them.

Overall assessment

The operators are an attractive target group for threat actors and can be enablers of complex schemes where large amounts of money can be laundered. This, combined with the fact that operators do not adequately understand what is the law requires from them, do not perform assessments of their operations in accordance with the law and do not take adequate customer due diligence measures, means that the risk of money laundering in the sector is increased.

In summary, vulnerability to money laundering in the sector is assessed as significant (3).

Risk – financing of terrorism

There are currently no known scenarios in which the sector is used to finance terrorism within the framework of the national risk assessment. The risk of terrorist financing in the sector has therefore not been assessed.

7.20 Trust administrators

Overall sector risk:

Sector

Operators who engage in activities relating to services such as the administration of a trust or a similar legal structure. This applies provided that the operator's activities do not fall under the scope of Chapter 1, Section 2, Paragraph 1(17–21) of the Money Laundering and the Financing of Terrorism (Prevention) Act (2017:630).

General description of the sector and related products or activities

Within a trust, an individual manages a property on behalf of someone else. A trust is a legal structure where the founder's ownership is transferred to an administrator in a specified way. The administrator is obliged to manage and control the property in accordance with the provisions outlined in the trust deed. The act of administration is performed exclusively for the benefit of the beneficiaries who are entitled to enjoy the property. Remuneration for the administrator's services comes from the property or from its returns.

A trust is a structure mainly found in countries that follow the Anglo-Saxon model, where legal capacity is lacking. The structure does not exist in Sweden for legal reasons but services related to trusts can be delivered in the country.[116] Swedish regulations apply to all cross-border activities conducted by Swedish companies or foreign companies registered in Sweden. For that reason, Swedish law also covers this type of service.

The services regulated in the legislation are administration, the provision of a registered office, post address and related services. These services may be professional services, offered by both natural persons and legal entities. The administrator is often a limited partnership where the administrator is a general partner with unlimited liability. The general partner then manages the assets in the trust, which are often invested via offshore accounts. The assets in a fund can be anything from cash and securities to real estate and cryptocurrencies.

The Swedish Companies Registration Office is unable to register activities such as *trust administration* in the anti-money laundering register and terrorist financing; therefore, these activities are registered under a number of other items. Exact statistics on the number of operators engaged in *trust administration* are not available. Companies that operate in the sector can likely be included in the group *legal activities* in the Swedish Companies Registration Office's anti-money laundering register. As of 31 December 2019, there were 803 registered companies in this

[116] Prop 2016/17:173, p. 459.

group.

Money laundering – description of risk scenario including known approaches (modus operandi)

• No information on known scenarios.

Threat – money laundering

Opportunity to use the sector for money laundering

A trust has no legal capacity and does not occur in Sweden for legal reasons. A trust's administrator can be located in Sweden, and a trust's address can be in Sweden. Therefore, trusts can fall under the supervisory responsibilities of the county administrative boards. The trust itself is always based abroad. This is one of many reasons that the authorities' knowledge of the sector is very low. Another reason is that the sector has not had adequate supervision and no reports have been made to the Financial Intelligence Unit of Sweden (Fipo) about operators in the sector. However, it is clear that a very high level of expertise (specialist) is required to conduct money laundering in the sector.

Starting a money laundering scheme is complex and takes time. But once the scheme is established, assets can be transferred quickly. Only legal entities are needed to carry out money laundering in the sector, and cash is used to a limited extent. The assets are typically transferred via bank transfers, and operators report that payments can also be made with electronic currency.

Anonymity and traceability

A threat actor can largely remain anonymous in the sector. The level of anonymity provided is often highlighted as an advantage by those who market the trust as a legal construct. In connection with the character review of the operators' representatives, the county administrative boards have difficulty contacting the representatives, as they often reside abroad.

Overall assessment

Given the authorities' limited knowledge of the sector and the opportunity to remain anonymous, the risk of money laundering is assessed as high.

In summary, the threat of money laundering in the sector is assessed as high (4).

Vulnerability – money laundering

Risk awareness

Operators in the sector report that they have done a general risk assessment and that they take adequate customer due diligence measures. Operators report that they obtain information about their customers' financial situation and that they provide adequate training to their employees.

Operators also report that the general level of knowledge in the sector is good and that it is rarely exploited for money laundering or terrorist financing. The county

administrative boards have not conducted any supervisory activities in the sector and cannot verify this information. The authorities' lack of information makes it difficult to assess risk awareness in the sector. This constitutes vulnerability.

In summary, vulnerability to money laundering in the sector is assessed as significant (3).

Risk – financing of terrorism

There are currently no known scenarios in which the sector is used to finance terrorism within the framework of the national risk assessment. The risk of terrorist financing in the sector has therefore not been assessed.

7.21 Board representation and nominee shareholders Trust administrators[117]

Overall sector risk:

Sector

Board representation

Natural persons and legal entities who serve as a board member, company legal officer, partner in a partnership or limited partnership or in a similar position in relation to other legal entities.[118]

Nominee shareholders

Natural persons or legal entities who have the function of nominee shareholders on another's behalf or measures taken with the intention of having another party serve in such a function, with the exception of assignments for a legal entity listed on a regulated market.

General description of the sector and related products or activities

Board representation

Services that provide a board member or corporate legal counsel are not professional services offered on the Swedish market.[119]

The operators referred to here are only persons who hold these functions on behalf of third parties and in accordance with standard business practice. This means that this assessment does not reference those who are appointed as "ordinary" board members in a company or association.[120]In other words, the service is not compatible with Swedish corporate law. Corporate legal counsel refers to a deputy function with responsibility for representing the company in relation to third parties. This type of service has not been offered in Sweden but is common in other EU countries.[121]

Even though the services are not available on the Swedish market, they can be exercised in Sweden through cross-border activities. An operator based in Sweden

---

[117] Board representation with a nominee shareholder is covered under the scope of the Anti-Money Laundering Act but a quantitative risk assessment has not been performed.

[118] Provided that the operator's activities do not fall under the scope of Chapter 1, Section 2, Paragraph 1st P 17– –21) of the Money Laundering and the Financing of Terrorism (Prevention) Act (2017:630).

[119] Prop 2008/09:70 p. 62.

[120] A corresponding application should be made for the function as a partner in a partnership or limited partnership.

[121] SWD 2008(09), p. 62.

may offer the services in markets where these are permitted.[122]

On 31 December 2019, the Swedish Companies Registration Office's anti-money laundering register contained 900 companies registered as engaging in board representation. Given the legal definition of the services, it is reasonable to suspect that those who have reported that they offer these services have misunderstood the legal definition and are simply not registered correctly in the register.

Nominee shareholders

A nominee shareholder's function is to conceal the true owner of a shareholding.

Money laundering – description of risk scenario including known approaches (modus operandi)

- No information on known scenarios.

Threat – money laundering

Extent

Board representation and nominee shareholders are activities that are not compatible with Swedish corporate law. These services do not occur in Sweden but do occur in other EU countries. Swedish operators can therefore offer these services in countries where they are permitted. The scope of the sector is therefore considered small with very few operators.

Capacity of threat actors

Board representation and nominee shareholders are relatively complex activities. The assessment here is that threat actors would need a high degree of knowledge about corporate law in Sweden and abroad.

Anonymity

Board representation is the provision of a board member or a corporate legal counsel. The board member completes an assignment on behalf of a third party. The corporate counsel serves in a deputy function and is responsible for representing a company in matters concerning third parties. A nominee shareholder's function is to conceal the true owner of a shareholding.

