



National Risk Assessment of Money Laundering and Terrorist Financing in Sweden 2024/2025

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

Abstract

This is the fifth report from the Coordination Function on the national risk assessment and of money laundering and terrorist financing in Sweden, and an update of the national sector-based risk assessment from 2020/20221. The Coordination Function consists of 16 public authorities and the Swedish Bar Association. The assessment is based on identification and analysis of threats and vulnerabilities according to the breakdown of sectors covered by the areas of application of the Swedish Anti-Money Laundering Act (AML act). The sectors have been risk assessed and the risks compared in a national context regarding the consequences they have for 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 and vulnerabilities are presented.

Money laundering risk assessment

Compared with the risk assessment from 2020/2021, the general risk level is deemed to be higher and more of the sectors are elevated to the highest risk level. The higher risk level is mainly due to the threat from organised crime, which is deemed to have increased and that crime has become much more integrated in the legal social structure. A partial explanation may also be that the authorities have gained more insight into crime, and the capability of threat actors since the previous risk assessment.

With regard to the social impacts that money laundering can lead to, the four sectors are deemed to be associated with high risk in a national perspective. These sectors are banking and financial, payment institutions, accountancy and auditing services and estate agents.

Risk assessment regarding terrorist financing

The infrastructure needed by organised crime to process and launder its proceeds is also used for financing terrorism. In contrast to money laundering, which concerns the source of money, it is the objective that characterises the financing of terrorism. No predicate offence is required and many terrorist crimes have been financed with relatively low funds from legal sources. The financing of terrorism in Sweden is largely deemed to be aimed at support functions that facilitate security-threatening activities, such as logistic support.

Among the organisations receiving funds from sources active in Sweden, are Partiya Karkeren Kurdistan (PKK), Islamic State (IS), Hamas, al-Shabaab, al-Qaida and Hizbollah. The transfer of funds to recipients is done through the regular financial system and informal channels, such as Hawala and couriers who transport gold and other physical assets over the borders. The use of new technology, such as cryptoassets, is also known to occur.

Contents

1	Introduction	6
1.1	Purpose and target group	6
1.2	Regulations	6
1.3	Overall method, sources and implementation	7
1.4	References	7
2	The Swedish context	8
2.1	Greater threats from organised crime	8
2.2	The financing of terrorism in Sweden mostly concerns support activities	11
2.3	Strong defences to combat money laundering and terrorist financing	11
2.4	The need for facilitators increases the risk of corruption	14
2.5	Transfers to illegal financial businesses	14
3	Risk assessment – money laundering	15
3.1	Risk by sector based on threat and vulnerability assessment	15
3.2	National risk assessment with regard to consequences	17
4	Risk assessment – terrorist financing	19
4.1	Terrorist financing – in a Swedish context	19
4.2	The intentions and capabilities of those posing a threat	20
4.3	Collection procedures	20
4.4	Procedures used for disposal of the money	21
4.5	Organised crime and terrorist financing convictions	21
5	General risks	23
5.1	Missing counterpart details	23
5.2	Facilitators among obliged entities	23
5.3	Money laundering using businesses as tools of crime	24
5.4	Cross-border financial activities	26
5.5	Activities not covered by the AML regulations	27
5.6	Factors that complicate supervision	28
6	Risk-mitigation measures	29
6.1	Greater transparency regarding transactions and accounts	29
6.2	Instrument for accessing facilitators and illegal financial activities	30
6.3	Better ways of countering companies as criminal fronts	31
6.4	More efficient money laundering supervision	32

7	Sector catalogue	34
7.1	Banking and financial institutions	35
7.2	Life insurance business	45
7.3	Securities business	49
7.4	Certain financial business	53
7.5	Insurance mediation	57
7.6	Issuers of electronic money	61
7.7	Fund operations	66
7.8	Payment institutions	71
7.9	Registered payment service providers, account information services	79
7.10	Consumer credit operations	81
7.11	Mortgage lending business	83
7.12	Crowdfunding services	86
7.13	Cryptoasset service providers	90
7.14	Registered estate agents and estate agencies	95
7.15	The Swedish gambling market	101
7.16	Merchants	109
7.17	Pawnbrokers	114
7.18	Approved or authorised auditors or registered audit firms	117
7.19	Accountancy and audit services	122
7.20	Tax advisers	126
7.21	Lawyers and law firms	129
7.22	Independent lawyers	135
7.23	Trust administrators	138
7.24	Art dealers	140
7.25	Company formation agents and business brokers	144
7.26	Business centres and postbox service companies	147
7.27	Board representation and nominal shareholders	149
7.28	Currency exchange	150
8	Process and method	155
8.1	Overall method and implementation	155
8.2	Definitions of threat, vulnerability and consequence	155
8.3	Process	156

1 Introduction

This is the fifth report from the Coordination Function on the national risk assessment and of money laundering and terrorist financing in Sweden, and an update of the national sector-based risk assessment from 2020/20221. The assessment is based on identification and analysis of threats and vulnerabilities according to the breakdown of sectors covered by the areas of application of the Swedish Anti-Money Laundering Act (AML act). The objective of risk assessment is to boost awareness of the risks Sweden is exposed to, propose measures to reduce risk and to support the authorities and enforcers in their threat and vulnerability assessments and to work with risk-reducing measures.

Money laundering and terrorist financing represent a threat to the financial system and our democratic society. The landscape for money laundering and terrorism financing is variable, and despite constant efforts to reduce the risk of the financial and non-financial sectors being exploited for such purposes, further measures are needed to close loopholes in the system. A risk-based attitude towards working against money laundering and terrorism financing is important to achieve a functional and effective regime in which various elements of society work together. Several different types of actors are involved in Sweden, with the supervisory authorities, law enforcement agencies and private sector companies leading the way. Civil society is also affected by work to combat money laundering and terrorist financing. Combating money laundering and terrorist financing is not just national, but is also international, including via collaboration within the Financial Action Task Force (FATF) and at EU level through legislation, guidelines and recommendations.

1.1 Purpose and target group

The purpose of national risk assessment is to identify, understand and assess possible threats, vulnerabilities and risks within the sectors covered by money laundering law. It also includes risk-reducing recommendations on the basis of the threats, vulnerabilities and risks that had been identified. The aim is to increase knowledge and awareness regarding the risks of money laundering and terrorist financing.

The national risk assessment is mainly directed to the obliged entities covered by the regulations on money laundering and terrorist financing, but also to the supervisory authorities, government offices and Coordination Function members.

1.1.1 The Coordination Function

The Regulation (2024:1367) on a Coordination Function for Measures Against Money Laundering and Terrorist Financing stipulates that there must be a Coordination Function within the Swedish Police Authority. The Coordination Function shall continuously identify and analyse the risks and methods for money laundering and terrorist financing in Sweden. It must also compile, update and publish national risk assessments for money laundering and terrorist financing at least every four years or as and when required.

The following 16 authorities, along with the Swedish Bar Association, fulfil this function: The Swedish Companies Registration Office, the Swedish National Council for Crime Prevention, the Swedish Economic Crime Authority, the Swedish Estate Agents Inspectorate, FSA, 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.

1.2 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 resilience: administrative and penal. The administrative regulations are key to preventing and countering financial businesses and other commercial activities being exploited for money laundering and terrorist financing. The administrative regulations mainly comprise the Anti-Money Laundering Act and is complemented by the various company acts and the Act on Company Principals (2017:631). The penal regulations seek to prosecute persons engaging in money laundering or terrorist financing and are mainly composed of the Act on Penalties for Money Laundering Offences (2014:307) and the Act on Terrorist Crimes (2022:666).

1.3 Overall method, sources and implementation

Analysis has been based on the FATF's method for risk assessment of the threat of money laundering and terrorist financing. The report is based on quantitative data and qualitative argumentation from the expertise of the Coordination Function's members.

The report analyses threats and vulnerabilities for the sectors covered by the areas of application of the money laundering act. See chapter 7 of the Sector Catalogue. Threats concern the capability of actors seeking to exploit a sector for money laundering and terrorist financing. Vulnerability covers the limitations and possible breaches within the respective sectors concerning their ability to resist threats and prevent money laundering or terrorist financing. The assessment of threats and vulnerability gives a risk value for each sector. The impact on society that can be caused by the risks is then analysed. The threats, vulnerabilities and risks presented in this report comprise the result of the Coordination Function's overall assessment.

Sources from all the Coordination Function's members have been used for this risk assessment. The Coordination Function's members have contributed quantitative data, qualitative argument and specialist skills through questionnaires and working group meetings in the form of descriptions of procedures, threats and vulnerabilities. Statistics of suspicious activity reporting (SAR) to the FIU and crime statistics from the Swedish National Council for Crime Prevention, the Swedish Prosecution Authority and the Swedish Economic Crime Authority have also been compiled. Dialogue has also been conducted with industry and sector representatives and parts of the charitable sector. An important factor has also been intelligence from the law enforcement authorities. Information from the various sources has been merged and used for the analysis.

Access to the information has been limited to certain sectors. The County Administration Board supervision service covers many and varied sectors, within which reliable data has been limited. Information on these sectors is therefore based to a large extent on trends and lessons learned from supervision of the County Administration Boards and through collaboration with other authorities and the opinion poll conducted by the boards in early 2020.

1.4 References

Risk assessment is divided into eight chapters. Chapter 2 provides an overview of Sweden based on situation, crime trends and changes in the law since the last sector based risk assessment. The aim is to provide a framework for the analysis and to describe the principle factors impacting the Swedish risk profile. Chapter 3 presents an overall assessment of risks for and consequences of money laundering in Sweden. Chapter 4 presents an analysis of the risk of terrorist financing in Sweden. The report covers the ability of the actors and procedures for terrorist financing, and what the consequences can be. Chapter 5 describes the overall risks deemed to impact several sectors, and should be read in addition to the sector-specific section. Chapter 6 presents proposals for risk mitigation measures at national level. Chapter 7 gives a description of the risks of money laundering and terrorist financing in the various sectors. Finally, chapter 8 presents a detailed description of the definitions, processes and methods of the risk assessment.

2 The Swedish context

The Swedish economy is small and open with its own currency, relatively large financial sector and a high level of digitalisation. The payments market is, in principle, fully digital and the use of cash is amongst the lowest in the world.¹ But cash is still deemed to account for a large part of the criminal economy² including as a means of payment for drugs. The criminal economy is deemed to turn over an amount in the billions in Sweden annually, with the money primarily coming from financial crime such as tax fraud, employment market crime and welfare crime, as well as from drug sales and embezzlement. Welfare criminality has revealed the vulnerability of the Swedish trust-based social contract, which has driven the development towards a more control-based system in which more authorities and municipalities have been delegated law enforcement responsibilities.

In a global perspective, organised crime continues to be at a relatively low level in Sweden, but the threat has gradually increased and is now deemed to be higher compared with the other Nordic and Baltic countries.³ The main characteristic of Swedish organised crime is deadly force connected to the criminal networks, which is clearly higher per capita than average for Europe.⁴ The use of deadly force also kills innocent victims to a greater extent than previously.

The criminal networks driven by financial gain and the underlying conflicts are often due to competition for criminal proceeds. Turning the tide therefore requires powerful measures to curtail the ability of those involved to earn and process criminal proceeds. The authorities and enforcers have a key role to play to break the chain of criminal proceeds. Proceeds from drug sales on the streets for example are converted, aggregated and gradually end up in the business accounts of Swedish banks where they can be invested in property, for example, or transferred abroad. If all the obliged entities in the chain adopted sufficient customer due diligence procedures, it would become significantly harder to run a criminal activity. The authorities can make it easier for the obliged entities, including providing reliable registers and sharing information, but will also have to conduct supervision and adopt measures for the obliged entities to live up to requirements.

2.1 Greater threats from organised crime

Drug sales and embezzlement are deemed to be the main sources of income for criminal networks in Sweden. The number of reported crimes in these categories has long been on the increase and accounted for nearly a quarter of all crimes reported in 2024, see diagram 2.1. Theft has dropped significantly over the last few decades. The statistics are an indication of the growing threat from organised crime in Sweden and how various preludes to money laundering have changed over time.

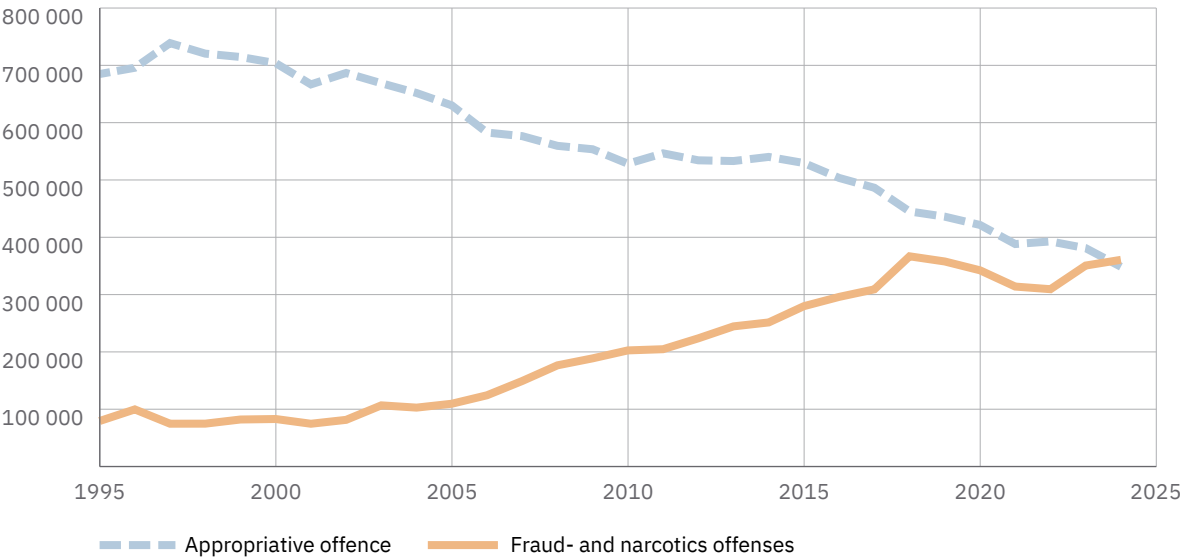
1 Swedish Central Bank, *Betalningsrapport 2025* (In Swedish).

2 "Criminal economy" covers the obtaining, laundering and reinvestment of criminal proceeds. Legal funds are also invested in criminal activities, such as the payment of black money and are also covered by the term.

3 Global initiative against transnational organized crime, <https://globalinitiative.net/initiatives/ocindex/>

4 The Swedish National Council for Crime Prevention, *Ökningen av skjutvapenvåld i Sverige*. (Brå 2024:7). (In Swedish).

Diagram 2.1 Reported crimes per year between 1995-2024

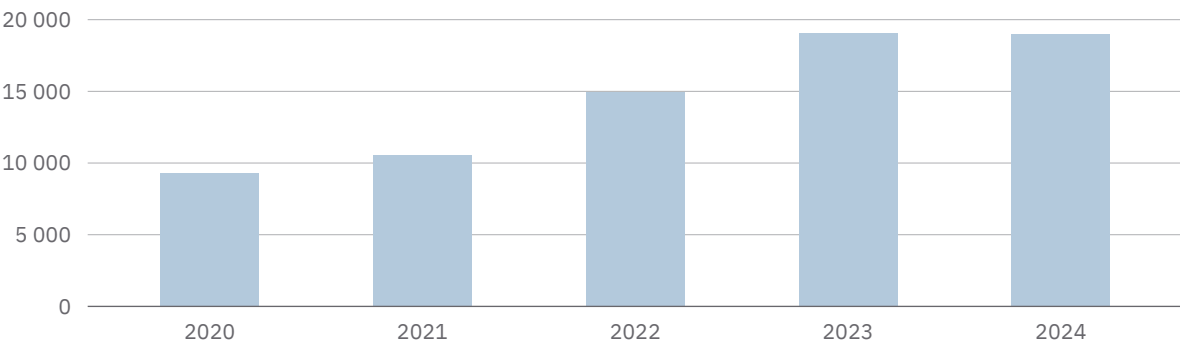


Source: The Swedish National Council for Crime Prevention

Proceeds from crime to be used in the legal economy have to be converted to seemingly legal earnings and assets at some stage. The large amounts generated within organised crime make totally different requirements for the way proceeds from crime are processed compared to individual criminals who can use their proceeds for private consumption or can launder money in their own regime. The volumes generated by organised crime require a systematic and large scale approach that requires access to companies and the services that Swedish obliged entities provide in the form of bank accounts, credit and audit services.

Society seeks to obstruct and prevent money from crime being laundered in the legal economy by various means. Legislation in this area has successively been tightened in line with awareness of the risks increasing for the obliged entities and authorities, whilst control systems to prevent money laundering have been bolstered. Since the AML act⁵ became law in 2014, the number of money laundering crimes reported has grown significantly. In 2024, the number of crimes reported during the year reached about 19,000, compared with just under 9,000 in 2020, see diagram 2.2.

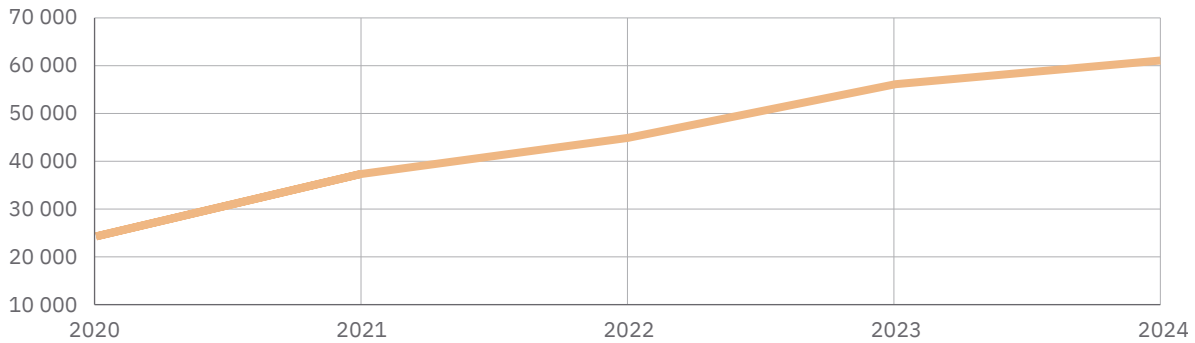
Diagram 2.2 Number of money laundering crimes reported



Source: The Swedish National Council for Crime Prevention

The number of suspected crimes reported to the FIU has also increased. In 2024, the FIU received over 60,000 reports of suspected money laundering or terrorist financing, which is more than double the 2020 level, see diagram 2.3. As can be seen from table 2.1, the banking sector stands for the majority of the change. Reporting from the non-financial sectors has also grown, but still only concerns a few incidents per year and is deemed to be under-reported.

⁵ Act on Penalties for Money Laundering Offences (2014:307).