These activities are designed to increase anonymity and reduce traceability in the ownership and management of companies. The fact that these activities are not permitted in Sweden means that, by definition, foreign companies constitute the customers for the service.

Overall assessment

The services offered in the sector are not compatible with Swedish corporate law; therefore, operators can only offer the services in countries where the services are permitted. The services are relatively complex in nature and threat actors need to

[122] Ibid p. 63.

have a high capacity to exploit the sector. There is a good opportunity to remain anonymous, as the fundamental idea behind the services is to increase anonymity and reduce traceability in the ownership and management of companies.

Vulnerability – money laundering

Ability to detect money laundering

The services offered in the sector relate to the ownership and management of companies. Therefore, there are no transactions in the traditional sense other than payment for the services performed.

The ability to detect money laundering in the sector can be very limited. This is because the corporate forms are not compatible with Swedish corporate law and there are few operators who offer these services in Sweden. The ability to identify the true principal is also very limited, as the basic premise behind the activities is to increase anonymity.

Regulatory compliance

The county administrative boards have limited information about the sector. This creates the risk that operators can conduct their business without complying with the provisions of the Anti-Money Laundering Act.

Overall assessment

No traditional transactions occur in the sector, other than payment for the services performed. The ability to identify the beneficial owner is also very limited, as the basic premise behind the activities is to increase anonymity.

Risk – financing of terrorism

There are currently no known scenarios in which the sector is used to finance terrorism within the framework of the national risk assessment. Therefore, the risk of terrorist financing in the sector has not been assessed.

7.22 Activities as an authorised auditor, approved auditor or registered audit firm

Overall sector risk:

Sector

The sector includes activities as an authorised/approved auditor or registered audit firm. This includes services such as auditing, attestation and certification assignments as well as auditing advisory services.

General description of the sector and related products or activities

Only authorised or approved auditors may perform auditing activities in a limited company. For listed companies with large-scale operations in terms of turnover, balance sheet total or number of employees, and for many financial companies, at least one of the company's auditors must be authorised.

The regulations on authorised and approved auditors and registered audit firms are found in the Auditors Act (2001:883). Since 2013, auditors can only be granted the title authorised auditor, but auditors who were approved before that can continue to work under the title of approved auditor.

Partnerships and limited companies that carry out auditing activities may, under certain conditions, be registered as audit firms. This means that the company itself – unlike an unregistered audit firm – can be appointed as auditor. However, an active approved or authorised auditor in the company must always be appointed as the principal auditor for every audit assignment. The principal auditor must sign audit reports and other statements.

Auditing

Auditing is the independent review and providing of a statement regarding information or certain conditions. The purpose of an audit is to increase the degree of trust in the information among external stakeholders, such as investors, creditors, customers, suppliers and authorities. An audit aims to create confidence in the accounts and management of the business.

Auditing regulations are mainly found in the Audit Act (1999:1079), the Swedish Companies Act (2005:551), the Co-operative Associations Act (2018:672) and the Foundation Act (1994:1220).

An auditor's assignments consist of financial audits and management audits and must be as thorough and comprehensive as good auditing practice requires.[123]Through the audit, the auditor must achieve reasonable assurance that

[123] Paragraph 3 of the Auditing Act. The same also applies in accordance with Chapter 9 paragraph3 of the Swedish Companies Act, Chapter 8 paragraph 3 of the Co-operative Associations Act and Chapter 4 paragraph 9 of the Foundation Act.

the financial statements are free from material misstatements in order to be able to express an opinion on whether the financial statements – in all material respects – have been prepared in accordance with applicable rules.[124]

An audit does not examine every individual transaction, but a selection is made and the auditor's work is focused on areas where there is a high risk of error and where any misstatements would be material to the financial statements.

Attestation and certification assignments

In addition to the above-mentioned auditing activities, authorised and approved auditors are also designated to perform other statutory audit assignments, such as issuing certificates and providing professional opinions or statements.[125] Examples of such assignments are auditor's certificates when capital contributed in-kind is received by the company when a limited liability company is formed, auditors' statements on balance sheet sheets for liquidation purposes or when dividends are paid at an extraordinary general meeting. Auditors can also perform other review activities for a client; for example, when a bank requests an independent review or for the valuation of specific balance sheet items. The purpose of these assignments is for the auditor to submit statements that increase the degree of trust in the information among external stakeholders.

Audit-related advice

Often, authorised and approved auditors also offer advisory services in areas that are closely related to auditing activities, such as management accounting, bookkeeping and taxation. This type of consultation is usually called auditing advisory services.

Key figures*	**Total for entire sector**
Number of authorised auditors	2,726
Number of approved auditors	349
Total number of authorised and approved auditors	3,075
Number of registered audit firms	176
Number of companies that employ internal authorised or approved auditors	724

* Number of authorised and approved auditors and registered audit firms according to the Swedish Inspectorate of Auditors auditor register as of 7 January 2020, and the number of companies that employ authorised or approved internal auditors as of 13 January 2020.

Money laundering – description of risk scenario including known approaches (modus operandi)

• It should not be possible to use the sector for money laundering or terrorist

[124] ISA 200 *Overall objectives of the independent auditor and the conduct of an audit in accordance with International Standards on Auditing.* International Standards on Auditing (ISA) are developed by the International Auditing and Assurance Standards board (IAASB).

[125] For example, in Chapter 2, paragraph 19; Chapter 13 paragraph 42; Chapter 15 paragraph 44; Chapter 18paragraph 6; Chapter 23 paragraph 25; and Chapter 25 paragraph 15 of the Swedish Companies Act.

financing. The risk for these activities is instead linked to the services provided by the auditors. These services can be used as a seal of approval for financial statements for businesses that have been used as part of a money laundering scheme or the financing of terrorism.

- This allows threat actors to use approved and authorised auditors or registered audit firms as facilitators – with or without their knowledge – to make illegal transactions appear legitimate and to make false documents and invoices appear to be correct.
- From the outside, the company may appear to be engaged in legal operations when in fact it is being used for VAT fraud, withdrawal of cash for payment while avoiding paying taxes, transfer of profits to the accounts of criminal actors or to enter criminal money into the company's accounts as turnover.
- There are also companies where part or the entire business plan is to commit fraud by issuing or paying false invoices. In order to conceal the origin of the money and create an impression of legitimacy for the company, criminal proceeds can also be divided and transferred between several different accounts, preferably across several jurisdictions. In addition, it is not uncommon for criminals to use strawmen or people who act as executives but are not the UBOs.
- These crimes are often difficult for outsiders or authorities to detect because they are carried out within established corporate structures. Once the annual report is published, a company may then be declared bankrupt and the UBO starts a new company.

Threat – money laundering

Scope

There is a need for auditing services in all industries. This creates a risk that money laundering transactions may pass through the sector, even though the actual act of money laundering has not taken place in the sector. In addition, the audit is done after the fact, i.e. long after a transaction has taken place. No actual funds are handled during the audit, which means that the services can only be used in advanced, long-term schemes.

Capacity of threat actors

Threat actors need a relatively high level of competence in finance, bookkeeping and auditing methodology to be able to exploit the sector as part of a money laundering and terrorist financing scheme.

Anonymity

Complex, large-scale money laundering schemes, where, for example, fraudulent identity documents or strawmen are used, can make it difficult for auditors to identify UBOs. Therefore, this provides an opportunity for threat actors to remain anonymous, even though the actor needs to have a certain capacity to achieve anonymity.