Diagram 2.3 Number of reports to the FIU

Source: The Swedish Financial Intelligence Unit (FIU)

Table 2.1 Number of suspect reports per sector

	2020	2021	2022	2023	2024
Lawyers and law firms	1	1	1	1	2
Certain financial business	163	383	454	434	660
Banking and financial institutions	18 342	27 801	33 665	39 246	45 477
Payment services ¹	4 032	6 743	4 948	4 723	4 437
Accountancy and audit services ²	6	9	33	67	140
Company formation agents and business brokers, etc.	0	0	1	3	13
Mortgage lending business	12	8	30	19	8
Registered estate agents and estate agencies ³	5	6	41	38	92
Fund operations	2	2	6	8	9
Insurance brokers	0	1	0	1	1
Crowdfunding services ⁴		0	0	0	1
Institute for Electronic Money	13	4	41	301	560
Other independent lawyers	0	3	5	8	6
Art dealers ⁵	0	0	0	2	12
Consumer credit operations	87	138	224	340	389
Life insurance business	17	33	27	51	68
Pawnbrokers	12	17	21	23	37
Auditing ⁶	8	20	28	32	84
Tax advisers	4	0	2	0	4
Gaming service providers	907	1 444	3 897	4 995	3 715
Currency exchange and deposit businesses	270	325	1 275	5 306	4 729
Securities business	6	4	4	18	22
Professional trade in goods	122	116	118	154	69
Supervisory authorities	8	7	2	0	9
Other authorities ⁷	488	463	290	366	796
Total	24 505	37 528	45 113	56 136	61 340

¹ The category includes payment service providers and payment institutions.

² Non-approved or authorised auditors or unregistered audit firms.

³ The category includes estate agents as from 2021.

⁴ Crowdfunding services were introduced in the money laundering act in 2021.

⁵ Art dealers were introduced in the money laundering act in 2020.

⁶ Approved or authorised auditors or registered audit firms.

⁷ Cash declarations from Swedish Customs have been excluded since 2022.

Source: The Swedish Financial Intelligence Unit (FIU)

The number of persons prosecuted for money laundering has also increased in recent years. In 2024, just under 5,000 people were prosecuted, three times as many as in 2020, see table 2.2. An important explanation for the trend is the higher number of bodies tasked with preventing the legal economy being used to process criminal funds. Compared with previously, money has also come more into the foreground in combating crime.

Table 2.2 The number of persons prosecuted for money laundering

	2020	2021	2022	2023	2024
The Swedish Prosecution Authority	1 580	1 852	2 308	3 156	4 813
The Swedish Economic Crime Authority	76	119	66	94	189
Total	1 656	1 971	2 374	3 250	5 002

Source: The Swedish Prosecution Authority and The Swedish Economic Crime Authority

2.2 The financing of terrorism in Sweden mostly concerns support activities

The infrastructure needed by organised crime to process and launder its proceeds is also used for financing terrorism. There are also examples of overlap between organised crime actors and violent extremism.

The financing of terrorism in Sweden is largely deemed to be aimed at support functions that facilitate security-threatening activities, in the form of transport and logistics. It can also concern donations to associations running activities within radicalisation, recruitment and training for violent extremism. Among the organisations receiving funds from sources active in Sweden, are Partiya Karkeren Kurdistan (PKK), Islamic State (IS) and its offshoots, Hamas, Hizbollah, al-Qaida and al-Shabaab.

The funds mainly come from voluntary donations and originate from legally-earned and criminal sources. Apart from voluntary collections, funds are also derived from blackmailing under threat of reprisals, similar to the threat profile arising from protection rackets within organised crime.

The laundering of the funds collected is performed through obliged entities in the regular financial system and through other, illegal channels. Hawala is a trust-based, informal means of transferring funds well established within a majority of diaspora in Sweden. Hawala offers low transaction costs and is often the only way to send money to certain areas, e.g. conflict zones. The Hawala system risks being used as a channel for terrorist financing, e.g. through transactions to conflict zones or areas where the financial infrastructure has broken down, or where targeted financial sanctions have been imposed.⁶ Another means of transferring funds to terror organisations is to physically transport gold and other valuables over borders. Such courier activities are deemed to be common between foreign intermediaries with suspected connections to terror organisations in the Middle East.

2.3 Strong defences to combat money laundering and terrorist financing

Legislation in the area has been developed rapidly and the preceding sector-based risk analysis has introduced secrecy-breaching rules that make it possible to collaborate and share information to a much greater extent than previously. The AML regulations have also been extended to cover more types of obliged entities. The law enforcement agencies have also been given more opportunities to confiscate criminal proceeds and several authorities have been tasked by the government with helping combat crime.

6 The Swedish Police Authority/the Coordination Function, *National Risk Assessment 2022 – Hawala: value changes in the alternative payment system*. Ref. no. A243.461/2023.

2.3.1 Better access to information

New legislation designed to improve access to relevant information includes:

Opportunities for operative collaboration according to chapter 4a in the AML act

The chapter was included in 2023 and introduces new forms of collaboration to deter, prevent or detect serious money laundering and terrorist financing. The addition permits collaboration between law enforcement agencies, the Financial Supervisory Authority (FSA) and credit institutions, and between law enforcement agencies and all authorities responsible for supervision according to the Anti-Money Laundering Act (AML).

Better information flow for combating crime

A new law⁷ that came into effect on 1 April 2025 improves ways of municipalities, regions, schools and authorities sharing information with law enforcement agencies to give them better chances of preventing and combating crime. They are obliged to pass information to the law enforcement agencies upon request and on their own initiative without secrecy representing an obstacle.

More information exchange between authorities

On 1 December 2025, a new secrecy-breaching provision⁸ came into effect, which ensures more information sharing between authorities. The provision is intended to give authorities access to information needed to be able to work more efficiently. Information held by one authority can sometimes be decisive for another to be able to fulfill its duties. The act makes it possible to share details on the personal or financial circumstances of an individual to another authorities if needed to investigate a crime, and to prevent or detect criminal activities, false payments and similar types of infringements.

Better access to obtaining details of electronic communication

The scope of the Data Collection Act⁹ has been extended to allow the FIU to collect information about electronic communications in the case of serious money laundering or business money laundering and serious crime if the measures are particularly important for deterring, preventing or detecting criminal activities deemed to be taking place in an organised form or systematically.

Better conditions for quality assurance of public registers

Since the preceding sector-based risk analysis, the Swedish Companies Registration Office has been given a clearer law enforcement role to counter crime committed within the framework of a company. A change in the law has given the authority greater powers to check and correct details in the register. The authority has also been allowed to demand personal attendance.

2.3.2 Tighter rules for obliged entities

The legislation that regulates the requirement for obliged entities has also been tightened and extended through:

Tighter licencing obligations

Currency exchange and payment services are now subject to licencing instead of the duty to register. The regulations have also been tightened with regard to consumer credit and only banks and credit market companies are now allowed to conduct such activities. Cryptoasset services are also an areas in which new requirements on permits for being able to operate such activities have been introduced. These tighter regulations are expected to raise entry barriers for fraudulent businesses.

⁷ The Act on the Obligation to Provide Information to the Law Enforcement Authorities (2025:170).

⁸ Prop. 2024/25:180.

⁹ Act on the Collection of Data on Electronic Communication in the Intelligence Operations of Law Enforcement Authorities (2012:278).

Criminal liability for illegal financial activities

In March 2026, a new act¹⁰ was introduced making financial activities conducted without a permit or registration with the Swedish Financial Supervision Authority illegal. The purpose of the new act is to combat money laundering and terrorist financing through such unlicensed businesses. In addition, the Financial Supervisory Authority can now impose fines on any organisation without the necessary licence or registration.

Extended duty to provide details

According to the AML act, clearing companies and providers of financial infrastructure handling immediate payments have been obliged since 2024 to provide the Swedish Police Authority (FIU) or the Swedish Security Service with all details needed for an investigation into money laundering or terrorist financing without delay.

Monitoring and reporting obligations for clearing companies

Since 2025, clearing companies are responsible for monitoring transactions between clearing participants which are also obliged entities. If a transaction is identified through such monitoring that can be assumed to be part of money laundering or terrorist financing, the clearing company must pass the details of its suspicions concerning the relevant obliged entities, and, if there are reasonable grounds for suspecting money laundering or terrorist financing or that property is deemed to originate from criminal actions, they must report the circumstances to the FIU.¹¹

New obliged entities

Since the last sector-based risk analysis, new obliged entities have been included in the AML act. The obliged entities added are providers of crowdfunding services which were included in the AML act of 2021, the suppliers of cryptoasset services added through an EU regulation in late 2024 and commercial art dealers, which, up to 2020, were only included for transactions that receive or pay out in cash. In 2021, the rules were extended to include registered estate agent firms and not just the individual estate agents.

2.3.3 New instrument for recovering criminal proceeds

A new instrument was introduced in autumn 2024 for recovering criminal proceeds in the form of so-called independent confiscation. The law makes it possible to confiscate property if it is clearly more than probable that property is the result of criminal activity rather than any other form of activity. Independent confiscation does not require that the property is linked to any specific crime or criminality of a given type, as it is sufficient if the property can be linked to an unspecified criminal activity. Most types of assets can be involved: accounts, cash, securities, cryptoassets, luxury goods, gold, vehicles, properties etc. The law is deemed to be very effective with regard to preventing actors higher up the criminal hierarchy from benefiting from criminal proceeds as it is often harder to prove specific crimes at this level.

2.3.4 Reduced money laundering of Swedish cash abroad.

The transportation of cash represents a common link in international money laundering. The purpose is often to introduce criminal proceeds into the legal economy by various means, especially via countries where there are plenty of opportunities to place cash in the financial system. Money laundering of Swedish cash via currency exchange abroad was previously estimated to be in the billions¹² every year, but is deemed to have been strongly reduced as there are no longer any obliged entities in Sweden that accept cash deposits from foreign banks. There may still be cash transfers in an out of the country outside the legal economy, such as within the framework of illegal Hawala activities.

¹⁰ Prop. 2025:26:42.

¹¹ Chapter 4, section 3a of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

¹² The Swedish Police Authority, *Penningtvätt genom utförsel av kontanter*. Ref. no. A320.761/2023. (In Swedish).

2.4 The need for facilitators increases the risk of corruption

As described above, a lot has been done since the last sector-based risk analysis to strengthen defences against money laundering and terrorist financing. The value of combating the criminal economy has also been the subject of ever-growing focus in the social debate, which has contributed to greater awareness of the risks of money laundering.

Meanwhile, criminal actors still need to launder money systematically and on a large scale, which means the services of the Swedish obliged entities are also required. This implies that criminals must find ways of getting around the control system and avoiding detection, and this is where facilitators play a key role.

Facilitators are a phenomenon which are attracting the increasing attention of the Swedish authorities. The term covers people engaged in legitimate activities from helping criminal networks through their employment or tasks. Such persons can, for example, provide advice on how to avoid checks, falsify employer certificates or open a bank account. The facilitator is often paid for their services, but can also be blackmailed and threatened to assist criminals. Many of the cases detected concern facilitators who are related to members of the criminal network, but also childhood friends and customers of persons in criminal networks are common, despite them being harder to detect.¹³ Facilitators who systematically and for payment offer their services for money laundering are known as professional money launderers or PMLs.¹⁴ PMLs can act on behalf of several different groups.

What facilitators engage in can in many instances be called corruption, i.e. abusing their position of employment or duty to the benefit of themselves or others. Europol has estimated that 60% of the criminal networks active within the EU use corruption as a means of exercising their criminal activities.¹⁵ A corresponding estimate for the Swedish element has not been made, but corruption is deemed to comprise part of the criminal infrastructure in Sweden as well. The frequency of such "corruption brokers", i.e. a middleman between recipient and one or more bribers indicates a more industrialised and professional use of bribes.

Sweden is still regarded as one of the least corrupt countries in the world, but has slipped in the rankings in recent years.¹⁶ Against a background of the threat from organised crime, the risk of corruption and uninvited influence continues to grow in Sweden. Trade associations have indicated that their members are increasingly being forced to provide services to criminals, e.g. falsified accounts or compiling false data.

2.5 Transfers to illegal financial businesses

Another consequence of higher risk awareness and tighter controls in many obliged entities is that criminals are seeking other ways to process criminal proceeds. Criminals have been known to run what appears to be a legal financial business to be able to launder money on a large scale. Purely illegal financial businesses have also been known to be run without a permit, and therefore not subject to controls and supervision. Such illegal services can involve illegal Hawala, transport, currency exchange, cash exchange, cryptoasset exchange and credit provision. Such illegal services are systematically offered by international money laundering networks, and believed to turnover billions in Sweden every year.¹⁷ The phenomenon is known as underground banking, and comprises a fertile bed for parallel social structures that fertilise the criminal economy.

The providers of illegal financial services are to various degrees and at some point dependent on the legal economy and banking system for their own handling. Even if they consequently leave certain tracks in the regular financial system, they are very hard to detect. Complicated structures of various network clusters in multiple countries are often involved. To deal with such crimes requires effective measures that reduce vulnerability in the sectors and access to information and collaboration between the authorities and obliged entities in Sweden, and between law enforcement authorities abroad.

13 The Swedish National Council for Crime Prevention, *Möjliggörare för kriminella nätverk, Om möjliggörare i kommunal, statlig och privat sektor*. (Brå 2024:2). (In Swedish).

14 PML is an abbreviation for professional money laundering.

15 EU Socta 2021 – *Serious and Organised Crime Threat Assessment. A corrupting influence: The infiltration and undermining of Europe's economy and society by organised crime*. Europol, 2021.

16 <https://www.transparency.org/en/cpi/2024>

17 *Finanspolisen informerar: Underground banking i Sverige*, August 2025. Ref. no. A067.512/2026. (In Swedish)

3 Risk assessment – money laundering

This chapter presents the overall result of risk and consequence assessment regarding money laundering. Firstly, an overview of the sector-specific risks is given, based on assessment of threats and vulnerabilities in respective sectors. A report on the overall national risk assessment follows, in which the analysis also considers the consequences of money laundering in a broader social perspective.

Sector breakdown in the national risk assessment is based on how the obliged entities are covered by the areas of application of the Swedish legislation on money laundering. The assessment concerns the risk of the obliged entities in a sector being exploited for or participating in money laundering. The procedures for money laundering can differ, as the services exploited can also be provided by obliged entities from other sectors. An example is the mortgage lending sector, which is primarily composed of small organisations licenced to provide credit, credit brokerage and advice to consumers, but does not include banks and credit institutions which also provide the same services. This is worth remembering when interpreting the result, not least with regard to consequence assessment taking into account sector size.

3.1 Risk by sector based on threat and vulnerability assessment

To be able to compare results, the assessment of threats and vulnerabilities is based on the same scale as in the previous sector-based risk analysis from 2020/2021. A couple of sectors have been added and another couple adjusted as a result of a change in the law. Otherwise, the biggest change is that the risk level is generally deemed to be higher compared with the last analysis. As can be seen in table 3.1, there are now no less than 16 sectors that have the highest risk level for money laundering.

The higher risk level is mainly due to the threat from organised crime, which is deemed to have increased and that crime has become much more integrated in the legal social structure. Criminal actors have the capability to use companies in their criminal activities and recruit or place facilitators who can help them circumvent various control systems.

A partial explanation may also be that the authorities have gained more insight into crime, and the capability of criminals. In recent years, investigations and intelligence, e.g. insights into encrypted communication between criminal actors, have both shown that the economic capacity of organised crime, the occurrence of corruption and awareness and ignorance all facilitate money laundering. The last sector-based risk assessment can therefore have underestimated the ability of criminal actors to exploit the services of obliged entities for money laundering.

Table 3.1 Risk by sector of money laundering

Sectors under the Swedish Financial Supervisory Authority	Threat level	Vulnerability level	Sector risk			
Banking and financial institutions						✓ High
Payment institution						✓ High
Payment service providers ¹⁸						✓ Low
Mortgage lenders						✓ High
Electronic money						✓ High
Fund operations						✓ Significant
Insurance mediation						✓ Moderate
Crowdfunding services						✓ Significant
Cryptoasset services						✓ High
Life insurance						✓ Moderate
Currency exchange						✓ High
Certain financial business						✓ Moderate
Securities						✓ Significant
Sectors under the County Administration Boards	Threat level	Vulnerability level	Sector risk			
Accountancy and audit services						✓ High
Company formation agents and business brokers						✓ High
Art dealers						✓ High
Business centres and postbox service companies						✓ Significant
Independent lawyers						✓ High
Pawnbrokers						✓ High
Tax advisers						✓ High
Trust administrators						✓ High
Merchants						✓ High
Sectors with their own supervisory body	Threat level	Vulnerability level	Sector risk			
Lawyers and law firms						✓ Significant
Estate agents						✓ High
Auditors						✓ Significant
Gambling						✓ High

Defences against money laundering are also deemed to have been strengthened in many of the sectors since the last sector report. Awareness of the risks of money laundering has grown in society and the alertness of obliged entities is generally deemed to be higher at this time. Many of the obliged entities have also overhauled their customer due diligence and checking routines. Despite the improvements, the control systems are still deemed to be inadequate to resist the major threat from criminal actors who need to continuously be able to launder large volumes of criminal proceeds. The level of vulnerability has therefore been adjusted upwards for some of the sectors, compared to the assessment made in 2020/2021. The background for threat and vulnerability assessment for the respective sectors can be read in chapter 7, Sector Catalogue.

¹⁸ Registered payment service providers only include account information services after a change in the law, see section 7.9.

3.1.1 Limitations in the assessment scale

The assessment scale used in this and the last sector-based risk analysis was formulated in accordance with the EU Commission's supranational risk assessment (EUSNRA). Given the way the levels of the scale are defined, the majority of the sectors are placed at the highest risk level. The steps of the scale are inadequate to differentiate between the sectors with high risk. Meanwhile, the lowest level on the scale implies such a low risk that it is only relevant for the sector of registered payment service providers, which, due to a change in the law no longer involves any activities that can be deemed to be exploited for money laundering. The Coordination Function therefore finds that the scale should be recalibrated before the next national risk analyses to give a more nuanced profile of risks associated with various sectors or procedures. For a more detailed description of the assessment scale and criteria, see chapter 8, Processes and approaches.