Overall assessment

There is a risk that money laundering may pass through the sector at some stage in the chain, even though the actual money laundering step has not been carried out in the sector. Complex, large-scale money laundering schemes can allow threat actors to make it difficult to identify UBOs and therefore allow them to remain anonymous.

The assessment here is that many threat actors use companies as tools for their money laundering schemes.

In summary, the threat of money laundering in the sector is assessed as significant (3).

Vulnerability

Ability to detect money laundering

Auditors are subject to the provisions in the regulations on customer due diligence and monitoring. In addition, the performance of an audit requires the auditor to have good knowledge of the individual customer's operations, management and organisation. The sector is also often characterised by long-term customer relationships, which provides good opportunities to detect abnormal behaviours or activities. The level of vulnerability in the sector is affected by the fact that auditors provide services in operations within all types of industries, some of which are high risk. But a key component of an audit is to assess the risks of irregularities in relation to the financial reporting.

The detection of money laundering can be difficult for those who do not have good knowledge of what different industry-specific approaches look like. The audit itself is done after the fact, i.e. long after a transaction has taken place. The likelihood of detecting money laundering at a later stage may therefore be low.

The audit obligation has been abolished for smaller companies. This also makes it is possible to carry out relatively extensive money laundering schemes in business forms that are not subject to a statutory audit requirement.

Finally, 85% of all corporations started today opt out of audits. The majority of the legal entities in EBM's investigations are limited companies. Given these conditions, auditing is an area of activity that is largely underutilised in the work to combat financial crime and money laundering, as limited companies that opt out of audits do not have an actor in their organisation who is obliged to report suspected money laundering.

Regulatory compliance

Auditors are subject to money laundering regulations. But they are also subject to a strict code of ethics where professional scepticism and independence are core values. This in itself should deter threat actors from attempting to exploit the sector.

If a scheme is able to be implemented without an audit due to the limited scope of the audit obligation, threat actors can choose to avoid an audit.

Auditors generally have good knowledge of the money laundering regulations. However, there may be uncertainties regarding the threshold for reporting to the

Financial Intelligence Unit of Sweden (Fipo) As the sector is largely characterised by long-term customer relationships and the auditors' statements must be well-founded, there is a risk of under-reporting if the level of suspicion is low.

Overall assessment

It may be difficult to detect money laundering in the sector because an audit takes place after the fact, i.e. long after a transaction has taken place. Additionally, complex, large-scale money laundering schemes can make it difficult to identify UBOs. The fact that the sector is characterised by long-term customer relationships and the requirement that an audit be based on well-founded statements can also create a degree of reluctance to report suspected money laundering if the level of suspicion is low. Overall, the assessment here is that auditors are generally well equipped to prevent their services from being exploited as part of money laundering or terrorist financing schemes. The vulnerability is therefore moderate.

In summary, vulnerability to money laundering in the sector is assessed as moderate (2).

Risk – financing of terrorism

There are currently no known scenarios in which the sector is used to finance terrorism within the framework of the national risk assessment. Therefore, the risk of terrorist financing in the sector has not been assessed. However, it should be noted that there is a potential risk that false invoices could be used as part of a terrorist financing scheme.

7.23 Advocates and law firms

Overall sector risk:

Sector

In terms of money laundering and terrorist financing, threats and vulnerabilities mainly relate to the activities of advocates or law firms, as an advocate acts on behalf of a client in financial transactions or real estate transactions. It can also relate to the planning or execution of transactions on behalf of a client (the services are specified in Chapter 1, Section 4, first paragraph of the Money Laundering and the Financing of Terrorism (Prevention) Act (2017:630).

General description of the sector and related products or activities

The practice of law and the Anti-Money Laundering Act

Advocates and law firms fall under the scope of the law only in the performance of certain services. However, the vast majority of legal assignments fall *outside* the scope of the aforementioned law.

The Anti-Money Laundering Act thus explicitly stipulates the scope of the law (Chapter 1, Section 2 , para. 20 and Chapter 1, Section 4, first paragraph) with regard to these services.

On 1 November 2019, the Anti-Money Laundering Act was supplemented with new provisions regarding supervision and intervention in relation to advocates and law firms (e.g. Chapter 7, Anti-Money Laundering Act and Chapter 8, Section 7 of the Code of Judicial Procedure).[126]

The Swedish Bar Association's supervision and training

Advocates have been subject to the Anti-Money Laundering Act since the second EU money laundering directive entered into force on 1 January 2005. The Swedish Bar Association immediately issued guidance for advocates to address issues that were of particular importance to their practice.

In response to the current anti-money laundering law (which came into force on 1 August 2017), the Swedish Bar Association drafted a new, comprehensive document to offer guidance to advocates.[127] The document laid out binding guidelines for advocates and law firms to follow in their practice in relation to preventing the exploitation of their legal practice for the purposes of money laundering or terrorist financing.

According to the Anti-Money Laundering Act and the Fourth and Fifth EU Money

[126] See SFS 2019:608, Riksdagsskrivelse 2019/20:1 Betänkande 2019/20:Ju U2 and Prop 2018/19:125.

[127] See *Guidance for advocates and law firms on the legislation to combat money laundering and terrorist financing – Swedish anti-money laundering legislation from a lawyer's perspective* adopted by the Board of the Swedish Bar Association 3 October 2019. See also Circular No. 18/2019

Laundering Directives, the Swedish Bar Association is obliged to effectively monitor and implement the measures necessary to ensure that those subject to the provisions of the legislation also comply with the legislation. Supervision shall serve to ensure compliance with the legislation and that advocates and law firms have the necessary training, administration and routines in place. Law firms that are subject to the provisions of the legislation, for example, must have established routines for customer due diligence, reporting, retention of information and documents, internal control, risk assessment, risk management and communication.

In 2009, the Swedish Bar Association enhanced its supervision of advocates and law firms with regard to compliance with the Anti-Money Laundering Act.[128] The enhanced supervision primarily relates to the submission of written information, but visits to individual firms also occur to a certain extent.

Since 2016, the Swedish Bar Association has also introduced a systematic supervision procedure of advocates and law firms.[129] The review has been carried out in various rounds, where 25 randomly selected law firms have been asked to answer questions in an audit report. The answers have then been compiled and analysed. In cases where it has been determined that additional information is needed, or where shortcomings have been discovered, a dialogue has been initiated with the respective firms. The purpose is to address the identified shortcomings as efficiently as possible.

This supervisory work will continue in 2021, at which time it will largely include law firms with fewer than ten associates.

The Swedish Bar Association has offered extensive (often free of charge) training initiatives in the form of full-day courses to increase knowledge of the anti-Money Laundering Act among its members. Since 2010, a portion of the compulsory courses for obtaining admission to the Swedish Bar also include education on legislation.

Key figures	**Total for entire sector**
Active Swedish advocates (excl. 33 EU lawyers who are members of a bar association in another member country and practice law in Sweden under the professional title of their home country)	6,158
Swedish associates at a law firm	2,711
Number of law firms	2,017
As of the beginning of 2020, a total of 225 of the country's law firms have undergone the proactive supervision. A total of 5,338 lawyers (of which 3,166 advocates) have been covered by the Swedish Bar Association's supervisory measures.	