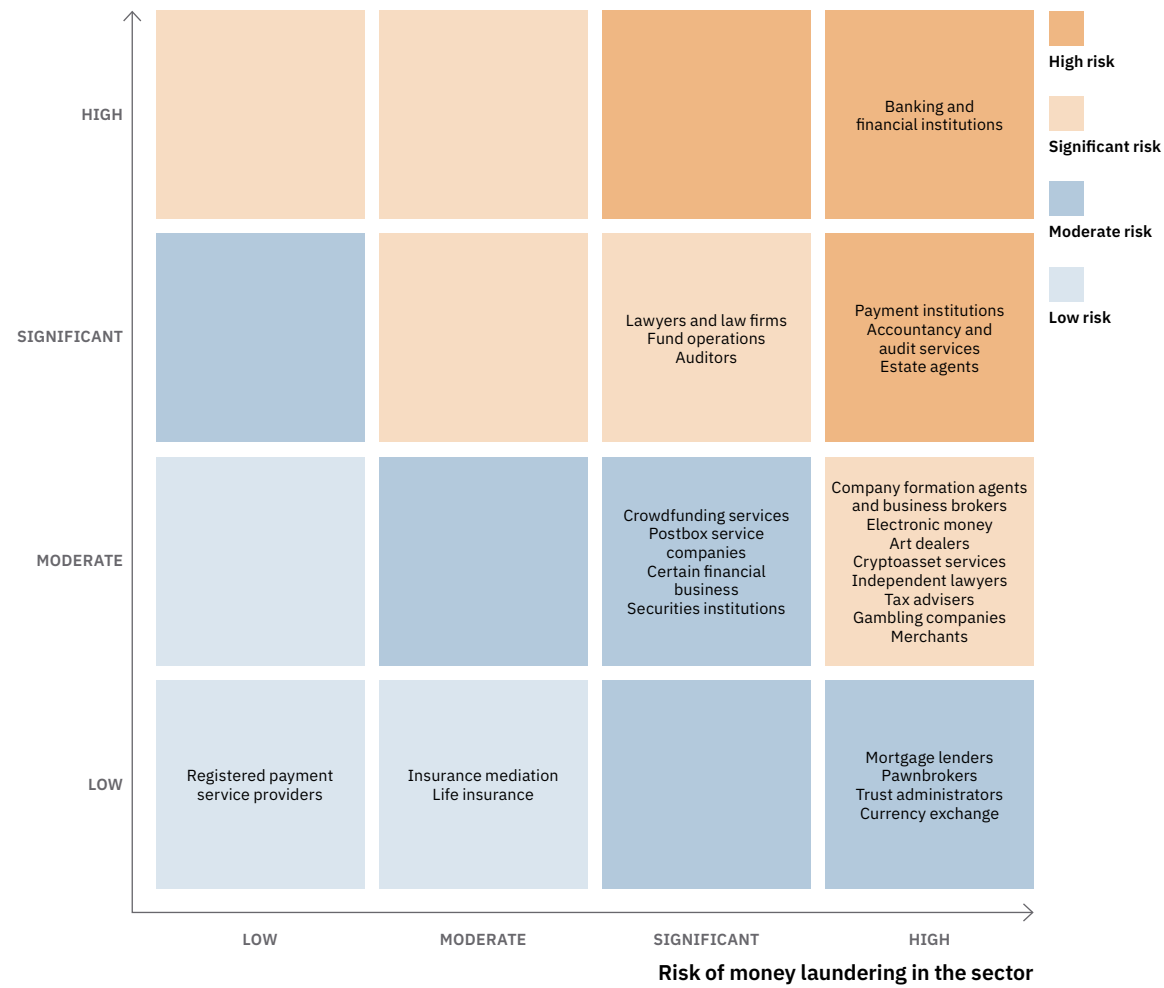
3.2 National risk assessment with regard to consequences

Apart from certain sectors that have been added or changed due to new legislation, the consequence assessment is unchanged in principle compared to the last sector-based risk analysis. The consequence assessment is based on two parameters: scope and social consequence. The first parameter is based on an estimation of how much money could potentially be laundered in the sector and the function the sector can fulfil for large-scale money laundering. The second parameter concerns to what extent negative diffusion effects can occur and affect other obliged entities in the industry, or cause damage to society, e.g. in the form of lost confidence in the judiciary or the financial system.

Given the consequence assessment, there are four sectors deemed to be associated with high risk in a national perspective. These sectors are banking and financial, payment institutions, accountancy and auditing services and estate agents, see table 3.2.

- **Banking and financial institutions:** Despite the banks' control systems improving in recent years, they are not deemed to be sufficient to prevent very large amounts of criminal proceeds being laundered through the sector. Apart from criminal actors thus being able to extract and benefit from their illegal gains, money laundering risks leading to loss of confidence in the financial system in Sweden. Given the high threat level, size of the sector and its importance to the financial infrastructure, the risk is deemed to be high in a national perspective.
- **Payment institutions:** The risk of money laundering in a payment institution is deemed to be on the same level as within the banking sector, but money laundering does not have the same consequence for society. Payment institutions also handle large transaction volumes, but do not offer the same opportunities for large-scale money laundering compared to the banking sector. Neither are the effects on society deemed to be on the same scale in terms of impacting confidence.
- **Accountancy and audit services:** With regard to this sector, it is primarily its size and the risks associated with companies as means to commit crime that explain the high risk level in a national perspective. The obliged entities in the sector should be able to fulfil a key function as guardians to prevent a company being exploited for criminal purposes.
- **Estate agents:** The threat level is deemed to be high, as property comprises an attractive means of laundering and investing criminal proceeds. Inadequate controls make it possible for Swedish and foreign criminal actors to launder large amounts through Swedish properties. The property market comprises an important part of the Swedish economy and extensive money laundering risks impacting confidence in the market's function and pricing.

Figure 3.2 Risk and consequence assessment at national level



4 Risk assessment – terrorist financing

This chapter presents how the terrorist financing can manifest itself in a Swedish perspective. The report covers the ability of the actors and approaches of terrorist financing, and what the consequences can be. Assessment of the individual sectors is reproduced in chapter 7, Sector Catalogue.

The main observations:

- **Low financial costs for the planning and execution of the attack.**
It is most likely at this time that a terror attack will be conducted by a lone individual or a small group, with simple means such as a vehicle, knife or firearm. This involves planning and preparation prior to an attack is not dependent on extensive funds.
- **Support activities are financed within Sweden.**
Terror organisations do not only need the right financial conditions to plan and execute a terror attack, they also need to maintain such things as infrastructure, recruitment, propaganda and training.
- **Income for terror activities comes primarily from collections through voluntary donations via physical and digital platforms, as well as criminal activities.**
Collections are made in cash and via deposits to accounts belonging to private individuals, associations, foundations and companies. The purpose of collections can be more or less transparent.
- **Money is primarily transferred through approaches that involve the banking sector, payment institutions, payment service brokers, Hawala and couriers.**
Such services are often used in combination with new technology such as cryptoassets.
- **Problems with obtaining evidence and overlap with other financial and organised crime.**
Convictions have previously been passed in Sweden regarding terrorist financing. A number of individuals suspected of terrorist financing have also been suspected, and in some cases prosecuted, for other crimes such as tax evasion, falsified accounts, theft, benefit fraud, drug crimes, smuggling and illegal trade in tobacco and other goods. But in recent years, several new convictions for terrorist financing have entered into force in the law, one in 2023, one in 2024 and three in 2025.

4.1 Terrorist financing – in a Swedish context

Obligated entities must report suspected money laundering or terrorist financing to the FIU. Transactions or suspicious behaviour can be reported, linked to terrorist financing. In contrast to money laundering, where the source of the assets is decisive – it is the objective that characterises the concept of terrorist financing. No predicate offence is required and many terrorist crimes have been financed with relatively low funds from legal sources.

The Terrorist Offences Act (2022:666) states that anyone collecting, receiving or providing money or other assets intended for the use of, or knowing that it is intended to be used to commit or in any other manner contribute to a terrorist crime, or attempting, preparing or conspiring to commit a terrorist crime, shall be convicted for terrorist financing. The same applies if the money or assets are intended to be used by a person, terrorist organisation or group of people committing or in any other manner contributing to terrorist crimes. The assets do not need to specifically be used for a terrorist attack. The provisions also apply to the financing of participation in or involvement with a terrorist organisation, public incitement to terrorism as well as recruiting, training or travelling for terrorism or in any other separate serious crime.

Terror organisations do not only need the right financial conditions to plan and execute a terror attack, they also need the capability to maintain such things as infrastructure, recruitment, propaganda and training. Terrorist financing in Sweden is primarily intended to strengthen various types of support activities rather than finance a terror attack. In this context, the activities that facilitate security-threatening activities are involved, such as financial, material and logistic support.

The Swedish Security Police regularly receive reports of actors in Sweden financing terrorism. These mainly involve persons and organisations suspected of financing terrorism abroad, but does include actors who pursue support activities within Sweden. An example of support activities in Sweden is people acting as facilitators and buying travel or arranging transport and accommodation for other individuals. Another example is making donations to associations running activities within radicalisation, recruitment and training for violent extremism. Elements of the suspected activity are well organised and involve multiple persons and organisations in Sweden and abroad, while other elements concern individuals. In several instances, there are overlaps between organised crime actors and violent extremism.

PKK is one of the most prominent organisations when it comes to collecting and distributing income from Sweden and the rest of Europe to support the central organisation. Apart from PKK; financing from Sweden is believed to go to other foreign terror organisations, including IS offshoots, Hamas, Hizbollah and al-Shabaab.

Given that international terror organisations have lost control over certain geographic areas, such as IS losing its territorial control in northern Syria and Iraq, they have also lost vital sources of income. This in turn has led to continued focus on cheap and simple alternatives for making attacks, rather than complex and expensive arrangements. This also means continued development of individuals acting along making attacks with simple means. It is also currently deemed most likely that terror attacks will be performed with simple means by an individual or small group. Experience shows that a large sum of capital is not needed for financial planning, preparation and execution of such attacks.

4.2 The intentions and capabilities of those posing a threat

A wide range of payment solutions – combined with rapid implementation of new technology – make collection and transfer of money quick, easy and at low cost. No extraordinary resources are needed in the form of specialist knowledge, advanced instruments or arrangements. No special ability is therefore necessary. In fact, international contacts are deemed to be a major factor for money finally reaching the intended recipient. Through the use of several collection methods and intermediaries in Sweden and other countries, the chances of concealment are increased.

Communication in social media and the use of digital banking and money transfer services support the collection and transfer of money. Thanks to the global reach of social media, many individuals can be reached by collection campaigns, propaganda and instructions for ways of sending money, e.g. cryptoassets. It is also on social media and digital platforms that many individual, mainly young, are radicalised and the intention to finance terrorism arises.

4.3 Collection procedures

The money suspected of being used for terrorist financing comes from various sources. It can be income from gainful employment, government or municipal contributions to private individuals or organisations as well as businesses and the sale of goods, services, property or companies. Capital from such sources can be legally or illegally acquired, and in several instances, both.

Collections and criminal activities are generally the leading ways of acquiring funds for terrorist financing on a large scale. Collections are made through physical and digital platforms and mainly in the form of voluntary donations. Collection campaigns are conducted by individuals and organisations, and can be in the public eye or in secrecy. Collection of money can be paid to accounts belonging to private individuals, associations, foundations and companies.

Digital platforms can consist of open channels on social media or closed fora where contact and an invitation are required to access the content. The advantage of digital platforms is that they generally reach a wide, international audience and that they can be simple to conceal who is collecting the money and the purpose of the collection.

Physical platforms include cultural associations and religious societies where collection is made physically in the form of cash and via deposits to an account. The purpose of the collection is not necessarily transparent, which means that in many instances, the donor is not aware that the purpose of the collection is wholly or partially to finance terrorism. Voluntary donations to collections are also used via aid organisations, including through collections being promoted as intended for support to crisis and conflict zones.

Apart from collections made through voluntary donations with more or less transparent purposes, there are also actors who not only run collections, but also obtain money from individuals and businesses for the purpose of financing terrorism. Out of fear for reprisals, such persons and businesses can find themselves forced to donate money. The activity can be compared to illegal tax collection, blackmailing and protection rackets.

4.4 Procedures used for disposal of the money

To transfer money from Sweden to terror organisations and individuals connected to these organisations abroad, licenced businesses can be used for illegal purposes. The banking sector and payment institutions are primarily used, but issuers of electronic money as well. Money can also be processed by persons and groups with no licence to do so according to the Act on Payment Services (2020:751), known as unregistered payment brokers.

Hawala brokerage is relatively well established within a majority of diaspora in Sweden. Hawala is an informal means of transferring money and is often independent of the international financial system, based on trust between the parties using it. The reason that Hawala is used in certain instances instead of, e.g. international payment service providers, is that the costs are relatively low and that it can be the only available alternative for transactions to certain areas of the world, including conflict zones. This makes the system attractive to actors who want to finance terrorism. A Hawala broker can apply for a licence as a payment institution for money transfers and be granted a licence from the FSA if the requirements are fulfilled. However, the majority of Hawala activities in Sweden are deemed to be run without a licence.

In common with the general public, violent extremists follow developments in technology and adapt and develop their operations accordingly. New payment solutions offer a wider spectrum of instruments. Violent extremists use virtual currencies amongst other things for their international transactions. Two reasons for doing so are the high level of anonymity offered for the sender and receiver, and that the currency is not linked to a specific issuer or state. On the other hand, there are some problems for terror organisations with converting the cryptocurrency once it has been received. Virtual currencies are also used as a means for courier and Hawala transfers.

Although new technological solutions offer violent extremists a wider spectrum of instruments, the traditional money transfer system continues to be very much in focus, as mentioned above. For example: payment institutions and Hawala are used to a great extent, as they generally can reach conflict zones at relatively low cost.

Using couriers is also a way of transferring money to terror organisations and involves cash or valuable objects, such as exclusive watches, gold and jewellery, being physically transported over borders. This is often done through intermediaries in countries outside Sweden, suspected of working for terror organisations in the Middle East.

4.5 Organised crime and terrorist financing convictions

Persons suspected of financing terrorism often commit other crimes. Criminal proceeds generated are suspected, individually or collectively with other capital, to be used for terrorist financing. The assessment of the information available is that terrorist financing in many cases overlaps other financial organised crime: tax evasion, falsified accounts, theft, benefit fraud, drug crimes, smuggling and illegal trade in tobacco and other goods. The purchase of goods and services on a black market can therefore have much greater consequences than the buyer is aware of.

Overlaps with other crimes also affect convictions within this field. Few convictions have been passed in Sweden regarding terrorist financing. There can be various explanations, including problems with producing evidence and that the Swedish Security Police focus more on prevention than prosecution. Several persons suspected of financing terrorism have been prosecuted for other crimes. But in recent years, several new convictions for terrorist financing have entered into force in the law, one in 2023, one in 2024 and three in 2025.¹⁹

On 20 September 2023, a person was convicted by Svea Court of Appeal for four years and six months for attempting to finance terrorism, a serious crime, by using the threat of violence to collect money for the PKK terror organisation. The report showed that PKK runs a very extensive collection network in Europe, including through the extortion of Kurdish traders. A highly-placed PKK leader is believed to have been in Stockholm and taken part in the decision that the plaintiff should pay money to the PKK.

On 27 November 2024, a person was sentenced to prison for one year for breaking the Act on Penalties for the Financing of Exceptionally Serious Crimes in Certain Instances (2002:444) (the predecessor to section 6 of the Terrorist Offences Act). The offender had conducted eight transactions to persons linked to al-Qaida and Hayat Tahrir al-Sham. The transactions were conducted by collections, principally via Swish. Transfers were then made from the offender's bank account via a cryptoexchanger to a cryptoplatform. The final recipients could then be identified through a block chain analysis.

On 14 February 2025, a person was sentenced to three years and three months in prison for terrorist financing, serious crime and other offences. The offender had collected, received and forwarded money to IS. He had send some of his own wages to cryptoaddresses owned by IS, and also helped IS by buying a e-visas to Ethiopia for a total of 28 people. In the latter instance, he received money from persons linked to IS and used it to pay for the e-visas.

On 9 February 2025, a person was sentenced to three years and ten months in prison for terrorist financing and serious crime. The offender was sentenced for two counts of terrorist financing. He had collected and received money via such channels as Swish and TikTok and forwarded it to IS via Western Union, cryptocurrency transactions and PayPal.

On 18 December 2025, a person was sentenced to three years and three months in prison for terrorist financing and other offences. the offender had forwarded money to IS by sending funds to cryptoaddresses owned by IS. He had also sent funds via other cryptoaddresses linked to various collection campaigns for IS, which was judged to comprise attempted terrorist financing.

¹⁹ Svea Court of Appeal, judgement 20.09.2023 in case no. B10051-23, Södertörns District Court judgement 27.11.2024 in case no. B6926-22, Attunda District court judgement 14.02.2025 in case no. B6548-24, Svea Court of Appeal judgement 09.12.2025 in case no. B14590-25 and Attunda District Court judgement 18.12.2025 in case no. B10593-24.

5 General risks

This chapter describes the general risks that are non-specific to individual sectors. It concerns the instruments used to make threats in the form of the use of companies and access to facilitators, and vulnerabilities in societies defences against money laundering and terrorist financing. Examples of such vulnerabilities include lack of transparency for accounts and transactions, as well as illegal activities despite the risks of money laundering or terrorist financing.

5.1 Missing counterpart details

Requirements for which details must accompany transfers of funds, such as whether the counterpart is regulated at EU level.²⁰ The main purpose of the regulation is to defend against criminal actors from concealing and transferring money from criminal activities and to prevent, detect and investigate the transfer of money from criminal activities, terrorist financing and other financial crimes.

Despite the requirements in pursuance of the EU regulation being in effect since 2017, it still lacks support in key parts of the Swedish payments infrastructure to handle the automatic transfer of necessary information.²¹ The fact that statutory details on account number do not accompany the transactions represents a clear vulnerability in the defence against money laundering and terrorist financing. Without access to the counterpart's account number, there is a risk that transactions and behaviour that should otherwise have a reasonable explanation can be perceived as suspicious, and conversely, that transactions for which such details should have aroused suspicion are not noticed by the obliged entities. These shortcomings can therefore allow actors to conceal the source of the funds, for example, by aggregating criminal proceeds from many donors in a bank, gambling or securities account. The FSA has ordered Bankgirot's Swedish bank owners to address the shortcomings by 31 December 2026. The order is directed to the Swedish owners of Bankgirot as they have the practical opportunities to ensure the shortcomings are addressed.

When reporting suspect transactions and behaviour to the FIU, valuable details on the counterpart are often missing, something that severely affects the FIU's ability to proceed. This leads to important connections remaining undetected, as the reported information cannot be linked with other information in the money laundering register, or with other police information. The chances of recovering criminal proceeds are also affected, as the money risks being forwarded before the missing details can be obtained.

Missing counterpart details also have negative consequences for law enforcement agencies, as the funds are hard to trace.

5.2 Facilitators among obliged entities

The need within organised crime to launder money on a large scale creates demand for facilitators among the obliged entities able to help the process. The fact that facilitators can abuse their position of trust to assist criminal networks represents a major vulnerability in the defence against money laundering. Because the obliged entities are there to protect the financial system, facilitators represent a risk of a threat to the system. Intelligence indicates that the phenomenon is widespread and that the problem with facilitators amongst, for example, bank employees, is significant and more extensive than previously thought. Chats from confiscated mobile phones are one source that shows that facilitators play a key role in laundering criminal proceeds, and that they operate within banks of all sizes. There are also obliged entities where not only individual employees, but also their officers knowingly facilitated money

²⁰ EU regulation 847/2015 came into effect on 26.06.2017 and was replaced by regulation 1113/2023 on 30.12.2024.

²¹ This concerns transactions that go through Bankgirot and data clearing, see FSA decisions ref. no. 24-11564, 24-11565 and 24-11566.

laundering. Examples of such facilitators are lawyers, who provide counsel, auditors who knowingly turn a blind eye and estate agents who contrive false property deals. 32 individuals have been identified by the police as registered auditors for nearly 3,000 companies.²²

In several instances, facilitators have made their trust accounts²³ available for money laundering transactions. Trust accounts can be used to conceal the source of money or who actually owns it, given that it is an obliged entity that owns the account. In the event of property purchases, for example, the purchase price can be diverted through the agent's trust account to mitigate the risk of banks involved querying or stopping the transaction. Lawyers also have trust accounts that can be used to give funds legitimacy, e.g. for the purpose of being able to invest criminal proceeds in companies or property.²⁴ Given the risk of facilitators, the lack of transparency in trust accounts is a problem. Without knowing who the money belongs to, there is a risk that the bank at which the account is held can be party to money laundering.