[128] The background and details regarding the Swedish Bar Association's enhanced supervision are set out in the memorandum *The proactive supervision of advocates and law firms - a matter of quality and trust, as well as independence and self-regulation.*

[129] See the Swedish Bar Association's information *To the members of the Swedish Bar Association. Information regarding effective supervision of law firms,* Circular No. 28/2015

Money laundering – description of risk scenario including known approaches (modus operandi)

- Threat actors can use advocates to, for example, create company structures that can then be used for money laundering or to create legitimacy for transactions that involve money laundering.
- **Exploitation of client funds account.** This concerns cases where the client seeks to use the law firm's client funds account to carry out transactions covered by the assignment. Advocates and law firms are, according to the Swedish Bar Association's guidelines, instructed to avoid using the law firm's client funds account unless it is necessary and seems reasonable for the transaction to be executed using the client funds account.
- **Sham transactions.** This involves creating a fictitious transaction within the scope of an assignment. For example, creating a fictitious company structure within the framework of an otherwise legal and "normal" assignment. In these cases, it is important that the advocate understands each individual transaction, action or circumstance within the framework of the assignment in order to be able to prevent the legal practice from being exploited for the purpose of money laundering.
- **Sham litigation.** Sham litigation is used as a means to obtain a judgement or decision that allows money to be used and transferred from one actor to another with the assistance of the authorities. This gives the transfer the appearance of legitimacy, and the person who is laundering the funds can show the origin of the money.

Threat – money laundering

Scope

The Swedish Bar Association is not subject to a reporting duty or mandatory disclosure rules. Instead, it is the individual advocates and law firms that are subject to these obligations.

Reports made in the sector have included large sums of money. This is likely due to the fact that advocates,

in cases involving suspected money laundering, report the total value of the business transaction. This may be the case even if the advocate's assignment only covered a certain portion of the arrangement and may not have included a money transfer. Although a business arrangement can involve very large sums of money, it is very unusual for advocates to handle these sums in their law practices. It is more typical for an advocate to provide legal advice that does not involve the management of financial resources.

Reporting from the sector is low, which may indicate high exposure to threats. But the low rate of reporting is likely related to the fact that the Anti-Money Laundering Act imposes a number of obligations that are often in direct conflict with the legal profession's statutory professional rules and core values.

The Anti-Money Laundering Act also lays out a number of situations where advocates are not obliged to report suspicious transactions. However, the most important reason for the low rate of reporting may be that advocates – in accordance with applicable legislation and the Bar Association's guidelines – invest significant resources into customer due diligence measures. In addition, advocates do not accept assignments if they do not feel confident in the checks they have done for the potential client.

Finally, the low number of reports could be due to the fact that advocates often have a very close and confidential relationship with their clients and a detailed understanding of the assignment. This means that they are better able to resolve uncertainties, and uncertain or incorrect reports can be avoided. The close client-lawyer relationship, as well as the advocate's in-depth legal knowledge, also means that the risk of money laundering in the sector is significantly lower than it is for operators in many other sectors. In cases where money laundering does occur, it likely involves sophisticated actors that implement advanced schemes. These schemes are also difficult to detect and therefore are not reported.

There are therefore a number of natural explanations for why the reporting frequency for advocates is low. Furthermore, it is apparent that the number of reports cannot be used as a benchmark for how well the legislation is working in practice. This holds especially true given the fact that advocates are also subject to other legislation, the aims of which are incompatible with the Anti-Money Laundering Act's reporting obligation. Furthermore, advocates are exempt from the reporting obligation in certain cases under the Anti-Money Laundering Act. Given these conditions, the overall exposure to threats can be assessed as moderate.

Anonymity

Advocates are obliged to conduct a detailed evaluation within their customer due diligence process before an assignment may begin in earnest. The close client-lawyer relationship, combined with the specialised legal knowledge of an advocate, also makes it difficult for threat actors to remain anonymous. However, in the case of complex, large-scale money laundering schemes, it is possible for a high-capacity threat actor to remain anonymous.

Capacity of threat actors

The use of the sector for money laundering requires a high capacity on the part of the threat actor. The reason for this is that schemes that involve legal services usually include major business transactions or arrangements that are more extensive or complex in nature. This means that there are relatively few threat actors with the capacity to carry out money laundering schemes in the sector. However, each individual case with a scheme that is more complex in nature presents a relatively large threat.

Overall assessment

The rate of reporting from the sector is low. This can be explained by the special regulations imposed on advocates in the legislation and the special conditions

under which advocates operate and carry out their assignments. The reports that are submitted involve large sums of money, but the scope of an advocate's assignment likely only covers a small portion within a suspected money laundering scheme, and it is thus likely that only a small part of the total reported sum is associated with money laundering. Threat actors need a high capacity to carry out money laundering in the sector, and it is difficult to remain anonymous.

In summary, the threat of money laundering in the sector is assessed as moderate (2).

Vulnerability – money laundering

Ability to detect money laundering

Money laundering in the sector is primarily believed to be associated with complex, major business transactions, which by their very nature are extensive and difficult to grasp. The schemes often involve a number of companies or legal entities. The reasons behind a transaction and the identity of the UBO can be difficult to determine. But at the same time, advocates are particularly well positioned to detect irregularities in their capacity as legal experts.

Furthermore, advocates often have a very close, confidential relationship with their clients as well as good insight into what an assignment entails. This means that any uncertainties can be resolved more easily. There is therefore a very good chance that attempted money laundering will be detected, unless the threat actor has a very high capacity, extensive knowledge and a carefully devised plan to avoid detection. If adequate customers due diligence measures are not taken, the ability to detect money laundering decreases. Therefore, an advocate must investigate to determine the identity of the UBO and analyse the purpose behind the assignment. If advocates fail to adequately perform these checks and analyses, this in itself can constitute a potential vulnerability.

The greatest vulnerability is considered to be the potential for advocates to be used as facilitators in a limited but important part of extensive money laundering schemes. High-capacity threat actors can also seek legal advice or legal assistance from advocates to implement criminal schemes that specifically target the legal profession. For example, this may be about creating an unauthorised company structure which is then used for more extensive money laundering schemes.

Regulatory compliance

Advocates are only subject to the provisions of the Anti-Money Laundering Act to the extent that they perform services specified in Chapter 1, Section 4 of the same law. Advocates are also not obliged to report suspected money laundering if the suspicion is based on information obtained in confidence when representing a client in legal proceedings. This also applies to advice to initiate or avoid legal proceedings, as well as when information has been obtained during the assessment of a client's legal situation (see Chapter 4, Section 8 of the Anti-Money Laundering Act).

There is no established requirement for an advocate to report suspected money

laundering when a potential client is rejected when thorough customer due diligence measures could not be performed, or an understanding of the assignment could not be obtained (see Bill 2016/17:173 p. 292). This means that there may be cases of money laundering that go unreported to the Financial Intelligence Unit of Sweden (Fipo) despite being known to the advocate. Advocates have no statutory obligations under the Anti-Money Laundering Act; at the same time, the duty of confidentiality, client loyalty and independence must be maintained in accordance with the Code of Judicial Procedure and other statutes.

The Anti-Money Laundering Act also imposes requirements that would entail deviations from the legal profession's core values. This conflict has led to the above-mentioned exemption from the reporting obligations for advocates. It also means that a number of other problems arise in applying the law. The reporting and disclosure obligation (in the Anti-Money Laundering Act) is incompatible with the confidentiality obligation to which advocates are bound. The Swedish rules for the competition of crimes (Lagkonkurrens) also means that the legal position is unclear as to when and how the advocate's duty of confidentiality may be broken as a result of the duty to report and provide information.

The prohibition of questioning with regard to information that has been entrusted to an advocate, and information obtained within the framework of an assignment, may only be broken under the conditions specified in Chapter 36, Section 5 of the Code of Judicial Procedure. This means that the conditions for when an advocate is obliged to testify in court also apply here. However, a lawyer is never under an obligation to disclose information that he or she has received in connection with legal proceedings, or when evaluating the client's legal situation. In some cases, the mandatory disclosure rules may also be excluded as a result of the European Convention's provision on protection against self-incrimination.

The reporting obligation also stands in conflict with another core value that applies to advocates, namely the obligation to loyalty. A lawyer's primary obligation is loyalty to the client. This may only be broken if it is supported by the law and professional conduct.

If an advocate reports a client to the police, he or she has an obligation to withdraw from the assignment immediately.[130] When an advocate withdraws from an assignment, he or she must do so in a way that does not conflict with the disclosure provision in the Anti-Money Laundering Act. However, it is not a crime for an advocate to advise his or her client against engaging in illegal activities, or to state that an advocate must not promote injustice per the Code of Professional Conduct.

Overall assessment

The sector differs from most other sectors, as the Anti-Money Laundering Act is only applicable when advocates perform certain assignments on behalf of a client as listed in the act. The law also contains additional exceptions that apply to advocates

[130] This follows from the ethical rules (3.4.2. Fourth item Code of Professional Conduct).

and law firms. In addition, there are a number of issues in the application of the legislation, as it stands in conflict with the obligations advocates undertake with respect to their clients. Those threat actors who are able to exploit the sector are likely to have a high capacity. At the same time, advocates are particularly well positioned to detect abnormal activities and transactions. It is also assessed here that advocates and law firms are generally very well equipped to counteract the use of their services as part of a money laundering scheme.

In summary, vulnerability to money laundering in the sector is assessed as moderate (2).

Risk – financing of terrorism

There are currently no known scenarios in which the sector is used to finance terrorism within the framework of the national risk assessment. Therefore, the risk of terrorist financing in the sector has not been assessed.

7.24 Swedish gambling market

Overall sector risk:

Sector

The sector consists of gambling operators that are subject to a licensing or registration obligation in accordance with the Gambling Act (2018:1138).

General description of the sector and related products or activities

The Gambling Act contains six different types of licenses:

- Licenses for state gambling (Chapter 5 of the Gambling Act (2018:1138)) may be granted to provide casino games at a casino, games on token gambling machines and certain forms of lotteries. Such a license may only be granted to limited companies that are directly or indirectly wholly owned by the state.
- Licenses for gambling for purposes in the public interest (Chapter 6 of the Gambling Act (2018:1138)) may include certain types of lotteries. Such a licence may only be granted to non-profit associations or registered religious communities whose main purpose is the promotion of the public interest.
- Licenses for commercial online gambling (Chapter 7 and 8 of the Gambling Act (2018:1138)) may be granted to provide casino games, online bingo and computer-simulated gambling machines and betting. Licenses are open to market participants.
- Licenses to provide land-based commercial gambling (Chapter 9 of the Gambling Act (2018:1138)) may include casino games that do not take place at a casino, goods gambling machines and card game tournaments under certain specified conditions. Licenses are open to market participants.
- Licenses to provide gambling on vessels in international traffic (Chapter 10 of the Gambling Act (2018:1138)) may cover gambling on cash and token gambling machines as well as casino games that do not take place online or at a casino.

In Sweden, the right to offer games for money has previously, with certain exceptions, been reserved for the state and organisations that promote the public interest. Private companies and other for-profit organisations have only been permitted to offer games for money in certain limited areas.

With the new gambling regulations that entered into force on 1 January 2019, the Swedish gambling market now includes companies and organisations that vary in size and character. The gambling market includes state-owned and state controlled companies, international gambling companies (with a large annual turnover) and small, non-profit associations that offer small-scale lotteries.

The turnover for different games varies significantly. The same applies to the risks associated with different games and the way the games are organised.

Temporary ordinance on responsible gambling measures due to COVID-19

On 2 July 2020 (in force until the end of June 2021[131]) provisions were introduced that:

- The deposit limit for games at online casinos may not exceed SEK 5,000 and the corresponding loss limits apply to games at token gambling machines.
- It is mandatory for players to set upper limits on their login time when playing at online casinos and token gambling machines.
- Bonuses offered by licensees who provide online casinos and token gambling machines may amount to a maximum of SEK 100.

Key figures	Total for entire sector
Number of companies	95*
Companies' turnover	SEK 24,782 million**
Companies' balance sheet total	No information
Number of employees	4,200***
Number of established business relationships	No information
Total Number of natural customers	**5,600,000****
Total number of legal customers	**0**

* Companies with licenses for the purpose of promoting the public interest are not included (20/12/2019).

** Net turnover (players' bets – winnings) (2019).

*** Permanent employees in Sweden. The Swedish Agency for Public Management (Statskontoret).

**** The general public (2020).

Money laundering – description of risk scenario including known approaches (modus operandi)

- The risk that games for money will be exploited for the purpose of money laundering differs between different types of games. The legal conditions that characterise the organisation, scope, distribution, anonymity, forms of deposit/payment and payment of winnings are important factors in determining the risk of money laundering.
- The risk is considered to be the highest for commercial online gambling, casino games at state casinos and betting (both online and land-based). The assessment is primarily based on the high stakes, winnings and high turnover in these activities. In the case of online gambling, the level of risk is affected by the players' use of gambling accounts, and in the case of land-based gambling; risk is affected by the use of cash.
- Even though no concrete information has been found to confirm this, the

[131] The Ordinance on temporary responsible gambling measures in connection with the spread of the COVID-19 disease initially applied during the period 2 July to 31 December 2020, but the government has extended the period of validity until the end of June 2021.

assessment here is that consumption of illegally acquired funds is the form of money laundering that is most common in the Swedish gambling market. Account transfer, transfer, reverse money laundering and the exchange of criminally acquired funds are other relevant threats.

- The use of gambling accounts presents an increased risk that the licence holder will be exploited for the purpose of money laundering. Gambling accounts can be used for purposes other than gambling, for example, to conceal the origin of illegally acquired funds. It is also possible for gambling accounts to be used to hold criminal proceeds. This scheme involves the transfer of funds from a bank account to gambling accounts exclusively to hold the funds in the account until they are moved at a later date. When withdrawals are subsequently made from the gambling account, these appear to be legitimate payments and can therefore be used to explain the origin of the money. In order to evade detection, funds transferred from a bank account to a gambling account can be used for games with minimal losses, only to be transferred at a later date from the gambling account to another bank account.
- There is also a risk of match fixing and other forms of gambling fraud. The ability to commit gambling fraud and manipulate results is likely to attract actors seeking to launder money, as the criminally acquired funds can not only be laundered but increased.
- Under the Gambling Act, transfers between gambling accounts are not permitted. However, funds can be transferred between players, for example, through deliberate losses in poker known as “chip dumping”. This can be done between players who are acting in collusion with each other or through improper use of e-IDs. Criminally acquired proceeds can also be transferred by means of chips and receipts or by changing the owner of winning lottery tickets.
- Even though there is currently no evidence that this has occurred, there is always a risk of infiltration or direct ownership in gambling companies by actors in organised crime. Businesses can be part of a money laundering scheme, as transactions carried out with illegally acquired funds can be concealed among a company’s legitimate transactions. There are examples on the international level of groups with ties to serious organised crime that exploit gambling companies to enable money laundering, to a certain extent. This can involve legal gambling activities, where black money is laundered into legitimate funds, or illegal gambling, where income should be regarded as criminal proceeds.
- The consumption of gambling using the proceeds of criminal activities is likely the most common form of money laundering covered by the Anti-Money Laundering Act.
- Exchange. Games where bets are paid in cash. For example, the payment of bets in small denominations and the paying out of winnings in larger denominations.
- Deposit to account. Games that offer the account transfer of winnings after cash bet payments. This method is considered to be used more extensively for games

with a high payout percentage. Gambling and winnings receipts can be used as verification in connection with an account transfer through a bank.