5.3 Money laundering using businesses as tools of crime

Large scale and systematic national and international money laundering through corporate structures and company accounts has been identified by authorities over several years.²⁵ Information from Europol indicates that among the criminal networks that comprise the biggest threat, 86% use legal corporate structures to launder their criminal proceeds.²⁶ Between 2020 and 2023, around 20% of the persons the Swedish Police Authority identified as network criminals in Sweden had some form of involvement in at least one company. In total, they had links to 23,000 companies, representing just under 2% of all Swedish companies. These companies often exhibit signs that make them particularly vulnerable to exploitations, such as short lifecycles, low or no declared turnover, high debt and frequent bankruptcies, which are all factors that complicate traceability and supervision.²⁷

Despite there being significant money laundering risks linked to companies, it is known that companies are the subject of money laundering reporting to the FIU to a relatively low extent. Only around 5% of all suspicious transactions reported to the FIU concern transactions between companies.²⁸

Based on the FIU's and Swedish Economic Crime Authority's full intelligence profile, it is known that most highly capable criminal networks use companies as platforms to some extent for their criminal schemes. The proceeds generated in the network often give rise to large scale money laundering.²⁹ Criminal proceeds can be merged with legal activities, which complicates detection and investigation of the crime. Corporate structures can shield individuals and make transactions possible to a large degree that can pass unnoticed through a control system, for example through a share of profits, group internal transfers or issuing false invoices. A company can also have accounts at several banks, which means the same company can be used to quickly pass large amounts between different accounts and financial institutions to complicate detection and investigation.³⁰

Authorities and private actors need strong powers to prevent a company being exploited by criminals. One challenge in this context has long been that public registers of companies do not always reflect the facts. Since the last sector-based risk analysis, the Swedish Companies Registration Office has been given a clearer law enforcement mandate and new means of checking details, and has begun a development process to improve register quality. Another challenge is that obliged entities do not share relevant information with each other. This means that when a bank detects non-conformity, the company can simply move its account to another bank.

22 In this context, auditors cover all accountancy and audit roles registered in the Swedish Companies Registration Office's various company registers, i.e. including lay auditors and elected auditors who are not subject to money laundering supervision. *The Swedish National Council for Crime Prevention, Företag som brottsverktyg – upplägg, systemsårbarheter och kopplingar till den kriminella miljön* (Brå 2025:20). (In Swedish).

23 Trust accounts are used to handle money on behalf of clients, separate from the firm's own funds.

24 *Finanspolisen informerar: Klientmedelskonton nyttjas för penningtvätt*, December 2023, Ref. no. A686.283/2023. (In Swedish).

25 See, for example, Swedish Police Authority (2024) *Professional money launderers – Sectors, approaches and links to criminal networks*. Ref. no. A154.174/2024. National Intelligence Centre (2024) *Historikbolag som brottsverktyg*. Ref. no. A274.795/2024 (in Swedish). *Finanspolisen informerar: Kriminella tvättar pengar genom företag*, May 2024. Ref. nr. A.258.551/2004. (In Swedish). *Finanspolisen informerar: Finansiella flöden och penningtvätt genom bolag i nätverksmiljöer*, September 2024. Ref. nr. A504.408/2024. (In Swedish). Ref. no. A504.408/2024. Europol (2024), *Decoding the EU's most threatening criminal networks*.

26 Europol (2024), *Decoding the EU's most threatening criminal networks*.

27 The Swedish National Council for Crime Prevention, *Företag som brottsverktyg – upplägg, systemsårbarheter och kopplingar till den kriminella miljön*. (Brå 2025:20). (In Swedish).

28 *Finanspolisen informerar: Kriminella nätverk tvättar pengar genom företag*, May 2024. Ref. no. A258.662/2024. (In Swedish).

29 *Finanspolisen informerar: Kriminella nätverk tvättar pengar genom företag*, May 2024. Ref. no. A258.662/2024. (In Swedish).

30 The Swedish National Council for Crime Prevention, *Företag som brottsverktyg – upplägg, systemsårbarheter och kopplingar till den kriminella miljön*. (Brå 2025:20). (In Swedish).

Risk awareness is deemed to have increased in obliged entities in recent years, but companies still need to strengthen their procedures and processes for knowing the customer and transaction monitoring regarding business customers. Transactions in different companies can look very different, even within the same industry, and can also vary over time for individual companies.

Obliged entities can, for example, subscribe to information on changes of officers from the Swedish Companies Registration Office to ensure that they have access to current details, but many fail to use this option. Know your customer procedures performed initially leading to an assessment of low risk may also be updated far too infrequently or not at all, according to the law enforcement authorities.

The consequence is that banks do not have the correct details of the company's officers can be that company involvement and its accounts are controlled by unauthorised persons. Intelligence confirms that details of authority, power of attorney and access to other people's safe deposit boxes giving authority to sign on behalf of the company are often contained in the banks' systems despite the company having changed its officers. Not all banks have integrated customer due diligence information in their monitoring of transactions, which makes it hard to identify non-conforming transaction behaviour. Such vulnerabilities combined with processing times for customer due diligence procedures mean that suspicious transactions in the company accounts can amount to many millions in value before the service is stopped or the customer terminated, whereupon money laundering continues in another company.

5.3.1 Established companies are particularly attractive

A report on established companies as crime instruments compiled within the National Intelligence Centre (NUC) by the Swedish Economic Crime Authority, Swedish Tax Agency and Swedish Police Authority shows that criminal actors have systemised the use of existing companies to conduct various forms of criminal activities. The companies are often used purely as consumable goods. The constant demand for new companies has created a market for shady company formation agents supplying criminal actors with a so-called established company. Established companies are defined as limited companies that have been sold by their former owners which are closed down, but still have approval for corporation tax, employer and VAT registration, bank account and credit rating. Using such established companies, criminal actors gain rapid access to companies that can be used for criminal purposes.³¹ On this background, established companies are a particularly attractive instrument for criminal activities, as they combine rapid access to financial infrastructure with superficial legitimacy that can be used to circumvent controls and lower the alertness of obliged entities.

5.3.2 Straw men and exploited identities

To enable criminal actors to distance themselves from the crimes they commit within the framework of their business often requires access to false or stolen identities. A market has grown for the sale of identity details, and there are examples of schemes under which individuals travel to Sweden from other EU states to register as a resident, open a bank account and obtain e-Identification. They then leave Sweden but leave their ID details and smartphone behind, which can then be exploited.³² Such identities can be used, for example, to register as a straw man on company boards, as account holder with banks or as an employee of a business for criminal transactions. The transactions must give the appearance of regarding wages or other forms of remuneration. Identities to use in this manner are in demand by the criminal actors, who regard them as goods for sale. In this way, criminal actors can fully control a business in someone else's name. The use of false and stolen identities reflects a decisive role in the use of a company as a crime instrument and avoids checks, supervision and investigation by the authorities. One way of preventing the use of straw men within

31 The Swedish National Council for Crime Prevention, *Företag som brottsverktyg – upplägg, systemsårbarheter och kopplingar till den kriminella miljön*. (Brå 2025:20). (In Swedish).

32 The Swedish National Council for Crime Prevention, *Företag som brottsverktyg – upplägg, systemsårbarheter och kopplingar till den kriminella miljön*. (Brå 2025:20). (In Swedish).

the financial system is that obliged entities demand a personal meeting more and more. The requirement that an individual can describe their business on their own can entail a higher threshold against the use of straw men.³³

5.3.3 Abuse of non-profit organisations

Criminal actors also exploit other forms of association for criminal purposes. Non-profit organisations offer a high degree of anonymity, may also have access to banking services and are registered for VAT and corporation tax. Companies that run the collection or administration of capital disbursed for other purposes are identified by FATF as risk-exposed, especially for terrorist financing. Such companies are normally run in Sweden by charitable societies or foundations.

With regard to foundations, there are details of officers available in the County Administrations Boards' registers of foundations, and changes have been made to the law for the purpose of crime prevention that adapt certain rules to the law pertaining to other company law.³⁴ Charitable associations do not need to register their officers and are only obliged to declare their beneficial owners in exceptional cases. The lack of transparency complicates the work of the authorities to detect associations exploited for criminal purposes and chances of obliged entities to know their customers properly.

5.4 Cross-border financial activities

Under EU law, financial companies licenced in other EU states can provide financial services in Sweden through a simple declaration to the FSA. Provision can be performed through the physical establishment of a subsidiary, but it is much more common for financial services under this type of cross-border activity to be provided with no form of physical presence in Sweden. In such instances, the Swedish authorities have very little supervisory responsibility, and cannot collect information from, or collaborate with, these obliged entities in the same way as for Swedish financial companies licenced in Sweden. Companies offering cross-border payment transactions are one of the types involved.

Given that these financial services are offered digitally, identification has to be performed remotely, which increases the risk of criminal actors being able to use false or stolen identities. Registration is often quick and easy and new customers can obtain access to the services directly, before their details can be checked. The ability and chances of these foreign obliged entities to, for example, check identities and personal details against Swedish registers can be limited, which makes it harder to achieve satisfactory customer due diligence. Furthermore, foreign obliged entities have less chance of assessing what is risky behaviour in a Swedish context compared to the market they normally operate on.

5.4.1 Risks of virtual bank accounts

The opportunity to use virtual international bank accounts also represents a vulnerability that can be exploited by criminals for money laundering. International Bank Account Number (IBAN) is a global standard for account numbers mainly used for international payments. The standard can also be used to create virtual account numbers (vIBAN). A large number of such virtual accounts can be linked to a single underlying bank account. The virtual account number can follow the standard for one country, but be linked to an actual bank account in another. That makes vIBAN an attractive instrument for criminals who want to make fast international payments without declaring the underlying account, account issuer or the actual recipient country.

This vulnerability is expected to diminish in line with implementation of the sixth money laundering directive, as the account and safe deposit box system will then have to include a virtual account with information on the issuing institution and who the account is issued to. Information on the underlying account will certainly then be searchable, but is still expected to not follow the transaction and can thus not be caught in automatic transaction monitoring.

33 The Swedish National Council for Crime Prevention, *Företag som brottsverktyg – upplägg, systemsårbarheter och kopplingar till den kriminella miljön*. (Brå 2025:20). (In Swedish).

34 Chapter 4, sections 17-20 and chapter 5, section 6 of the Foundation Act. The changes concern disqualification for proxies, a ban on straw men and the duty to report for auditors if they suspect financial crime.

5.5 Activities not covered by the AML regulations

Under the national risk assessment, the Coordination Function has identified activities deemed to be associated with the risk of money laundering or terrorist financing, but that are not covered by the AML regulations.

5.5.1 Accounts not supervised in the Mekanismen account and safe deposit box system

The Mekanismen account and safe deposit system does not include all obliged entities offering customers deposit facilities.³⁵ Mekanismen³⁶ is a technical platform that connects authorities quickly and efficiently to get information on the existence of accounts and safe deposit boxes at the institution, and to determine the identity of owners of such accounts and boxes. Companies covered are Swedish credit institutions and securities companies licenced to receive customer funds in accounts. Foreign credit institutions and securities companies with subsidiaries in Sweden are also covered by Mekanismen. Financial companies with no licence of their own to provide deposit accounts are an example of obliged entities not covered by the regulations. Customer holdings are concentrated on the financial company's trust account in a bank, and only the financial company is identified as the account holder in Mekanismen, not the company's customers. The same applies to gambling company accounts with banks.

5.5.2 Consultancy firms regarding company and property businesses

Transactions in the form of transfers of commercial properties and mergers, acquisition or purchase of companies between a value of SEK 100 to 200 billion take place in Sweden every year and often involve foreign investors. Complex ownership structures can be involved, something which creates the right conditions for circumventing sanctions or concealing that money comes from criminal activities. Companies providing consultancy in connection with this type of transaction therefore need to be aware of the risk of money laundering.

But not all such consultancy is covered by the AML regulations. The AML act explicitly only refers to consulting services provided by lawyers and impartial legal advisers. Auditors and estate agents providing such services are explicitly covered by the regulations as obliged entities as defined by the AML act. If a company is run within a law firm or registered accountancy firm, it will be covered by the AML regulations and be subject to supervision.

Consultancy in connection with property or company business can also be offered by other companies and professional categories not included in the AML regulations. Such consultancy is not subject to requirements on customer due diligence procedures or reporting. This is a problem, given that risk is associated with the activity as such and should not be conditional on the professional title of the consultant. It can be compared with tax consultancy which is covered by the regulations regardless of who offers the service.

5.5.3 Cryptoassets as a means of payment

Virtual currency offers a greater degree of anonymity than, for example, bank and card payments, and can in many respects be compared to cash. Cash purchases over a certain amount incur requirements for money laundering checks, but there is no corresponding regulation of virtual currencies as a means of payment for the purchase of goods, despite the risk of money laundering being deemed to be high. This applies despite the issuers of cryptoassets and suppliers of cryptoservices now being covered by the MiCA regulations³⁷ and AML regulations. In contrast to cash purchases, cryptoasset purchases can also be made remotely. The lack of regulation means that goods such as cars or boats can be sold for payment in a virtual currency without the vendor having to conduct anti-money laundering checks. This risk is mitigated through the EU's new AML regulations. According to the regulation, natural and legal persons trading in high value goods in a regulated or largely professional activity must report all transactions that involve the sale of certain high costs goods when acquired for non-commercial purposes. Reporting must be made to the FIU.

³⁵ Act on Accounts and Safety Deposit Box Systems (2020:272).

³⁶ The Swedish Tax Agency is the authority for the Mekanismen technical platform. Actors within Mekanismen are issuing authorities, institutions and the Swedish Tax Agency as the authority responsible for the system. The Swedish Tax Agency's role as system responsible is completely separated from its ordinary authority role.

³⁷ Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

An effective means of realising criminal proceeds is to buy prepaid cards for virtual currencies which can then be used as a means of payment. There is a wide range of such gift vouchers that can be sold without any customer due diligence procedures, as they are only valid within a limited network and therefore do not fulfil the criteria for electronic money. In practice, such gift vouchers are often just as usable as electronic money, as some of the networks are very large marketplaces offering a wide range of goods and services. There are also platforms where it is possible to buy cards for many different networks in once place. Because there is no limit to how many cards can be bought, or on the amount, the card can be used to launder large sums.

5.6 Factors that complicate supervision

To follow is a description of some circumstances that comprise a hindrance to effective supervision.

5.6.1 Risk of unclear supervisory responsibility

There are activities for which supervisory responsibility is shared between several authorities, something which makes it hard to run uniform and effective supervision. One example of when supervisory responsibility overlaps is financial companies which also offer accountancy services and thus come under the supervision of the FSA and the County Administration Boards. Another example is consultancy linked to the transfer of commercial properties or in connection with mergers, acquisitions and disposal of companies. Unclear supervisory responsibility implies a risk that supervision falls between two stools and that supervisory activities are not carried out despite the risks justifying it.

5.6.2 The importance of supervisory priorities

In Sweden, there are thousands of obliged entities spread across five supervisory authorities and one self-regulating body. The large number of obliged entities means heavy demands for the authorities to work risk-based and to direct their supervision to the areas of greatest risk. In this context, the opportunity to share information between authorities is a welcome result of the legislation. Collaboration with law enforcement authorities can improve the chances of directing supervision to ensure that resources are used most effectively. Another aspect of the limited resources is that it can be hard for an individual authority to have sufficient capacity for method development. There is also potential to collaborate here, as the supervisory authorities have similar requirements to identify risk factors for companies as crime instruments or facilitators, for example. Uniformity around control, objectives, priorities and financing of the supervisory sector can lead to greater collaboration and efficiency.

5.6.3 Limited access to criminal records

It is currently impossible to request details from criminal records within the framework of current anti-money laundering supervision. Extracts from criminal records would enhance the choices and priorities of the authorities and provide the basis to be able to use resources more efficiently.

On the other hand, the supervisory authorities have limited access to the records in connection with suitability testing and applications for authorisation. But one limitation is that several of the supervisory authorities only get extracts of a certain types of crimes, mainly financial. Information on, for example, serious drug-related crime would give the authorities a better chance of detecting links to criminal activities and to identify potential facilitators among obliged entities.

6 Risk-mitigation measures

A lot has been done in recent years to strengthen defences against money laundering and terrorist financing. Not least major changes with regard to secrecy-busting rules and the opportunity to collaborate to counter the problem. Meanwhile, the threat remains from organised crime and thus the need to regularly launder criminal proceeds on a large scale. It is therefore imperative to continue efforts to reduce vulnerabilities that make it possible for criminal actors to handle and launder criminal proceeds. To follow are proposals for a number of measures that the Coordination Function believes will help reduce vulnerabilities identified in working with this risk assessment.

6.1 Greater transparency regarding transactions and accounts

A clear vulnerability in Sweden's efforts to combat money laundering is that legislation on what information should accompany transactions is not complied with, due to breaches in the Swedish payment infrastructure. The fact that information on account numbers is missing in transfers between various obliged entities weakens the chances of banks detecting deviations in their transaction monitoring. This vulnerability is systematically exploited by criminal actors to conceal and launder money by using accounts in various banks. The FSA has ordered Bankgirot's Swedish owner banks to address the gaps by 31 December 2026, but until then, the vulnerability remains. Measures that could help boost transparency regarding transactions and account holders are proposed in this section.

6.1.1 Regulatory right to details in suspicious activity reports (SAR)

The fact that all relevant information does not accompany transactions gives, in turn, major consequences for the work of the FIU, as details of who has sent or received money is often missing from SARs. Counterpart details are also missing sometimes, despite both sender and receiver being customers of the reporter and the obliged entity thereby has access to the details. The Swedish Police Authority therefore needs to be able to stipulate which details must be included in an SAR. It is worth noting that not all types of obliged entities have access to information on who is the counterpart in a transaction. The regulations therefore need to be formulated to take into account the various circumstances of the obliged entities.

Proposal:

- Give the Swedish Police Authority the power to stipulate which details an obliged entity should provide when reporting according to the Anti-Money Laundering Act.

6.1.2 Increase the content of Mekanismen

The current regulations do not make it possible to see accounts in Mekanismen for customers of financial companies with no licence of their own to provide deposit accounts. Customer deposits are concentrated in the trust accounts of financial customers in a bank. The bank providing the account cannot see which persons or company the money in the account belongs to, which complicates the bank's risk assessment and customer due diligence checks. The lack of transparency also curtails the opportunities of law enforcement authorities to track transactions as well as identify and recover criminal proceeds.

The same problem exists for funds transferred to gambling accounts at gambling companies³⁸. Such accounts can be used to conceal and move criminal proceeds.

The pending sixth anti-money laundering directive expands the scope of account mechanisms for EU states. According to the directive, financial institutions as well as credit institutions will be covered, which means that significantly more financial companies will be forced to join the Swedish account and safe deposit box system. This probably implies that many of the financial companies that currently provide, for example, savings accounts that in reality are sub-accounts to a trust account that the financial company has in a bank will be obliged to join on behalf of another company in the future (e.g. securities management). On the other hand, it will not mean that the owner of the

³⁸ Government commission on measures to counter gambling accounts being used for criminal activities (Fi2023/03186).

"sub-account" will be covered by the system, it is only the owner of the actual bank or payment account who will continue to be accessible for searching. To increase transparency, the Mekanismen will have to include details of the owners of "sub-accounts".

Proposal:

- Investigate the possibility of extending the Act on the Account and Safe Deposit Box System (2020:272), so that obliged entities with a licence to receive funds with the obligation to report will be obliged to keep details of the owners of sub-accounts accessible for searching.

6.2 Instrument for accessing facilitators and illegal financial activities

In line with awareness of risks increasing and tighter checks in many obliged entities, the demand for facilitators who can help criminal actors circumvent the control systems is growing. Criminal actors have also been known to run what appears to be a legitimate financial business to be able to launder money on a large scale. In such cases, there is not just one individual on the inside, but the entire company that facilitates money laundering. Another consequence of tighter checks in respectable obliged entities can be that criminals will turn to underground banking to a greater degree, i.e. purely illegal financial activities that are completely out of the scope of checks and supervision.

Facilitators and the illegal activities work in concealment and are very difficult to detect for a single obliged entity or authority. The proposal in this section aims to provide better means for detecting and combating the problem.

6.2.1 Preventive legislation should cover money laundering crime

Access to intelligence is deemed to be key to be able to identify facilitators and illegal financial activities. The opportunity to use preventive and secret coercive measures to prevent very serious crime occurring within criminal networks was expanded in October 2023. Money laundering and commercial money laundering were not included, despite network criminality being motivated to a high degree by financial gain and violent crime often arises from conflicts provoked by profitable crime.

Proposal:

- Investigate the possibility of extending the Act on Measures to Prevent Certain Very Serious Crimes (2007:979) to cover large-scale money laundering and large-scale commercial money laundering.

6.2.2 The possibility of collaborating with several types of private actors

The possibility of collaboration between authorities and with private actors is a clear factor for progress when it comes to combating the problem of facilitators and underground banking. The secrecy-busting rules in pursuance of the AML act only permit collaboration with certain designated authorities and credit institutions. Law enforcement authorities see the need to be able to collaborate with multiple actors to combat money laundering, such as clearing companies, telecoms companies and e-identification companies.

The possibility of collaboration is wider, given that the EU's new AML regulations, but continues to be limited to certain authorities and to obliged entities covered by the AML regulations. The Collaboration Function believes that the threat from organised crime in Sweden creates the need to be able to collaborate with all authorities and private actors that could be relevant to combating the problem. Given that crime is adaptable and it is hard to predict every need, the opportunity ought not to only be limited to obliged entities and relevant authorities according to the regulation.

Proposal:

- Investigate the possibility of a national addendum to article 75 in the forthcoming EU regulation, that will allow law enforcement authorities to collaborate with all authorities and private actors according to need.

6.2.3 Cash declarations at the inner border and the option of sanctions

Intelligence indicates that the transportation of cash represents a common link in international money laundering. The purpose is often to introduce criminal proceeds into the legal economy, especially via countries where there are plenty of opportunities to place cash in the financial system.

Even if the export of Swedish kronor to launder cash via foreign banks is deemed to have been reduced, the risk remains that criminal actors will use cash in various currencies to move value between countries. Large amounts of cash generated from crime are extracted, handled and reinvested continuously in new criminal activities and can still involve transportation over borders. There is an existing requirement for reporting the import and export of cash over a certain amount at the outer border. To further reduce the risk, preparation is underway to apply the existing requirement at the inner border as well. On 1 April 2026, a new law comes into effect that introduces corresponding requirements for the inner border.

It should also be possible to apply effective, proportional and deterrent sanctions against breaches of the requirement for declaration of cash when crossing the border. The Coordination Function believes that fines, the scheme in use in Sweden at the moment, is inadequate to achieve the desired effect. Several other EU states apply much stiffer sanctions, including in the form of a percentage of the amount involved.

A criterion for the regulation to have the desired effect is also that background checks can be made when the declarations are submitted. An analysis of the declarations at the outer border made by the Swedish Police Authority for the government commission on the recovery of criminal proceeds shows that more than 20% of people submitting declarations appeared in police intelligence records with details on crimes including drugs, financial crime, terrorism and extremism. With no checks or follow-up, the declarations can give undesirable legitimacy to the money transferred over borders. It is therefore important to ensure resources for checking and intelligence collaboration between Swedish Customs and the Swedish Police Authority so that imports and exports can be stopped in the event of suspicion of criminal activity.

Proposal:

Make the import and export of cash connected to criminal activities harder by:

- apply tougher sanctions for infringements of the requirement to declare cash funds to Swedish Customs and
- overhaul the Customs Data Act to support intelligence-based checks.

6.3 Better ways of countering companies as criminal fronts

Organised crime systematically uses companies and other forms of associations to commit crimes. Companies provide the conditions to extract, handle and launder large volumes of criminal proceeds, and large scale money laundering always involves companies in principle. Companies as a front for crime are difficult to detect for authorities and private obliged entities, such as banks. Complex structures of companies in multiple lands can be involved, where money earned legally can be blended with criminal proceeds. The use of straw men and stolen identities reduces transparency and makes detection harder. To follow are proposals for measures to support detection and combating companies used as fronts for crime.

6.3.1 Central register of shareholders

Poor transparency regarding shareholders in unlisted companies mean criminals can conceal ownership of property and other assets, and make it harder to identify companies used as fronts for crime. To identify changes of ownership in companies, the authorities and obliged entities need more details in the Swedish Companies Registration Office of changes to the board of directors and intelligence from other sources. Access to information on shareholders in unlisted companies should make the process significantly more efficient and increase the chances of detecting and stopping companies being used for criminal activities.

Proposal:

- Investigate the possibility of setting up a central register of shareholders in unlisted Swedish companies.

6.3.2 National ID centre responsible for combating money laundering

In response to a government mandate to improve collaboration to maintain and spread competence on identity issues, the Swedish Tax Agency, Swedish Police Authority, Swedish Migration Agency and the National Government Service Centre have proposed setting up a national ID centre to support other national authorities within the field of identity. Proposed activities for the centre will include structuring and sharing analyses and intelligence as the basis for operative functions within national authorities.

The Coordination Function welcomes the proposal and emphasises the importance of such a centre making an active contribution to combating money laundering, as false and stolen identities are systematically used.

Proposal:

- Mandate the proposed national ID centre to actively take part in efforts to combat money laundering.

6.3.3 Greater transparency regarding non-profit organisations

Non-profit organisations are not subject to the same requirements regarding accounting and auditing, or transparency concerning their representatives, as other forms of association. Non-profit organisations are believed to comprise a front for criminal actors who want to use money from criminal activities. Charitable associations do not, for example, need to register their officers, but can still use banking services, register for VAT and corporation tax and receive donations.

The lack of transparency makes it hard to achieve satisfactory customer due diligence insight and can mean that banks sever their relationships with such organisations or cannot provide such organisations with services to transfer funds to recipients in high risk countries. The Coordination Function believes that greater transparency regarding non-profit organisations should reduce the risk of such organisations being exploited for criminal purposes and supporting the activities of shady actors.

Proposal:

Consider increasing transparency regarding non-profit organisations by:

- setting up a register of officers for charitable societies and give them a company registration number.
- introduce mandatory checks for donations.

6.4 More efficient money laundering supervision

6.4.1 Supervision of the anti-money laundering laws regarding consultancy firms

The anti-money laundering laws do not cover all companies providing consultancy linked to the transfer of commercial properties or in connection with mergers, acquisitions and disposal of companies. The AML act explicitly only refers to consulting services provided by lawyers and impartial legal advisers. Other professional categories offering such services, e.g. auditors and estate agents, are implicitly in their role as obliged entities. But such services can be provided by non-obliged entities as defined by the AML act.

When a consultancy firm is run within a law firm or registered accountancy firm, that company will be covered as such by the regulations and be subject to supervision regardless of the title of the consultants. Companies offering such consultancy but which are not a law or audit firm are therefore not covered by the provisions of the AML act. Neither are there requirements for such companies to be registered in the Swedish Companies Register for money laundering, nor with any supervisory authority, as the company is not subject to supervision. The risk of money laundering through corporate and property trading should be the same, regardless of the professional titles of consultants. There is therefore good reason to consider whether the law should be tightened to cover consultancy services, regardless of who provides them corresponding to the general regulations which apply to tax advice.

Proposal:

- Consider a national addendum to the AML regulations so that the services referred to in chapter 1, section 4 of the AML act are covered, regardless of who provides them.

6.4.2 Access to criminal records for money laundering supervision

The supervisory authorities have access to criminal records in some instances, including in connection with suitability testing and applications for authorisation. On the other hand, they cannot request details within the framework of conducting supervision. Being able to should make the supervisory work of the authorities more efficient and support selection and prioritisation.

Furthermore, one limitation of the current regulations is that several of the supervisory authorities only get access for certain types of crimes, mainly financial. Given how intertwined various forms of criminality are, and bearing in mind the problem of facilitators, widening the range to cover more crimes, such as drug crimes, is necessary.

Proposal:

- Extend the existing legislation by giving all supervisory authorities the power to request information from criminal records within the framework of supervision concerning money laundering and terrorist financing, and by extending such information to include more types of crime.

7 Sector catalogue

The following chapter presents a catalogue of the sectors that come under the auspices of the AML act. A description is given for each sector of the activities and industry entities in the sector, along with certain key figures. The catalogue includes a risk assessment based on threat and vulnerability analysis of each sector. Money laundering risks are assessed quantitatively on a four-tiered scale, while the risk of terrorist financing is only presented in qualitative terms.

The sectors are presented in the order of the areas of application stated in the AML act.

7.1 Banking and financial institutions

Overall sector risk:



Banks and credit market companies are obliged entities whose core operations are deposits and lending. Such companies also provide financial services, such as payments and transfers, securities transactions and card issuing.

General description of the sector and related products or activities

Banks facilitate payments via a payment system and receive money in accounts. Banks and credit market companies both receive refundable funds from the general public, provide credit, apply credit guarantees and the acquisition of liabilities for financing purposes or facilitate leasing.

The sector is large and diversified. It includes, for example, the major Swedish banks who offer a comprehensive range of products, medium-sized banks, small banks occupying niches within specific products, membership banks and locally-based savings banks. There are also foreign companies offering products to customers in Sweden through subsidiaries. Banking or credit market companies require a licence to operate from the FSA – with a few exceptions. The terms and conditions are set out in the Banking and Financing Business Act (2004:297) and the Banking and Financing Business Ordinance (2004:329). Savings banks are also governed by the Savings Banks Act (1987:619).

The diversification of the sector implies that the risk of money laundering and terrorist financing can differ widely, but because the national risk assessment is based on sectors, an overall risk assessment of the sector is made here.

Key figures	
Number of companies	158
Number of employees	62 709
Number of business connections established	52 690 807
Company balance sheet total	17 805 441 315 846
Company turnover	488 136 396 959
Total number of physical customers	52 339 955
Total number of legal customers	2 064 002

Source: The FSA's periodic reports on money laundering, reference date 31.12.2024. The details are based on the reports of the institutions to the FSA and the table can, therefore, include data which deviates to some extent from the actual situation.

Money laundering – description of the risk scenario including known approaches

Because most account transactions pass through the banking system, the sector is subject to an almost unlimited number of approaches for money laundering. Banks can comprise a platform for simple and complex arrangements, on which everything from Swish transactions and cash withdrawals to integration of large scale crime proceeds via investment products can be part of money laundering. To follow are examples of such approaches.

Company accounts used to a greater degree

When it comes to large scale money laundering, the use of company bank accounts has increased. Most high capacity criminal networks use companies for their criminal methods. Companies within different industries can be exploited in parallel to meet demand within money laundering, for example, the handling of large cash flows or frequent transactions between different company accounts. The flow in

company accounts can be harder to detect than transactions in private accounts.³⁹ To conceal money laundering, complex transaction chains and many intermediaries can be used, which leads to poor transparency.

Proceeds from crime are laundered through front companies and their bank accounts

Criminal proceeds from labour market criminality, such as tax fraud, can be laundered by so-called front companies⁴⁰ and their bank accounts. Front companies are consumer item and can be startups, takeovers or acquisitions, the purpose of which is to be used for money laundering. They will often have no activities of their own, nor annual reports. Companies that have been taken over or acquired often have an established bank history, which increases their legitimacy for invoicing or transactions.⁴¹ Front companies are used in various types of industries, such as construction and catering, wholesale and auto dealers and within cleaning.

Front companies intentionally used as fronts for crime by successively maximising the proportion of black money in their economy before they are wound up when discovered. They are usually used for short periods before their bank accounts are closed or they go into bankruptcy. Due to their expected short lifetime, criminal networks have access to a large number of active and dormant front companies. Criminal activities can thus be conducted even if one or more front companies is closed down or goes bankrupt.⁴²

"Service intensive" companies, such as construction companies, are known to buy money laundering services from criminal networks to remunerate black labour. Companies that buy such services make payment to a front company via the financial system, often based on a false invoice. The money is passed through a series of front companies; some of it is often transferred abroad and some is transferred to the service intensive company to pay black wages with. The arrangement supports large scale money laundering through complex transaction chains, with the actual beneficial owner hidden behind stolen identities or straw men (see below).

Suppliers of factoring services facilitate money laundering

For approaches involving false invoices, factoring services are important to the money laundering arrangement. Factoring is a financial service in which a company sells to or borrows against its invoices via a factoring company. Factoring services can be used for fraud and money laundering by the factoring company buying invoices which do not have an actual underlying claim. A criterion for factoring services to be used in this way is that the factoring company does not make a thorough investigation of the company and the individuals behind it before buying the invoices. When a criminal network systematically exploits a company which has a good credit rating and history requires more than an automated and superficial check to detect criminal activities. Criminal actors can also offer factoring services themselves, knowingly making money laundering possible. Payments are distributed to several different recipients without any form of customer due diligence procedures being conducted. Such suppliers of factoring services also adapt their activities to avoid inspections and investigation by the FSA.⁴³

Cash withdrawals from ATMs

Withdrawing cash from a bank account via an ATM is a common means of money laundering. It is used, for example, to launder criminal proceeds or other crimes when the proceeds are layered to degrade traceability. Cash withdrawals are often made by straw men or persons with access to a withdrawal card and code. Criminal proceeds can also be paid into an account via ATMs as part of money laundering.

39 *Finanspolisen informerar: Kriminella nätverk tvättar pengar genom företag*, May 2024. Ref. no. A258.662/2024. (In Swedish)

40 Front companies are also referred to as invoicing companies. Front companies can be used in different ways, such as money passing through their accounts, as an administrative function to issue invoices or certificates, or as agencies for temporary employment.

41 Swedish Police Authority (2024), *Systematisk penningtvätt inom den rysktalande organiserade brottsligheten*. Ref. no. A629.012/2024. (In Swedish).

42 Swedish Police Authority (2024), *Systematisk penningtvätt inom den rysktalande organiserade brottsligheten*. Ref. no. A629.012/2024. (In Swedish).

43 *Finanspolisen informerar: Kriminella nätverk tvättar pengar genom företag*, May 2024. Ref. no. A258.662/2024. (In Swedish).

Account straw men provide their bank accounts to others

Account straw men provide access to their bank accounts for others to launder money. Account straw men send criminal proceeds between bank accounts through, for example, account transfers, Swish or foreign payments. Young people are often used as account straw men. Account straw men may receive payment for their participation in money laundering, or are forced to do so by other criminals.

Exploiting the eID of others

Criminal actor activities can be concealed behind stolen identities by using the eID of other people. Experience from criminal investigations show that the exploitation of identities and abuse of eID is high. Threat actors use eID and safety deposit boxes belonging to other people, e.g. people who have emigrated or using stolen identities. In this way, safety deposit boxes can be open in their names, but are controlled by the threat actor. Accounts can also be opened in several different banks in parallel to be used for money laundering.

False personal details

Experience from crime investigations show that false personal details are widely used in criminal circles, including to apply for credit. Personal details are something given by employers to the Swedish Tax Agency for everyone receiving pay, benefits or other forms of remuneration and false details mean that their owner does not do the work for which payment is made. Using false personal details, criminal actors can improve their credit rating, making it easier to get loans from banks, which can then be repaid using the proceeds from crime. Access to credit can also be condition for running a business which is also used for money laundering, e.g. auto dealers. Being able to detect anomalies early in a credit granting process is decisive to prevent credit fraud with money laundering as a consequence.

Digital payment services and instant payments

Banks offering fast digital transfers of money can be especially vulnerable to exploitation for money laundering. By improving their preventive measures combined with the fall in the use of cash in Sweden, banks have made it harder for criminals to use cash. They use cards and Swish to a greater extent than previously instead. Instant payments such as Swish make it possible to transfer money to a recipient's account in seconds. Of the total number of transactions reported as suspicious to the FIU in 2024, 50% were made via Swish.

Constant technological innovation in the finance sector means that new digital payment services and instant payments are developed, which is reflected in the money laundering that can be observed nationally and internationally. Digital payment services and instant payments are common within various types of money laundering structures, along with payment in illegal goods. In a diversification process, Swish transactions are deemed to be a very effective tool. Transaction details show that the proceeds from, for example, fraud, are spread between various accounts via Swish immediately after the fraud has been committed. Sometimes the total is divided up further and passed on to various recipients, for example, to facilitate withdrawals via ATMs. The money is also moved abroad via other payment platforms or the purchase of cryptocurrencies, for example.

Private banking

Private banking is a form of wealth management advice provided to wealthy private customers at around 40 banks in Sweden.⁴⁴ Such advice can involve financial planning, capital management, law, tax advice and foreign investment. According to the FATF, a private banking account can be attractive to money launderers, especially for laundering the proceeds of corruption. This is because private banking customers usually have a lot of capital and use services which have international range.⁴⁵

⁴⁴ Details from the periodic money laundering report 31.12.2024.

⁴⁵ FATF *Specific Risk Factors in the Laundering of Proceeds of Corruption* (2012).

Leasing

Black money can be integrated and layered through leasing. A threat actor can enter into a leasing agreement for a product that does not exist. Payments are then made by the threat actor or an accomplice and represents a transfer of capital without anything in return. Products, such as vehicles, are also sometimes refinanced through repeated leasing. When the product is partially paid, it is refinanced through a new leasing agreement from another leasing company or bank, using the product as collateral (the residual value). The various leasing companies or banks are not usually aware of each other. The product is then sold, if not already sold, abroad. Other persons than the lessor can also make payments.⁴⁶

Facilitators and professional money launderers

In line with the efforts of banks to counter money laundering becoming more effective, the needs of criminals grows for facilitators employed by banks able to mitigate the risk of transactions being caught by checks and eliminating the tracks of crime proceeds. Facilitators can also use false income figures to help criminal actors to compile credible applications for various types of credit. Intelligence shows that there are facilitators employed in banks of all sizes.

Money laundering can be conducted by taking a loan from one or more institutions and paying it off with criminal proceeds using a PML. PMLs can either be the facilitator employed by the bank, or someone who has created a channel to a facilitator at the bank and who facilitates loans for commission to persons who do not actually meet all the criteria. To follow are two examples of how such an arrangement could look.