Threat – money laundering

Scope

Only natural persons are able to participate in games for money. This means that legal entities are not included among the actors that use the sector for money laundering. The opportunity to carry out money laundering in the sector is considered to be relatively good. Commercial online gambling is available twenty-four hours a day, both for people who want to play games for money and those who want to launder money. When playing at physical casinos or betting, it is also possible to play with cash. Depending on whether the gambling agent accepts cash, these funds can be used to a relatively large extent. It is also possible for gambling receipts to be used as documentation in the accounting of persons other than the person who engaged in the gambling activity.

High stakes and winnings, as well as a high repayment of winnings – in addition to a high turnover – create relatively attractive conditions for money laundering. Money can also be laundered quickly in the sector, as gambling companies offer fast transactions and fast registration of new gambling accounts.

Capacity of threat actors

In the case of commercial online gambling, a valid e-identification is required and the deposit to the gambling account is made in SEK through an approved payment service provider. In the case of physical gambling agents, it is possible for a natural person with a gambling account to use cash, though all games for money played with these agents must take place through a gambling account. However, it is possible to exploit another person's identity to create and use a gambling account. Therefore, a threat actor does not need to have a high capacity to be able to launder money in the sector.

Anonymity

The customer's identity is verified through an E-identification check performed by the gambling company when a gambling account is registered online. Requirements for the identification and registration of visitors and players also apply to casinos and land-based betting. However, threat actors can remain anonymous by exploiting the identities of others.

Overall assessment

Natural persons can gamble with cash when playing at casinos and in land-based betting. Online games for money are accessible twenty-four hours a day. Threat actors need no special capacity to be able to launder money in the sector. However, a threat actor may need to access borrowed or hijacked identities in order to create and use gambling accounts while remaining anonymous.

In summary, the threat of money laundering in the sector is assessed as high (4).

Vulnerability – money laundering

Ability to detect money laundering

Based on information from the Swedish Gambling Authority, gambling companies have developed a number of tools, mainly for controlling customers through internal monitoring systems. These tools can detect gambling patterns that are consistent with money laundering and fraud. However, some gambling companies still apply a reverse control system where it is relatively easy to deposit money. On the other hand, it can be more difficult to withdraw money from gambling accounts due to the checks that are performed.

It is possible to use false identity documents to open one or more gambling accounts. These accounts can then be used as tools to carry out fraud, money laundering or terrorist financing. Identity fraud therefore poses a high risk when a new customer relationship is established with a gambling operator.

The Swedish Gambling Authority has discovered that some gambling companies have fallen short when performing their customer risk classification and in the follow-up of their customers' risk profile. Therefore, the assessment here is that there needs to be an increase in the overall level of competence in gambling companies in this respect. When smaller deposits are made, the risk that it will take significant amount of time before a gambling company detects suspected money laundering increases. Despite the existing control systems, risk naturally increases in activities that involve a large number of transactions and high turnover.

There is also a risk that gambling companies will be formed for the sole purpose of laundering money from criminal activities. There is a risk that schemes will become increasingly advanced and difficult to detect. The ownership structure of a gambling company can be very complex, such that the parent company can be based in a country outside the EU, with UBOs that are difficult to identify.

Traceability

There is generally a good opportunity to trace money used in gambling. Money is placed in a gambling account and must then be transferred back to a bank account. However, it is possible for several different people to make deposits to the same gambling account, making it difficult to trace the money after the funds are withdrawn from the gambling account. For example, the money can be transferred to a foreign bank account. Swedish banks have shown a tendency to be increasingly hesitant to accept gambling companies as customers. Therefore, there is a risk that gambling companies will seek banks outside the EU. In cases where gambling companies operate in Sweden and use a bank outside the EU, the ability to trace transfers is decreased. Furthermore, a gambling company that operates in Sweden is under no obligation to use a Swedish bank. Gambling companies are only required to indicate their main bank when applying for a licence.

Online gambling companies tend to engage in activities that span different sectors and can use the payment institutions' ability to repay winnings as a marketing

strategy. In addition to gambling companies, banks and payment institutions are also required to complete the money laundering chain. It is difficult for operators and law enforcement agencies to gain insight and detect irregularities in the transaction chain, from the time the funds are deposited in a bank account, moved to a gambling account and then back to a bank account. All games for money must be in Swedish kronor, but there is a risk that the money will quickly change form when depositing and withdrawing from a gambling account. However, many gambling companies have turnover requirements for the money, which reduces the risk that gambling accounts will only be used to transfer money further.

There is also a certain level of vulnerability when online gambling companies rely exclusively on e-identification to verify identities. Therefore, it is possible for a player to borrow or misuse another individual's e-identification, and to remain anonymous to a certain extent.

Regulatory compliance

Since 1 January 2019, any gambling companies seeking to promote and market themselves in Sweden must have a Swedish gambling licence. A gambling company may not market itself to Swedish players without a licence.

The Swedish Agency for Public Management has found that the degree of channelisation (the proportion of players who gamble with companies holding a Swedish gambling licence) was 85 per cent in 2020.[132] Even though the degree of channelisation has increased since the period before the new regulation was introduced, there is still widespread gambling in Sweden with companies that do not have a Swedish gambling licence.

The Swedish Gambling Authority cannot carry out supervisory activities for gambling companies that do not hold a licence in Sweden. This increases the vulnerability to money laundering in the sector. The Swedish gambling company market is largely international in character. Most of the gambling companies operating in Sweden with a licence are based in Malta. The gambling industry is characterised by a rapid pace of development, and there have been a large number of changes, including major changes, in the gambling market.

There is a risk that gambling companies will have inadequate customer due diligence measures, as some gambling companies only perform checks when withdrawing gambling winnings – not for registration or deposits into a gambling account. There may also be a reluctance to report suspicion when it concerns the most profitable customers if the level of suspicion is low.

There is also a risk associated with international gambling agents who offer cross-border gambling on Swedish horse racing abroad, with players then having the option to have any winnings paid out to a foreign bank account. The Swedish Gambling Authority is unable to carry out supervision of gambling agents in other

[132] Swedish Agency for Public Management (Statskontoret) (2021:5), Evaluation of the re-regulation of the gaming market (Interim report 4. Second year with the new gambling regulation). www.statskontoret.se/globalassets/publikationer/2021/2021-5-webb.pdf

countries, as the agent registration takes place with the gambling authority in each country.

Overall assessment

Some gambling companies still use a reverse control system, where it can be easy to deposit money into a gambling account, but more difficult to transfer the money to a bank account. The traceability of transactions in the sector is inadequate, and there is therefore a risk that multiple people will make deposits into the same gambling account. There is also a risk that legal entities will form gambling companies with the sole purpose of laundering criminally acquired money.