An auto dealer has sold cars financed by loans provided by the bank based on false information. A front man is used as the borrower and the loan is repaid by other persons. The same car may have been sold (and pledged) several times within a short period of time. The credit manager at the bank can be part of the money laundering structure and be a PML.

A front man has helped criminal actors who needed a mortgage by arranging contact to a bank employee. The bank employee knowingly approved the mortgage based on false information. Multiple facilitators have been involved in such frauds, for example brokers and bank employees.

There are also criminal actors who have sold a criminal scheme that involves facilitators as a service to other criminals. Apart from criminal actors planning and executing loan fraud for their own benefit using facilitators at a bank, they also sell the fraud scheme as a service to other criminals. The service is widely marketed and can almost be described as "illegal loan brokerage", in which the loan broker has a contact network of front men willing to borrow in their name, or when a PML who arranges the loan has contact to one or more bank employees who approve the loan on false grounds. In some instances, the broker and the bank employee take a fee for their work. A fee of 20% of the loan is common.

Bank employees have also been known to participate in various types of activities linked to a company scheme. Such a scheme is mainly intended to approve false payslips, knowingly overpay companies or to value credit unreasonably.⁴⁷

The interface between criminal networks and banking sector employees can be illustrated using this example:

A criminal network with high potential of violence and major influence on the local community runs a multi-million money laundering racket. Individuals in the network are also suspected of money laundering. Property is over-valued to increase the amount of a potential loan. The network uses a series of different PLMs, including brokers, bank employees and building permit administrators, of which several have direct family links to the network.

⁴⁶ Finanspolisen informerar: Kriminella nätverk tvättar pengar genom företag, May 2024. Ref. no. A258.662/2024. (In Swedish).

⁴⁷ Swedish Police Authority (2024) Professional money launderers – Sectors, approaches and links to criminal networks. Ref. no. A154.174/2024.

Threats – money laundering

Scope

45,477 SARs were received by the FIU in 2024 from banking and financing institutions⁴⁸, which is more than double compared to 2020, when 18,342 reports were received. The sector accounted for just under 7 out of 10 reports received by the FIU in 2024.

Companies within the banking sector play a key role in society and provide a wide range of products and services to private individuals and companies. The wide range implies a risk of the sector being exploited for money laundering. Criminal actors can make transactions through several products in the sector, as easy and quick accessibility risk confusing identifying the money's source.

Threat actor capabilities

As a digital banking and payment market contributing to flexible and quick payment solutions, it has also allowed criminals to commit embezzlement and to quickly launder and hide their proceeds. It is easy to open a bank account and to avail oneself of the bank's products and services, including Swish. The fact that technological progress is constant is being used by actors in criminal circles. Unusual transaction patterns related to Swish is the main cause of banks reporting private individuals to the FIU. Every other reported transaction in the money laundering register was a Swish transaction in 2024.

Complicated money laundering schemes require better skills of the threat actor. The presence of PMLs in the banking sector and their direct links to organised crime and criminal networks shows a high degree of ability amongst threat actors. The demand for facilitators among bank employees is expected to remain even after bank money laundering checks have been tightened, which increases the need for expertise to circumvent the system.

Reports received over the last few years from law enforcement authorities clearly point to the ability of threat actors to exploit vulnerabilities, especially within the use of company accounts at banks for large scale money laundering.

Anonymity

The Swedish financial markets have come far in their digitalisation process, and use various forms of eID to a large degree to identify customers. Digitalisation means that bank customers can handle their online banking more easily, but also mean new risks that the banks must understand and adapt their processes and procedures to.

Legal persons are often used for money laundering in the banking sector. The use of straw men, front men or falsified documents allow anonymity for natural and legal persons committing crime, something which increases the risk of money laundering.

The large and medium-sized banks establish their customer relationships remotely to a large degree, which can allow threat actors to remain anonymous through the use of a stolen identity or front man. The larger banks have introduced the option of being able to call in their customers to a physical meeting at a bank office to verify their identity and conduct customer due diligence procedures.

Banks that provide their services exclusively online and onboard customers remotely, known as neobanks, can be relatively easy for a threat actor to exploit from an anonymity perspective, as individuals whose identities are used as straw men may knowingly hand over their electronic identification credentials for the threat actor to use.

The customers of some banks are found to a greater degree in the local community. Some other banks have physical premises, something which can help them check the identity of customers if deemed necessary. Meanwhile, smaller banks have fewer resources for AML procedures, and there are a number of examples of how they have been used to launder money.

The large banks have invested more resources in improving their defences against money laundering in recent years. There is therefore a risk that threat actors refused by the large banks move their accounts to smaller or niche banks, such as neobanks with a banking licence.

⁴⁸ Concerns banking and financial institutions including credit market companies.

The use of trust accounts can imply better chances of anonymity. Such accounts can be used to conceal and integrate crime proceeds in the financial system, for example, through investment in property or securities, which is shown in reports from the FATF and FIU.⁴⁹

Correspondent links are a key component in the global payment system and provide private individuals and companies with international payment services. But they can also represent a better chance of anonymity, as the financial companies provide services via correspondent links to actors they do not have a direct business connection with. The institution needs to rely on the counterpart have an effective and appropriate procedures and checks to prevent money laundering.

As mentioned before, companies and other legal constructions are deemed to be attractive to money laundering. Complex ownership and control structures can give threat actors more anonymity, as it can be hard for banks to get to understand them properly.⁵⁰

Summarising assessment

Companies within the banking sector play a key role in society and provide a wide range of products and services to private individuals and companies. The wide range implies a risk of the sector being exploited for money laundering. Suspicious activity reporting to the FIU in 2024 from the banking and financing sector more than doubled compared to 2022, but a hidden proportion is still deemed to exist. Intelligence indicates that threat actors have the ability to exploit vulnerabilities in banks to process criminal proceeds, in particular through company accounts. The companies used for large scale money laundering often resemble a legitimate business, dependent on a bank account and bank services such as credit provision. There is also demand for facilitators among bank employees able to ensure access to services and to help criminal actors to circumvent bank control systems. The sector is multifaceted and the risk profile varies between institutions to a large extent, based on size, number of customers, products and services offered, geographic exposure in the form of international transactions and distribution channels.

In conclusion, the threat regarding money laundering in the sector is deemed to be high.

Vulnerability – money laundering

The chances of detecting money laundering

The sector generally has good resources to counter being exploited for money laundering, but there is still potential to continue improving them, given the changeable nature of crime. Efforts to combat money laundering at banks are usually based on three lines of defence. The first line contains persons engaged in running the business. Their responsibility is to identify, monitor and handle the operative risks of the business, including those linked to money laundering. Defences within the second line consist of functions for risk management and regulatory compliance. These functions monitor, evaluate and support the risk management regulatory compliance of the first line in some instances. The third line of defence consists of audit functions (internal or external) that evaluate the risk management regulatory compliance of the first and second lines of defence.

Banks and credit market companies have criteria for how they identify, rate, monitor and report the level of especially important risks. They have also established procedures and processes, and generally have a well-constructed monitoring system for customer transactions. However, various IT systems within the same company are not always compatible, such as the customer due diligence and transaction monitoring systems, which complicates the possibility of an efficient and functional control system to deal with money laundering risks. The banks generally find it harder to detect non-compliant or suspicious transactions in business accounts than in private accounts, which is exploited by threat actors. One reason for the problem may be that the transaction amounts are generally much higher than for private accounts, and that commercial transactions can be much more complex and differentiated, which makes it more a challenge to detect non-compliant behaviour. The high transaction volumes,

⁴⁹ *Finanspolisen informerar: Klientmedelskonton nyttjas för penningtvätt*, December 2023, Ref. no. A686.283/2023. (In Swedish).

⁵⁰ The Swedish Financial Supervisory Authority (2025), *Prioriterade risker inom penningtvätt och finansiering av terrorism*. Ref. no. 25-2399. (In Swedish).

wide range of products and services, number of customers and ability to make cross-border transactions are all inherent risk factors that increase the risk of money laundering, and complicate detection of money laundering transactions.

The large Swedish banks have considerable financial and human resources to combat money laundering. Their AML functions are usually extensive and monitor transactions through advanced systems. Given the level of resources and access to systems, the chances of detecting money laundering should be good.

In line with the major banks improving their level of prevention, there are indications that criminal actors are turning to small and medium-sized banks with fewer resources to combat money laundering. The smaller banks also often offer a range of services that is similar to the larger banks, and that entails the same risks. There is, therefore, a risk that some of the risks that previously centered around the major banks has now passed to the smaller ones.⁵¹ The risk profile of the larger banks is still deemed to be high.

Another vulnerability is that banks, due to current legislation, cannot share information between themselves on who they have ended a customer relationship with. This means that a customer whose account has been closed due to irregularities can go to a new bank without that bank knowing that the previous bank will have nothing more to do with that customer. But the opportunity to collaborate according to chapter 4a of the AML act, which came into effect on 1 January 2023, has meant that several collaboration projects have been created between credit institutions and the FIU, which has increased the chances of detecting money laundering.

In line with the efforts of banks to counter money laundering becoming more extensive, the need for facilitators employed by banks able to mitigate the risk of transactions being caught by checks and eliminating the tracks of crime proceeds grows. As mentioned above, intelligence shows that there are facilitators employed in banks of all sizes. This is a vulnerability that reduces the chances of detecting money laundering.

Compliance

Awareness and knowledge of the AML regulations is generally good within the sector. The organisational criteria are deemed to be good, and the larger institutions have allocated more resources to their control functions. More extensive measures within customer due diligence are therefore being implemented.

The FSA has found from its supervisory activities that the banks by and large have systems, procedures and documentation in place, but there are several breaches in analysis, assessment, follow-up and measures implemented in several instances. The FIU also believes that the efforts of the banks to combat money laundering and terrorist financing have improved in recent years, after glaring failures revealed by investigation into the activities of Swedish banks in the Baltics in 2020. But the banks need to go further to ensure that their internal rules and processes match their requirements and have the intended effect. In its investigations, the FIU identified breaches in the general risk assessments of all the banks. As a rule, such risk assessments have been inadequately adapted to the business according to the FIU's assessment.

Most of the FIU's investigations have also shown that the banks do not always adopt sufficient measures to know their customers. In several instances, such details as purpose and type, risk classification of customers and details of the beneficial owner were missing. Room for improvement is therefore still deemed to exist in the preventive efforts of the banks. For example, law enforcement agencies find that banks fail to react to their own monitoring procedures, despite major changes to company boards, something which should affect customer due diligence. Neither do banks always cancel authority to access an account, despite changes in company officers.

The banking sector is also deemed to have improvement potential with regard to detecting and reacting to changed transaction patterns that could be due to money laundering. Large increases in transaction amounts have often been detected too late, including in connection with vishing fraud⁵² and international VAT fraud, known as Missing Trader INtra-Community (MITC).

In line with the major banks improving their ability to combat money laundering, threat actors have been forced to find new ways of laundering money. Part of the risk is deemed to have migrated to the medium-sized banks. Experience gained from supervision indicates that medium-sized and niche banks generally have lower regulatory maturity compared with the bigger banks, which affects their ability

51 The Swedish Financial Supervisory Authority (2025), *Prioriterade risker inom penningtvätt och finansiering av terrorism*. Ref. no. 25-2399. (In Swedish).

52 Telephone fraud.

to detect money laundering. This can be exploited by criminal actors. Medium-sized banks are generally deemed to have certain breaches in regulatory compliance, and often fail to adequately assess how their products can be exploited for money laundering. Experience from supervisions of medium-sized banks shows that details on purpose and type of business accounts are not always obtained, that tighter customer due diligence procedures are not always known and that the beneficial owner is not always investigated sufficiently.

Supervision by the FSA of the subsidiaries of foreign institutions has found that their activities have not been adequately adapted to the Swedish market in several instances. For example, the subsidiary's general risk assessment has either wholly or partially been conducted based on the foreign parent company's general group risk assessment. That means no general risk assessment for the Swedish subsidiary.

Niche banks are generally deemed to work on improving their ability to defend against money laundering and to comply with regulations, including through new IT systems and improved customer due diligence procedures. The Authority's supervision also indicates that niche banks do have breaches in parts of their regulatory compliance, such as inadequately dealing with risks associated with their customers and not adequately adopting tighter customer due diligence procedures. Experience from supervision also shows a problem linked to resource levels with regard to dealing with alarms generated by transaction monitoring.

Missing counterpart details

Counterpart details play a key role in being able to assess whether a transaction or behaviour is suspicious. Missing counterpart details therefore implies a risk of transactions and behaviour which should otherwise have a reasonable explanation can be regarded as suspicious. That implies a risk of transactions where counterpart details should have raised suspicion are not noticed by obliged entities. Missing counterpart details also make sanction compliance difficult.

When reporting suspicious transactions and behaviour to the FIU, details of the counterpart are often missing. This also occurs in situations when the reporting obliged entity is obliged to have such information, including when all the parties involved are customers of the reporting obliged entity. Such failures have serious consequences for how the FIU proceeds: they complicate identification of transactions arising from one and the same counterpart, and make it harder to select reports for deeper analysis.

Summarising assessment

The sector is large and diversified. Resources, organisational factors, risk awareness and degree of maturity can differ within the sector. The sector in general can be said to have made progress in its efforts to combat money laundering in recent years. But despite the relatively good resources allocated by the banks for risk management, the control systems are not deemed to be adequately effective in relation to the threat.

Against a background of increased threat from organised crime, vulnerability is still deemed to be significant in a national perspective. Efforts to combat money laundering and terrorist financing must be consistent and continuous. To have any effect, the entire chain of measures must be linked and constantly updated in response to a change in conditions. This is also a criterion for an effective monitoring system.

Resources, organisational criteria, risk awareness and degree of maturity can differ within the sector, but the control systems are generally deemed to be inadequate to meet the threat from criminal actors dependent on banking services for laundering their criminal proceeds. A clear vulnerability in the ability of banks to combat money laundering is the fact that statutory counterpart details do not automatically accompany transactions between different banks, due to gaps in the Swedish payment infrastructure. The lack of this information makes it harder for the banks to identify transactions that can be part of money laundering. The extensive occurrence of facilitators employed in banks of all sizes is another obvious vulnerability.

In conclusion, vulnerability to money laundering is deemed to be significant.

Risk scenario, including known approaches of terrorist financing

Collections in a bank account occur to varying extent for the purpose of terrorist financing. The bank accounts in question can belong private individuals, companies, funds or associations. Collections can be made through payment brokers, cash deposits and bank transfers. The money then leaves the banking sector in various ways, sometimes gradually during the collection, or when the collection is complete. Transfers can be made via card transactions or transfers to payment institutions or payment brokers. Cash withdrawals are also an option, in Sweden or abroad, frequently in or near conflict zones.

The objective is often for the money to reach terror organisations or individuals connect to foreign terror organisations. Foreign transactions can also be used for terrorist financing. Funds acquired legally and illegally are used to finance terrorism. With regard to legally acquired funds, for example wages and donations, individual transactions and small amounts are usually involved.

Transactions linked to funding terror-related activities also occur in the banking sector. An example of such activities is people buying travel or arranging transport and accommodation for others. Signs that transactions can be linked to terror-related activities include

- an unfeasible number of travel-related purchases
- unusually high number of purchases at various filling stations and payments for car parking
- an unfeasible number of hotel bookings.

Companies can be used a crime fronts to finance terrorism, including through false invoices (see also under 7.19, Accounting/audit services).

Credit can be gained on false grounds and without the prospect of repayment with the objective of financing terrorism (see also under 7.10 Activities with consumer credit).

Threat – terrorist financing

Scope

The same criteria as for money laundering play a decisive role for the extent of terrorist financing in the banking sector. The sector is easily accessible for the purpose of terrorist financing.

Threat actor capabilities

No special ability or knowledge is needed to run a simple form of collection, to make cash withdrawals or to execute individual transactions for the purpose of terrorist financing. But running a collection systematically and extensively does probably require better awareness of the procedures and choice of banking services.

When it comes to opening a bank account and using the bank's products and services, the principles are the same as for money laundering. Knowledge of the customer due diligence procedures and transaction monitoring systems used by the banks can make it easier to avoid being detected or reported to the FIU, and can make it easier to avoid banking services being withdrawn.

Anonymity

As described in the section on money laundering, neither a natural or legal person is anonymous, but it is possible to use a straw man, for example. But this is deemed to be significantly more unusual in the context of terrorist financing compared with money laundering. For more systematic and extensive terrorist financing, funds and charitable societies can be used, probably due to the lack of insight into their structure and activities for banks and the authorities.

Vulnerability – terrorist financing

The chances of detecting terrorist financing

The section on money laundering reports on risk management and control systems used by the banks. The vulnerabilities described there also apply to terrorist financing. Regarding terrorist financing, the use of the banking sector as just one sector out of several in a long transaction chain is also a complicating factor, and that the transaction chain includes various obliged entities within the sector. When combined with the fact that the ultimate destination of the money is decisive – and not its sources or approaches used – this makes it hard for the banking sector to detect suspicious transactions. Furthermore, the amount in question is generally significantly lower within a terrorist financing context compared with money laundering. This is a state of affairs that makes it hard to identify transactions linked to terrorist financing.

Compliance

When it comes to compliance, the assessment is the same as for money laundering. Although the FSA has found in several instances after supervision that obliged entities within the sector did not perform a deeper analysis regarding terrorist financing in their general risk assessment. Geographical risk factors have not been taken into consideration to a sufficiently large extent and product risk assessments have not been assessed separately between money laundering and terrorist financing. Furthermore, obliged entities have failed to conduct sufficient analyses at aggregated level of the SARs on terrorist financing sent to the FIU.

7.2 Life insurance business

Overall sector risk:



The life insurance business involves activities run by insurance firms offering savings insurance and risk insurance.

General description of the sector and related products or activities

Savings insurance can comprise either traditional life insurance, unit-linked or deposit-linked insurance.

Traditional life insurance is a form of savings in which the insurance company manages the policyholder's money. The policyholder is guaranteed a certain amount upon maturity. This means that no less than the guaranteed amount can be disbursed, regardless of stock exchange performance, but the amount can be higher depending on the return on investment. The insurance company invests the capital in a mix of assets such as shares, property and interest-bearing securities.

Unit-linked fund insurance is a type of saving in which the policyholder chooses himself which funds the money will be invested in. The funds can be changed at any time. A deposit-linked insurance is a also type of saving in which the policyholder chooses himself which assets the money will be invested in. Compared to unit-linked insurance, the assets can also be, for example, shares and other securities. Which assets the policyholder invests in is stated in the insurance company's investment guidelines and the insurance contract. Compared to traditional life insurance, the policyholder is not offered any form of guarantee. The policyholder bears the investment risk instead.

Savings insurance can also be divided into pension insurance and endowment insurance. Pension insurance can be in the form of a public sector or private pension scheme. Public sector pensions can either be collectively agreed or individually. The employer is the policyholder for public sector pensions, whilst the employee is the insured. For collectively agreed public sector pensions, the employer makes pension contributions compared to private pension insurance where it is the policyholder who makes the contributions to their own pension insurance. There are limits to pension insurance for what age pension disbursement can start and for how many years they can run. Capital insurance is a form of savings that combines insurance and investment, and has fewer limitations than pension insurance. But there are limits to endowment insurance concerning when repurchase can take place, for example after one year or up to fifteen years.

Risk insurance is comprised of life, sickness and accident insurance and disbursed as a lump sum payment or as period payment.

The insurances are distributed either via the policyholder themselves or via insurance brokers. The policyholder's own distribution can be done via advisers or the insurance company's websites. Several of the biggest unit-linked and deposit-linked insurance companies in Sweden are owned by banks.

Life insurance businesses are mainly regulated by the Insurance Business Act (2010:2043) and Insurance Distribution Act (2018:129). The configuration of insurance products can be linked to national taxation rules and the social security system. A significant majority of policyholders (natural and legal persons) are resident in Sweden.

Key figures	
Number of insurance companies	30
Number of employees	5 899
Number of business connections established	8 122 279
Company balance sheet total	3 675 194 105 125
Company turnover	174 537 391 432
Total number of physical customers	7 640 752
Total number of legal customers	969 290

Source: The FSA's periodic reports on money laundering, reference date 31.12.2024. The details are based on the reports of the institutions to the FSA and the table can, therefore, include data which deviates to some extent from the actual situation.

Money laundering – description of the risk scenario including known approaches

A threat actor or front man invests in savings insurance. A endowment insurance policy is often used, with subsequent repurchase or disbursement according to the insurance contract (see also under 7.5, Insurance brokers). Disbursement is made either to the policyholder or the person named as beneficiary in the policy. The policyholder can change the beneficiary provision at any time.

Threats – money laundering

Scope

Life insurance products turn over huge amounts, which makes them attractive to criminal exploitation for money laundering. But for pension insurance the risk of money laundering is low, given the limitations on from which age pension disbursement can start and for how many years they can run. For endowment insurance, the risk is higher, but often contains caveats to prevent premature repurchase. These factors are deemed to make life insurance products less attractive from a money laundering perspective, especially for layering crime proceeds for example, as fast transactions are often a precondition.

As far being exploited for various money laundering schemes, the sector is therefore deemed to primarily be used for the long-term integration of criminal proceeds in the legal economy, as traceability of such proceeds can be relatively obscured.

Threat actor capabilities

The threat actors need to know about the products and be able to plan their approaches. It cannot be excluded that the volumes laundered within the sector risk being high in individual cases, and that well-planned schemes are used to a large extent.

Anonymity

The chances of tracking transactions are complicated by the threat actor using straw men and complex corporate structures are used when taking out pension insurance for example, as part of a criminal scheme. International schemes have been identified in which facilitators within an insurance company have taken part in packaging complex products, for example. If an insurance company is owned by a foreign holding company, there are also money laundering risks associated, as the chances of conducting supervision on foreign owners are low.

Summarising assessment

The sector's products normally have a low transaction rate and endowment insurance often carries limits that prevent premature repurchase. Threat actors also need to know about money laundering schemes in the sector, or have access to facilitators with such knowledge and abilities, for example, professional money launderers. The volume laundered risks being high in individual instances. More advanced money laundering schemes using facilitators cannot be ruled out. Consequently, the sector is deemed to have a certain risk of money laundering.

In conclusion, the threat regarding money laundering in the sector is deemed to be moderate.

Vulnerability – money laundering

The chances of detecting money laundering

The transaction rate in the sector is relatively low and the sector is not exposed to cash. The transactions are mainly deemed to be national. Foreign endowment insurance products are known however, which risks impairing traceability and the ability to make checks. Traceability for national transactions, which are largely administered via Swedish credit institutions, is generally deemed to be good.

The life insurance products regarded as representing the biggest risk of money laundering are endowment insurance, mainly deposit-linked. Deposit-linked insurance has a short placing horizon, often including time restrictions for when repurchase can be made and the options for placing are unrestricted. Vulnerability to money laundering can also be present in the instances when a life insurance company is owned through a foreign holding company, as the chances of conducting supervision on foreign owners are low.

Compliance

Several of the life insurance company's compliance functions assess the risk of money laundering as being high and which the company must address. The compliance functions are often relatively small, especially in relation to the size of equivalent functions in the large credit institutions. The function can consist of one person in smaller life insurance companies. The internal audit function is also often small in relation to the size of equivalent functions in credit institutions. The compliance and internal audit functions can also be contracted out.

If the company has limited resources for combating money laundering in its first line of defence, and there are similar limitations for the second and third lines of defence, it can lead to there being inadequate risk awareness within the organisation.

Supervision by the FSA⁵³ has identified that the companies can improve their anti-money laundering efforts, including by better adapting risk assessments to the ways their products are exploited for money laundering to the specific risks they face. There can also be a risk from distribution via third parties, such as insurance brokers. In such instances, business and remuneration models imply a risk of insurance companies have lower incentive to check the transactions conducted through brokers.

The funds invested in insurance policies rarely go via the life insurance company. Most contributions go through the traditional banking system instead. Such types of transactions are therefore partially checked by the credit institutions, which have relatively high capacity to monitor transactions.

Life insurance companies do not need to identify, monitor and handle the risks related to money laundering themselves. They can only rely on the measures taken by other obliged entities. Normally, the biggest life insurance companies have more resources to check and those companies that own or belong to a group including a bank, naturally have access to group systems dedicated, for example, to detecting money laundering. However, many of the functions for compliance and internal audit run by the companies have identified breaches in the checking environment.

⁵³ Dealing with the risk of money laundering by the life insurance companies, FIU supervision no. 32, January 2025.

Reports and SARs made by the sector to the FIU have increased since 2020, but remain at a low level. In 2024, the sector submitted a total of 68 SARs. The fact that reporting remains low can be due to the vulnerabilities described above, but could also be the result of the scope of money laundering within the life insurance sector is smaller than for other financial activities. However, the FSA has noticed in its supervision⁵⁴ that the companies report few activities and suspicions to the FIU, and that several companies have not reported any suspicious transactions or activities at all. This is despite there being relatively many alarms arising from their transaction monitoring. But this could be due to the scenarios of many companies for detecting suspicious activities are inadequately adapted to their business.

Summarising assessment

The sector is cash-free and transaction speed in the sector is relatively low. However, several of the compliance and internal audit functions of the life insurance companies are often relatively small, and can comprise only one person in the smaller companies. Limited resources can imply lower risk awareness within a life insurance company. Consequently, the sector is deemed to have a certain risk of money laundering.

In conclusion, the threat regarding vulnerability to money laundering in the sector is deemed to be moderate.

Risk – terrorist financing

There is no known approach by which the sector is used for terrorist financing in Sweden at this time. No international surveys have been conducted. The sector's risk of terrorist financing has therefore not been assessed.

⁵⁴ Dealing with the risk of money laundering by the life insurance companies, FIU supervision no. 32, 31 January 2025.

7.3 Securities business

Overall sector risk:



Obligated entities within the securities industry invest or offer services within investment on a professional basis.⁵⁵ Securities businesses are often international and the companies within this sector can provide services within multiple jurisdictions.

General description of the sector and related products or activities

The securities market is dominated by the banks licenced to provide investment services. A minority of large actors dominate the sector and account for the majority of employees, turnover and assets in the sector. Apart from these, there is a majority of small businesses in the sector.

Securities companies are mainly regulated by the Securities Market Act (2007:528). Chapter 2, section 1 of the act sets out the main products and services that can be provided. The most common services are:

1. receiving and forwarding orders for one or more financial instruments
2. executing orders on behalf of customers
3. portfolio management
4. investment advice

Trading in securities can either be conducted directly by the broker (point 2) or indirectly through advice or the brokerage of orders (points 1 and 4).

Securities companies have to be licenced by the FSA. There are also securities companies that have several different types of licence, such a licence for insurance brokerage.

Key figures	
Number of companies	118
Number of employees	2 454
Number of business connections established	1 052 473
Company balance sheet total	23 418 491 504
Company turnover	16 629 950 224
Total number of physical customers	891 288
Total number of legal customers	171 461

Source: The FSA's periodic reports on money laundering, reference date 31.12.2024. The details are based on what the institutions reported to the FSA.

The key figures indicate that the number of companies in the sector is about the same as in the last sector report. But the number of customers and established business connections has risen considerably, which may explain the increases in turnover and assets.

⁵⁵ Chapter 1, section 2(1), para. 3 of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

Money laundering – description of the risk scenario including known approaches

Threat actors can use the sector's products themselves or via a front man, for example by buying and selling securities with money from illegal activities. The objective is to diversify or integrate money. In addition, investments in most types of securities can yield returns, making them an attractive means of integrating criminal proceeds into the legal economy over the long term.

Investments in securities can involve several different long and complicated transaction chains designed to conceal the source of the funds. Because the money has passed through long chains in the financial system, it appears as legal when it is invested in securities. The use of various banks for various transactions can also make it hard to gain an overview of the full transaction chain for obliged entities and authorities. In other words, the sale, repayments and repurchase of securities can create a legitimate explanation for the source of the assets. To follow are examples of such approaches.

Insider trading using secret identities

Using front men or complex corporate structures, people with an insight into their company can commit the crime of insider trading by conducting transactions in the sector. This means that the threat actor uses information unknown to the general public for personal gain by trading in securities, for example. The proceeds of that crime can then be laundered by trading in other securities or layered through the financial system to accounts in Sweden and abroad. Such schemes can be run in real time.

Lending through corporate bonds used for money laundering

A company can be pledged for the purpose of money laundering by using corporate bonds as part of the scheme. A broker issues the corporate bonds and sells them to customers who invest in the bond. The company later reimburses the bond with funds from illegal activities such as layering and integration. The capital brought in by the issued bonds can also be used to finance other illegal activities. The scenario includes other types of schemes in which financial instruments can be used for money laundering.

Deposits to another person's securities account

The services of the broker can be used to diversify money by threat actors transferring it to the securities accounts of other people. The broker can check that disbursements only go to the account that belongs to one customer, but does not have the same opportunities to check when deposits are made. This means that large values can accumulate from many different depositors. When the money is later disbursed, the recipient bank only sees that the money originates from the customer's securities deposit account, which gives an apparent legitimate explanation as to its source.

Threats – money laundering

Scope

The scope and frequency of money laundering in the sector is hard to assess, as the number of SARs to the FIU is low. Very large transaction amounts can, however, be found in the reports that are received. Intelligence exists that a number of threat actors use the sector's products and accounts to layer and integrate funds from criminal activities, and that they use the sector to commit predicate offences to money laundering, for example, various types of financial crime and investment fraud.

Threat actor capabilities

A certain level of expertise is required from threat actors for more complicated money laundering schemes, along with facilitators to run money laundering in the sector. For those actors with high capability – i.e. access to know-how, capital and facilitators – considerable opportunities for money laundering are deemed to exist.

Anonymity

It is believed to be hard to anonymously conduct transactions within the sector. There is therefore a risk that front men are used, which impairs the chances of identifying the principal. Fairly complex corporate structures in Sweden and abroad can also reduce transparency for transactions and in that manner conceal the identity of the principal.

Summarising assessment

Intelligence exists that a number of threat actors use the sector's products and accounts to diversify and integrate funds involving individual criminals and actors linked to organised crime. The sector can be exploited, for example, by funds from various depositors being concentrated in a receiving account. At the next level, the recipient of the funds can refer to the sale of securities certificate to legitimise the sources of the funds.

In conclusion, the threat regarding money laundering in the sector is deemed to be significant.

Vulnerability – money laundering

The chances of detecting money laundering

Transactions involving securities can often be conducted in real time, which makes them attractive to exploit for money laundering. International companies are involved in the sector, operating with licences from low-taxation jurisdictions. These obliged entities help increase the sector's vulnerability to money laundering.

There is vulnerability in the sector due to it not always being possible to identify the individuals who conduct transactions in the sector. For example, trading in securities through corporate structures which are complex or not fully transparent. Businesses and transactions with counterparts in jurisdictions with less effective AML systems are also deemed to increase vulnerability.

The rules for why certain types of international transactions⁵⁶ have to be reported to the Swedish Tax Agency are regarded as reducing vulnerability to money laundering to some degree. Another factor that reduces vulnerability is that the sector is mainly cashless.

Compliance

A large part of the companies in the sector have few employees. This often means that their checking functions are small. This can affect the handling of money laundering risks and limit risk awareness in the company. Reports from company functions on compliance are relatively limited in scope and breaches are rarely identified. When an adviser becomes Swedsec-licensed, they are required to be aware of parts of the AML regulations. The requirements include awareness of customer due diligence procedures, transaction monitoring and reporting suspicious transactions to the FIU. Supervision of the sector has identified areas of improvement with regard to risk management, including practical compliance for companies with their own internal instructions. Checks (such as those described in their internal rules) may not always be implemented or only implemented to a limited degree.

Few SARs reach the FIU from the sector. 22 reports were received in 2024, and 6 in 2020.

Experience from supervision⁵⁷ show that securities companies have processes and routines in place in the AML procedures, but that there is room for improvement. Risk assessment of how their products can be exploited for money laundering are not always adequately adapted to the specific risks found in the business. Some companies active within several sectors do not seem specifically aware of the securities business in their general risk assessments, and focus instead on another type of activity that they also run. The companies can also take very different views on which risks are associated with the industries to which their customers belong. Some companies distribute most of their securities products through companies external to their own group, which can increase their vulnerability to being exploited for money laundering. Neither is transaction monitoring deemed to be fully adapted to the activity. For example, companies can have a suspicion of market abuse, but have not been aware that the transactions

⁵⁶ Statement of payments from or to countries outside Sweden (KU80 and KU81).

⁵⁷ Dealing with the risk of money laundering by the securities industry, Swedish Financial Supervisory Authority supervision no. 31, January 2025.

can indicate money laundering. The low degree of reporting to the FIU in relation to the number of alarms generated by the sector's transaction monitoring systems can be due to companies lacking or only having a few scenarios that are fully adapted to the activity they are engaged in.

Summarising assessment

There is generally room for improvement in companies with regard to internal risk management and their handling of money laundering risk. The sector is believed to under-report suspicions to the FIU. International transactions with, in some instances, shady ownership structures and beneficial owners for most of them also contribute to higher vulnerability.

In conclusion, the vulnerability to money laundering in the sector is deemed to be significant.

Risk – terrorist financing

There is no known method by which the sector is used for terrorist financing in Sweden at this time. No international surveys have been conducted. The sector's risk of terrorist financing has therefore not been assessed.

7.4 Certain financial business

Overall sector risk:



Certain financial business are a diversified category consisting of natural or legal persons professionally running certain financial services as defined in the Banking and Financing Business Act (2004:297), such as leasing and factoring.

General description of the category and related products or activities

All companies in the category whose financial activity is subject to mandatory registration with the FIU and covered by the AML regulations. The category includes obliged entities conducting one or more of the activities stated in chapter 7, section 1, first and second paragraphs and fifth-twelfth paragraphs of the Banking and Financing Business Act. A large number of activities of varying character are involved:

- providing or brokerage of credits
- participating in financing (e.g. factoring and leasing)
- provision of means of payment
- assuming guarantees
- participation in securities emissions
- provision of financial advice
- holding securities
- running letter of credit activities
- provision of safety deposit services
- running currency trading.

Common to the various activity categories is that they concern examples of activities that a credit institution can run within the auspices of its licenced bank or financing business. Exempted from the obligation to register are financial companies, which, according to the law, are covered by an obligation to be licenced, e.g. a credit or payment institution.

Those companies that are registered to run certain financial activities must state which type of activities they intend to run.

Transformed sector

The act that regulates certain financial business has previously covered a wider range of them. In conjunction with the entry into effect of EU regulations, suppliers of crowdfunding financial services and cryptoasset services are removed from the legislation.⁵⁸ They now comprise their own sectors (see under 7.12 Crowdfunding financing and 7.13 Suppliers of cryptoasset services).

⁵⁸ Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937 and Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

The sector previously also included deposit brokers running activities in accordance with the Deposit-Taking Activity Act (2004:299). The act ceased to apply on 1 January 2021 and only some companies were registered before the law was repealed who continue to offer deposit-taking activities. Those companies are not subject to supervision by the FSA, but the authority does check the suitability of owners and management amongst other things.

The latest amendment to the act came into effect on 1 July 2025, when currency exchange became subject to a separate act, (2025:250), which lays down a requirement for licencing (see also under 7.28, Currency exchange). In conjunction with the amendment, the act changed name from the Act on Currency Exchange and Other Financial Activities to its current name.

As from 1 March 2026, certain other financial activities will be covered by the Act on Criminal Liability for Illegal Financial Activities (2026:56). This implies that it is a criminal act to provide the service without being registered.⁵⁹

Key figures	
Number of companies	316
Number of employees	6 580
Number of business connections established	884 420
Company balance sheet total	309 205 123 296
Company turnover	50 401 186 902
Total number of physical customers	1 693 764
Total number of legal customers	167 181

Source: The FSA's periodic reports on money laundering, reference date 31.12.2024. The details are based on the reports of the institutions to the FSA and the table can, therefore, include data which deviates to some extent from the actual situation. The key figures above are for currency exchangers and certain financial activities jointly, as the sectors were previously regulated by the same act.

Money laundering – description of the risk scenario including known approaches

Leasing

There are a number of known money laundering schemes that involve leasing companies. They are often a question of alleged goods leased out for payment with criminal proceeds. A threat actor sets up a leasing agreement for a product that does not exist, for example. Payments are then made by the threat actor or an accomplice and represent a transaction without anything in return. Black money can be integrated and diversified.

Another approach involves a leasing company setting up a false leasing agreement regarding, for example, property or equipment through a company to embezzle a payment from an unsuspecting credit institution. Some equipment is not leased out to the company customer and in many instances is not even bought in by the leasing company. In fact, the money is forwarded to the company customer in the form of a loan. Repayment of the loan is then made from crime proceeds from the company customer to the leasing company through monthly invoices. The income to the leasing company can finally be used to repay the credit institution or repayment may only be made partially or not at all. In some instances, both the leasing company and customer company have links to organised crime.

Factoring scheme

Black money can be laundered and recycled through factoring, either through the provider of the service being exploited or consciously facilitating the scheme. When the actor is exploited, it buys invoices without thoroughly investigating the company and the individuals before buying the invoices. The actor then risks buying an invoice that has never existed or with an inflated value. In such instances, the factoring company is being exploited for fraud and money laundering. In those instances when the factoring company has knowingly bought false invoices, it is owned or controlled by threat actors who thereby knowingly facilitate money laundering (see also section 7.1 Banking and financing institutions).

⁵⁹ Prop. 2025/26:42, Criminal liability for illegal financial activities.

Corporate credit

Credit provision to companies is also common in the sector. It can be exploited for money laundering in the same way as other approaches when lending is disbursed with criminal proceeds.