In summary, vulnerability to money laundering in the sector is assessed as significant (3).

Risk – financing of terrorism

There is a risk that gambling accounts will be used to transfer money to foreign bank accounts, which are not subject to Swedish regulations. An additional risk is that gambling accounts will be used to a larger extent, as gambling accounts will not be covered by the new bank account register law.

Appendix:
Definitions of threat, vulnerability and consequence

According to the Financial Action Task Force (FATF), *risk* is a function of three factors: threat, vulnerability and consequence. According to the FATF, it is up to individual countries to establish a product or process based on a method decided by the country's stakeholders. The definitions of threat, vulnerability and consequence are appropriate starting points.

In this risk assessment, the scope of the Anti-Money Laundering Act's application has been evaluated. This has been performed through an assessment of a variety of issues the coordination function has been tasked with addressing. These issues have been raised in order to identify and rate threats and vulnerabilities. The documentation used for the risk assessment has, in certain cases, been supplemented by responses to questions sent out by supervisory authorities to operators in each sector. The collected responses have subsequently been assessed jointly.

In addition to the sector-by-sector analysis, an analysis has also been carried out to evaluate the potential consequences of these identified threats and vulnerabilities on the national level. More detailed definitions of FATF's threats, vulnerabilities and consequences are provided below. A generic application of the definitions has been used to create a conceptual framework for all the actors that have participated in this national risk assessment.

A **threat** is a person or group of people, object or activity with the potential to cause harm to, for example, the state, society or the economy. The threat can be criminals and their facilitators, as well as their funds and activities. Threats are often an important starting point for developing an understanding of the risk of money laundering and terrorist financing. In order to be able to perform the risk assessment, it is important to have insight into the entire chain. In the case of money laundering, it is necessary to understand both the predicate offences and the criminal proceeds as well as the actual process of laundering the criminal proceeds. In the case of terrorist financing, one needs to have insight into both of the origin of the funds and how the funds are used to finance terrorism.

The concept of **vulnerabilities** comprises the factors that can be exploited by the organisation or individuals that constitute a threat or that may support or facilitate its activities. Vulnerability in this context represents the conditions that constitute weaknesses in different systems or certain features of a particular country. Vulnerabilities may also include the features of a particular sector, a financial product or type of service that make them attractive for the purposes of money laundering or terrorist financing.

Consequence generally refers to the impact or damage that money laundering or

terrorist financing may cause. This includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society as a whole. Consequences thus relate to the potential impact of money laundering and terrorist financing over the short term and long term and how these activities can impact the population, specific communities, the business environment, national and international interests as well as the reputation and attractiveness of a country's financial sector.

According to the FATF, risk assessments must include an evaluation of threats, vulnerabilities and consequences. As it is generally difficult to determine or predict the consequences associated with a particular risk or vulnerability, it is generally accepted that such an analysis does need to be an in-depth analysis but can constitute an overall picture of the potential consequences that threats and vulnerabilities pose for society at large. In this national risk assessment, the coordination function has decided to include an impact assessment. The method for this assessment is presented in the following pages.

Appendix:
Process and method

In the autumn of 2019, the coordination function initiated a knowledge inventory in order to produce a national risk assessment for 2020/2021. Based on the results from the previous national risk assessment from 2019 *(System Focus),* the working group for the national risk assessment decided that the approach for this year's assessment would be to perform a more in-depth analysis of areas that fall under the scope of the Anti-Money Laundering Act's application (*Sector-based Approach*).

The EU's supranational risk assessment (EUSNRA) was used as a model for this risk assessment. The advantage of the EUSNRA was that it contained both qualitative and quantitative assessments of money laundering and terrorist financing, as well as product and sector descriptions. Another reason the EUSNRA was used as a model was that it allowed for the harmonisation of the Swedish national assessment with the EU's assessment.

Four main steps were taken in the creation of the national report:

STEP 1. In the autumn of 2019, the working group adopted a joint project plan and 40 issues to address in relation to threats and vulnerabilities. The purpose of identifying issues to address was partly to facilitate the identification and sorting of relevant information, and partly to be able to more easily assess information before developing a risk matrix. The matrix was designed using a number of specific variables and indications as well as overall parameters.

FIGURE Risk matrix

Risk Criterion Parameter Indicator		
Threat of money laundering and terrorist financing	Scope	1. Capacity – number of actors
		2. Extent of money laundering
	Accessibility	1. Capacity of threat actors
	Attractiveness	1. Anonymity
Vulnerability to money laundering and terrorist financing	Ability to detect	1. Cross-border flows
		2. Speed and traceability of transactions in the sector
		3. Development rate
		4. The quality of operators monitoring system
	ikelihood of prosecution and conviction	1. Opportunity for prosecution and conviction
		2. Sector-specific legislation
	Regulatory compliance	1. Risk awareness in the sector
		2. Regulatory compliance in the sector
		3. Reluctance to report

All authorities were asked to collect both quantitative and qualitative data for this risk assessment and the matrix.

For the *supervisory authorities* (including the Swedish Bar Association) within the coordination function, this included engaging in dialogue with sectors and members, as well as gathering data through surveys distributed to operators or the analysis of periodic reporting.

Law enforcement authorities collected data from a variety of sources, including intelligence, in order to develop a sector-specific knowledge bank on threats linked to money laundering and terrorist financing.

In addition, specific material was ordered from research bodies (the Swedish Defence Research Agency, FOI), and products relevant to the risk assessment were internally produced (e.g. a review of all money laundering judgements during the years 2018/2019).

STEP 2. In 2020, a number of working group meetings were held with law enforcement agencies, supervisory authorities, industry organisations and voluntary organisations. A special method group was established to ensure that the risk assessment followed the same assessment template between the working group meetings. The method group was tasked with ensuring quality, clarity, reliability and validity. All members of the coordination function were invited to participate in the process.

In parallel with the collection and processing of information, an analysis and writing phase was initiated in the autumn of 2020. The data was regularly shared among members of the working group responsible for creating the risk assessment, allowing all members of the coordination function to be informed and involved in the decision-making process.[133]

STEP 3. During the autumn of 2020, the material collected for each identified issue was evaluated by sector (see the indicators/parameters in the matrix). This resulted in a risk value for each sector.

The sectors were assessed based on threats and vulnerability, which are specified in the matrix below and in the risk scale:

Risk scale

During the process of developing the assessment, the working group decided that only money laundering risks would be assessed quantitatively, while risks linked to terrorist financing would be assessed qualitatively.

The result of the assessment for each indicator in the matrix was defined based on a risk scale.

The scale indicates the threat and vulnerability level for each sector. The

[133] The working group included all members of the coordination function, but not the Swedish Prosecution Authority.

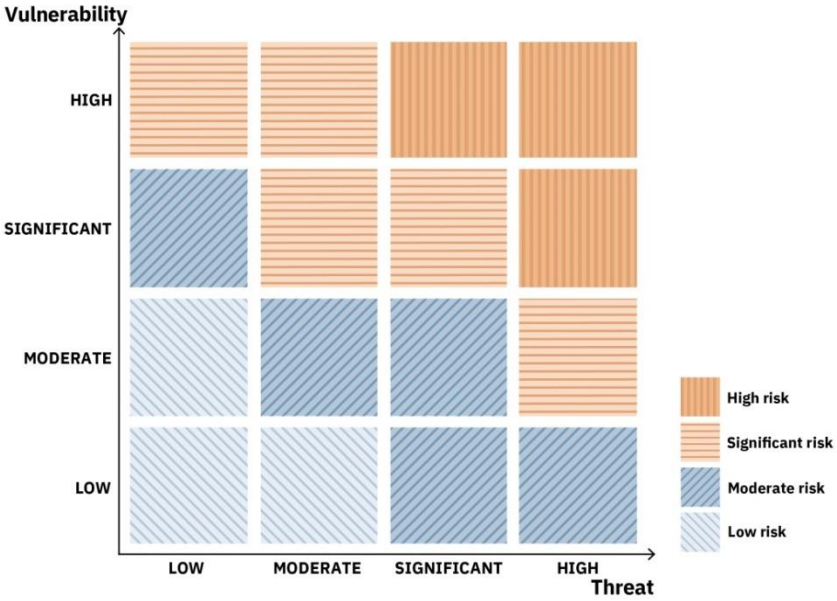
assessment of threats and vulnerabilities for each sector was initially scored on a scale of 1–100, and then converted to a value between 1–4. The assessments of threats and vulnerabilities were then weighed together to generate a risk level according to the procedure illustrated in the matrix below. If the threat is assessed at the highest level (4), and the vulnerability level is assessed to be at least significant (3 or 4), the weighted risk is classified as high (4). The same applies to the highest level of vulnerability, that is, if it is combined with a high or significant threat level.

However, as is shown in the matrix, the distribution is not entirely symmetrical when weighing the risk levels moderate (2) and significant (3):

- *Risk value 2* results if a threat value is assessed to be 3 and the vulnerability value is assessed to be 2.
- *Risk value 3* results if the threat value is assessed to be 2 and the vulnerability value is assessed to be 3.

The slightly greater emphasis placed on vulnerabilities in assessing risk is consistent with the methodology in the EU's supranational risk assessment and is based on the assumption that vulnerabilities can lead to future threats.

Matrix for threats, vulnerability and risk



The criteria for the risks are given in the table below.

TABLE Risk criteria for Threats and Vulnerability

Risk criteria	Low (1)	Medium (2)	Significant (3)	High (4)
Threat	No indications criminals intend to use this approach for money laundering.	Criminals have capacity to use the sector for money laundering.	Criminals use the sector for money laundering.	Criminals use the sector repeatedly for money laundering.
Vulnerability	Negligible risk of money laundering given effective barriers and control systems.	Some risk of money laundering in the sector as the sector has effective but not completely impervious control system	Significant risk that the sector will be used for money laundering as control systems have limited effect.	High risk that the sector will be used. Control systems are lacking or are not suitable for the purpose.

Consequence scale

After assessing threats and vulnerabilities, the results were analysed based on the impact model for society at large. The consequence of money laundering was assessed based on the sector's *turnover/power* (1–4) and the sector's estimated *societal impact* (1–4).

TABLE Impact assessment template based on a sector's scope (size)

Scope/power		Social impact	Weighted results
How much money is handled in the sector?	**How suitable is the sector for large-scale money laundering?**	**How is society at large impacted?**	
< SEK 5 billion	Conditions are completely unsuitable for large-scale money laundering in the sector.	Only individual operators are affected.	1
SEK 5-250 billion	Certain conditions exist for large-scale money laundering in the sector.	Money laundering can have a negative impact on the entire sector, for example, damaged confidence.	2
SEK 250-1000 billion	The sector can play a significant role in large-scale schemes.	Negative effects that impact society at large can arise outside the sector, such as inflated property prices.	3
> SEK 1 trillion	The sector fills a necessary function in large-scale money laundering schemes.	Money laundering can have a negative impact on the national level, for example, threatening financial stability or Sweden's international reputation.	4

STEP 4. After completing the sector assessment, both with regard to individual sectors and the national consequences, the working group analysed the results and adjusted the assessments that had values that bordered between different risk levels.

Over the course of its analysis work, the working group also put forward a number of preliminary proposals for risk mitigation measures to reduce the risk of money laundering and terrorist financing at the national level.

Appendix: Special challenges for county administrative boards

While producing material and information for the national risk assessment, it became evident that the county administrative boards face special challenges. The county administrative boards have limited resources in relation to the number of operators who are under their supervision. The operators who fall under the scope of the county administrative boards' supervisory assignments come from a wide variety of different sectors. Other authorities – which, similar to the county administrative boards, have a supervisory assignment based on the money laundering regulations –
also carry out other forms of supervision within their area of responsibility. Some authorities also have an authorisation procedure, where the operators are required to apply for authorisation and be approved before being allowed to operate a particular business. This is not the case for operators who fall under the scope of the supervision of the county administrative boards (apart from pawnbrokers).

Below is a description of some of the main challenges the county administrative boards face, which were identified in connection with the preliminary work to develop the national risk assessment.

County Administrative Boards' information collection

In preparation for the national risk assessment, the county administrative boards sent out questionnaires in the spring of 2020 to all the operators who were registered in the Swedish Companies Registration Office's anti-money laundering register on 1 December 2019. About 75 percent of these responded to the survey. When analysing the answers, it was noted that some operators misunderstood the questions. This applies, for example, to questions about the business's turnover and the number of employees.[134] This had a negative effect on the sector assessments and the descriptions of the sectors under the supervision of the county administrative boards.

The county administrative boards also noted that there were a number of operators who responded to the survey based on the assumption that they conduct activities with a reporting duty, even though they do not. Furthermore, as the accuracy of the survey answers regarding the operators' turnover and number of employees can be called into question, the county administrative boards have

[134] In terms of turnover figures, several respondents misunderstood the direction that turnover should be stated in thousands of kronor (SEK thousand) and instead stated the entire sum, i.e. in kronor (SEK). In terms of the number of employees, several respondents stated that the value was zero, even though the number should include the owner and management.

instead obtained this information from the search service *Retriever.*[135] Retriever can retrieve public information, such as annual reports, which are submitted to different authorities.

The key figures presented in the sector descriptions come from the above-mentioned search service and are therefore based on statistics from annual reports submitted to the authorities. Therefore, they cannot be considered reliable figures. However, this does not apply to the operators who run individual companies. Individual companies rarely have an annual report from which information can be retrieved. Therefore, information regarding the turnover and number of employees for individual companies could not be retrieved from the search service.

Given the problems described above, the figures and conclusions that the county administrative boards present in their sector descriptions should therefore be seen as likely estimates rather than facts.

Unregistered operators

Operators subject to the county administrative boards' supervision do not need a special permit[136] to conduct their businesses. However, they are obliged to report their activities to the Swedish Companies Registration Office's anti-money laundering register. It is likely that there are a substantial number of operators who, despite being subject to the reporting duty, have not reported their activities to the register. This contributes to deficits in the information that the county administrative boards have about the operators in the sectors that are subject to their supervision.

Registration error

During supervision or major mailings to registered operators, the county administrative boards found that a number of these operators do not conduct activities subject to the reporting obligation. There are believed to be several reasons for these incorrect registrations. Operators may have changed the activities they conduct since initial registration. It may also be due to a misunderstanding or misinterpretation of the law, which may mean that operators who are not covered under the scope of the Anti-Money Laundering Act have responded to the county administrative boards' questionnaire.

[135] www.retrievergroup.com/sv/

[136] In order to conduct pawnbroker activities, a permit must be granted by the county administrative boards.

SAMORDNINGSFUNKTIONEN MOT PENNINGTVÄTT OCH FINANSIERING AV TERRORISM