Threats – money laundering

Scope

Because the sector is so multi-faceted, the methods used by threat actors can vary, depending on the type of obliged entity. Analyses by law enforcement authorities⁶⁰ have indicated that companies within the sector are exploited within criminal schemes and sometimes knowingly are run as purely criminal fronts. Factoring companies can be used for fraud and money laundering by them buying invoices which do not have an actual underlying claim. There are also approaches for of lending money to companies. The funds loaned are suspected of coming from crime and the credit beneficiary in such instances has criminal links. Repayment of loans to the credit provider can also be made using the proceeds from crime in some instances. There are a number of money laundering schemes that involve leasing companies. They are often a question of alleged goods leased out for payment with criminal proceeds. In some instances, both the leasing company and customer company are suspected of links to organised crime.

Threat actor capabilities

Leasing companies can be exploited by a threat actor by entering into leasing contracts and paying for the lease with criminal proceeds for use of the leased object, e.g. a car, or by aggressively paying off the lease and becoming the owner of the leased object to be able to sell it. False documents can be used in the application for a leasing contract. Factoring companies can be exploited by a threat actor by, for example, selling false invoices, via which they create an apparent explanation for transactions. Threat actors also collaborate with leasing and factoring companies, or actually control them.

Anonymity

Anonymity is possible in instances that concern transactions between companies and when the beneficial owner (i.e. the person who is the ultimate beneficiary of laundered money) operates behind straw men on the board.

Summarising assessment

Because the sector is so multi-faceted, approaches can vary depending on the type of obliged entity. There are examples of companies within these business categories being exploited or run as pure crime fronts, and examples of companies within the sector owned or controlled by threat actors.

In conclusion, the threat regarding money laundering in the sector is deemed to be significant.

Vulnerability – money laundering

The chances of detecting money laundering

The sector is deemed to be close to the limit for existing cash handling, and few international transactions are conducted within it. Businesses within the sector still risk being used to launder money.

The AML act does not differentiate between companies, as it applies the same requirements despite it concerning reportable and not statutory licencing. Statutory registration is also associated with simplified rules within other areas. In contrast to companies licenced according to the Banking and Financing Business Act (2004:297) (LBF), no capital requirements are applied to actors with registration obligation according to the Certain Financial Operations (Reporting Duty) Act (1996:1006) (LVA). Neither is there any reporting duty, no requirement for an auditor and no requirement for any special form of association. The threshold for running a business is therefore lower for a registration obligation actor according to the LVA than for financial companies licenced according to the LBF. Other requirements for owning and managing for these licences are limited compared to the businesses that must be licenced.

⁶⁰ Finanspolisen informerar: Kriminella tvättar pengar genom företag, May 2024. Ref. no. A258.662/2024. (In Swedish).

The risk of financial companies being exploited for money laundering is probably higher for companies required to register than for those that require a licence (for example, see prop. 2024/25:67, p. 52). It may be that the relatively low thresholds for setting up that registering entail, compared to applying for a licence, attract shady and sometimes purely criminal obliged entities to the sector. There is therefore a risk of a threat actor deliberately turning to a company obliged to register for the purpose of avoiding detection, which makes companies running certain financial activities vulnerable to being exploited for money laundering.

Compliance

Risk awareness in the sector varies between different business types. It can depend on the fact that certain types have only been in existence for a short time, and that the sector partially consists of small actors. Awareness and knowledge of the AML regulations is deemed to be low. The overall regulatory maturity is generally deemed to be low.

Because the sector consists of small companies, the criteria for managing risks linked to money laundering are a challenge; for example, when the company has to set up functions for combating money laundering.

Summarising assessment

Risk awareness in the sector varies between different business types. The sector mainly consists of small companies. Awareness and knowledge of the regulations for money laundering is generally deemed to be lower in small companies that do not have the same well-developed control functions that large companies have.

In conclusion, vulnerability to money laundering is deemed to be significant.

Risk – terrorist financing

There is no known method by which the sector is used for terrorist financing in Sweden at this time. No international surveys have been conducted. The sector's risk of terrorist financing has therefore not been assessed.

7.5 Insurance mediation

Overall sector risk:



Insurance brokers are natural or legal persons that professionally broker insurance products on behalf of insurance companies. This includes presenting insurance agreements and doing the preparatory work such as informing and advising before entering into an agreement, and in some instances, placing a financial instrument within the framework of an insurance product.

General description of the sector and related products or activities

Insurance brokers perform insurance distribution and are mainly regulated by the Insurance Distribution Act (2018:129). Insurance distribution requires a licence. Many actors within the sector are small businesses, usually with one to five employees, but the majority are large companies with many employees.

The sector for insurance distribution is divided into accident insurance and life insurance, similar to the division in the section on life insurance. This sector description only focuses on brokers of life insurance. The risk of money laundering when life insurance is distributed is highest when it concerns the distribution of endowment insurance. The same applies to the policyholder's own distribution of endowment insurance.

When an insurance broker distributes insurance products, it is always the insurance company that is the customer's contracting party. The insurance company is the actual owner of the financial instrument in an endowment insurance. All contributions and repurchases of insurance products are made through the insurance company. The responsibility for customer due diligence lies with the broker and the insurance company.

Key figures	
Number of companies	397
Number of employees	3 880
Number of business connections established	624 820
Company balance sheet total	16 248 971 182
Company turnover	8 628 431 467
Total number of physical customers	1 036 229
Total number of legal customers	192 978

Source: The FSA's periodic reports on money laundering, reference date 31.12.2024. The details are based on the reports of the institutions to the FSA and the table can, therefore, include data which deviates to some extent from the actual situation.

Since the last sector-based risk assessment, there are about 200 fewer companies in the sector. The reduction is due to many natural persons relinquishing their licence and applying for a new legal licence, and that the market has consolidated. Examples include a broker organisation buying up 40 member companies in 2021. Since the last sector-based assessment, there are also fewer legal customers, which is due to consolidation of the market.

Money laundering – description of the risk scenario including known approaches

Poor customer due diligence exploited

Brokered business relationships, i.e. those established and maintained through an insurance broker rather than directly between two principals, can comprise a risk scenario due to insufficient customer due diligence. Brokered savings products then risk reaching customers whose intention is to use them as part of a money laundering scheme.

There is also a risk of individual insurance brokers actively facilitating money laundering for criminal actors, for example, through ignoring shortcomings or errors in customer due diligence.

Examples of non-compliant customer behaviour:

- The customer will take out insurance for an amount that is unrealistic given the purpose of the insurance.
- The customer nominates a beneficiary outside the immediate circle of the policyholder.
- Frequent change of beneficiary.
- The customer repurchases an insurance, followed shortly after by making a new deposit.

Risks linked to endowment insurance

An endowment insurance policy is a form of savings scheme in which the capital is invested in an insurance policy owned by an insurance company. Endowment insurance products are more flexible than other insurance products, which implies particular risks of money laundering. A person can invest money from crime proceeds in an endowment insurance policy and then withdraw the money via "repurchasing". The policyholder can freely nominate a beneficiary, whether a natural or legal person, and a threat actor can therefore be appointed as beneficiary.

Possibility of mortgaging, pledging, or transferring endowment insurance policies

Additional risks linked to endowment insurance policies (and to top hat plans), are that it is possible to mortgage, pledge or transfer them. That means that other parties than the original policyholder can become a customer of the insurance company, which increases the risk of anonymity and impairs traceability. In some instances, it is even possible that someone other than the policyholder is responsible for premium contributions, which can also create anonymity and impair the traceability of the money.

Threats – money laundering

Scope

The threat profile within the sector is similar to that described in the section on life insurance (see section 7.2). The sector's products generally have a low turnover rate and the terms and conditions attached to the product often prevent or make early repurchase impossible, which can be used as a method for money laundering. Although money laundering is not deemed to be widespread in the sector, the volume of money that could be laundered is regarded as significant.

Threat actor capabilities

A threat actor trying to exploit an insurance broker must be familiar with the product to some extent, and be able to carefully plan money laundering, either themselves or through facilitators. This reduces accessibility to life insurance products, making them less attractive for money laundering. However, the threat profile is deemed to be higher when savings products are sold via insurance brokers, as they often do not have the same resources for initial customer due diligence that large insurance companies have. There is also a risk that individual insurance brokers can act as active facilitators for money laundering on behalf of criminals.

Anonymity

It is deemed to be hard for a threat actor to use the sector's products anonymously because of the extensive customer due diligence and identification requirements applied to obliged entities within financial services, especially within life insurance and savings products. But the possibility of anonymity

does exist through mortgaging, pledging or transferring endowment policies being possible, and that it is possible for someone other than the policyholder to be responsible for premium contributions. A beneficiary can also be a person who is not a customer and is therefore unknown to the obliged entity.

Summarising assessment

The sector's products normally have a low transaction rate and often have constraints that prevent or make premature repurchase impossible. The threat actors need to know about the products and the chances of acting anonymously within the sector are low. Although money laundering within the sector is not deemed to be widespread, the volume of money that could be laundered is regarded as large. There is also a threat that individual insurance brokers can act as active facilitators for money laundering on behalf of criminals. Consequently, the sector is deemed to have a certain risk of money laundering.

In conclusion, the threat regarding money laundering in the sector is deemed to be moderate.

Vulnerability – money laundering

The chances of detecting money laundering

The transaction rate in the sector is deemed to be relatively low and the sector is not exposed to cash. However, the sector's products can act as long-term placements for criminal proceeds that are already integrated, or are on the way to being integrated, in the legal economy.

The risk of money laundering in the life insurance sector primarily arises upon deposits being made, savings and repurchase of savings products via deposit-linked insurance products, and these risks are not addressed in the first instance by insurance brokers. The main risk exposure for brokers lies instead in the initial handling of customer due diligence.

Initial customer due diligence procedures should be performed by the broker in a business relationship. Many brokers within the sector are small or family enterprises which may not be able to conduct effective customer due diligence compared to larger companies. For example, small brokers often have limited access to system support to investigate a politically exposed person (PEP) and to check sanction lists compared to large brokers.

Another vulnerability is that life insurance companies rely on the initial customer due diligence conducted by the broker, which can impair the effectiveness of the company's own customer due diligence process and ongoing monitoring of the relationship.

Yet another vulnerability is the conflict of interest that exists in the sector. This conflict concerns the commission brokers earn from life insurance companies when brokering a product. A customer due diligence process can lead to more refusals, which implies that the economic incentive risks affecting the thoroughness of the customer due diligence process negatively. This can increase the risk of non-compliant or suspicious transactions being conducted, such as a large deposit in life insurance just before retirement, which can enhance layering and integration.

Compliance

There are significant differences between insurance brokers when it comes to risk awareness and organisational prerequisites. For smaller brokers, the prerequisites for good risk awareness and adequate system support can be poor. By licencing or certifying insurance brokers through some form of licencing body, customer requirements in tests can be linked to parts of the AML regulations. But conflicts of interest can still arise related to remuneration models, which can lead to lower incentives for distributors to strengthen their risk management procedures.

Potential under-reporting is mentioned in the report to the FIU in the previous sector-based risk assessment. The fact that insurance brokers have only submitted one money laundering report to the FIU in 2024 indicates this is continuing.

Summarising assessment

The transaction rate in the sector is deemed to be relatively low and cash is not used. Most transactions are national, and traceability is deemed to be relatively good. However, risk awareness does vary between obliged entities and reporting to the FIU is almost non-existent. One vulnerability is the conflict of interest in the sector concerning the commission brokers earn from life insurance companies when brokering a product. Another vulnerability is that life insurance companies rely on the initial customer due diligence conducted by the broker, which can impair the effectiveness of the company's own customer due diligence process and ongoing monitoring of the relationship. Consequently, the sector is deemed to have a certain risk of money laundering.

In conclusion, the threat regarding vulnerability to money laundering in the sector is deemed to be moderate.

Risk – terrorist financing

There is no known method by which the sector is used for terrorist financing in Sweden at this time. No international surveys have been conducted. The sector's risk of terrorist financing has therefore not been assessed.

7.6 Issuers of electronic money

Overall sector risk:



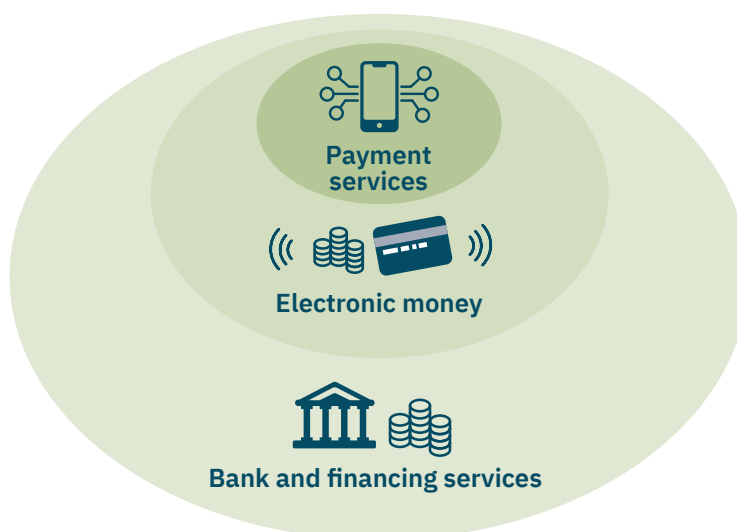
Electronic money is an electronically stored monetary value that represents a drawing on the issuer. Electronic money is given in exchange for funds to execute payment transactions according to the Payment Services Act (2010:751), and is approved payment funds by parties other than the issuer.

General description of the sector and related products or activities

To be able to issue electronic money (e-money) usually requires a licence from the FSA according to the Electronic Money Act (2011:755). Any issuance of electronic money has required a licence since 1 July 2025, and the category of registered issuers has been scrapped.⁶¹

An institution for electronic money (e-money institution) can also provide payment services according to the Payment Services Act (see also 7.8 Payment institutions). On the other hand, a company licenced to provide payment services cannot issue e-money under the auspices of its licence, although banks and credit market companies may under the auspices of an existing licence.

Figure 7.6.1 Visualisation of consumption of licence



E-money comes mainly in two forms: hardware and software based products. Hardware based e-money is stored as a physical product, e.g. on a card, and is transferred to the recipient through reader devices, such as a card reader. In common with most payment cards, e-money has an offline limit which means that it can only be used for purchases up to a certain amount set by the issuer without being connected. The card reader saves the card data and sends the file once connection is restored. Software based e-money is stored on a computer or smartphone and requires internet connection to transfer the money.

An example of services regarding e-money are prepaid cards. In such instances, funds are deposited in a trust account owned by the e-money institution, and that a user has deposited via a payment method for future purchases.

61 Prop. 2024/25:67

Foreign companies within the EEA licenced to issue e-money in their own country do not need a licence from the FSA to issue e-money or offer payment services in Sweden. But any actors running cross-border activities in Sweden with no subsidiary or representative must be registered in the FSA's register. Registration is executed when the FSA has received notification from the actor's own country. There are around 230 foreign e-money institutions with cross-border activities registered in the FSA's register at this time.

Key figures	
The statistics do not include companies in other EEA states offering their services in Sweden.	
Number of companies	7
Number of employees	192
Number of business connections established	113 937
Company balance sheet total	2 784 820 435
Company turnover	362 022 797
Total number of physical customers	206 574
Total number of legal customers	23 344

Source: The FSA's periodic reports on money laundering, reference date 31.12.2024. The details are based on the reports of the institutions to the FSA and the table can, therefore, include data which deviates to some extent from the actual situation.

Money laundering – description of the risk scenario including known approaches

The approaches for laundering crime proceeds are changing and developing in line with new payment solutions and actors entering the market.

E-money institutions primarily aim at corporate customers, which increases the risk of exploitation for money laundering by criminal actors using the company as a front.

Neobanks

Due to the wide area of applicability, e-money institutions can also fall under the title of neobank. Neobanks have been previously assessed by the Coordination Function in a separate national risk assessment.⁶² Neobanks offer bank-like services associated with a significant risk of money laundering. Many of them offer services that provide a degree of anonymity, amongst other things. They also provide fast, international transactions with many parties and jurisdictions involved, which impairs the traceability of such transactions.

Criminal actors use neobanks widely for such purposes as varying their money laundering schemes, layering money and spreading their illegal assets. Neobanks are used in money laundering schemes when criminal proceeds are moved from regular bank accounts to a neobank account, sometimes via different payment platforms.

Currency exchange and card payments

E-money institutions can provide payment services, which means they can provide services that facilitate card payments, such as issuing cards and other payment instruments and the redemption of card transactions. They can also conduct currency exchange, i.e. professional trading in notes, coins and travellers checks in foreign currencies. (see also 7.8 Payment institutions).

Banking as a service

Banking as a service (BaaS) is a business model that makes it possible for financial companies to provide platforms via their APIs for financial services and products to their corporate customers, which in turn can offer bank-like services to their customers under their own brand. This does occur amongst e-money institutions, who can then facilitate digital provision of standardised financial products and services online through their platforms and financial infrastructure.

⁶² The Swedish Police Authority/Coordination Function. *National risk assessment 2023/2024 – Neobanks*. Ref. no. A340.719/2024.

Threats – money laundering

Scope

There are only a few companies licenced to issue e-money in Sweden, but they can offer their customers the option of large transaction volumes. The number of foreign institutions offering their services in Sweden has also grown in recent years, which implies greater accessibility which has raised the threat of money laundering further.

Threat actor capabilities

A business activity is required for threat actors who are trading and have to pay other traders in e-money linked to them. A certain amount of capability is needed to start a company for the purpose of laundering money. Companies being used as fronts is becoming more common, which indicates that threat actor capability has increased in recent years.

Anonymity

E-money institutions feature a high degree of technical innovation and digitalisation. In principle, all customer contact is digital and the process to become a customer is quick and wholly digital. This opens opportunities for the exploitation of identities and account straw men, which is deemed to be attractive to criminal actors. In addition is the fast processes for setting up new customers and business associates via which customers can sometimes have access to products and services without the e-money institution having verified the details the customer has provided.

Using the prepaid cards of e-money institutions, threat actors can remain anonymous and hide assets. Prepaid cards can be loaded with a value which can then be used with less traceability than a traditional bank card. Transactions using such cards are immediate and the chances of anonymity are deemed to be high. There is also a risk of the card being used by people other than the holder. These factors increase the degree of anonymity and the threat of money laundering within the sector.

Transactions via e-money institutions and other forms of neobanks are flexible, fast and international, and offer the opportunity for criminal actors to use an account at a neobank for concealment and to deal in and consume cryptoassets.

Summarising assessment

There are only a few companies licenced to issue e-money in Sweden, but they can turnover large amounts and make large transaction volumes possible. Using the prepaid cards of e-money institutions, threat actors can remain anonymous and hide assets. In principle, they are wholly digital with fast onboarding processes, which increases the risk of using account straw men and the exploitation of identities. Transactions via e-money institutions and other forms of neobanks are flexible, fast and international, and offer the opportunity for criminal actors to use an account at a neobank for concealment and to deal in cryptoassets.

In conclusion, the threat regarding money laundering in the sector is deemed to be high.

Vulnerability – money laundering

The chances of detecting money laundering

The facility of being able to quickly move large amounts inside Sweden and abroad impairs traceability within the sector. E-money institutions offer their corporate customers large credit facilities, which, when combined with international transactions and the ability to make cash withdrawals abroad, increases the risk of money laundering.

Through amendments to the Finality Directive⁶³, e-money institutions have been given access to local payment systems within the EU and direct access to the central settlement systems such as Bankgirot and RIX. Access to RIX gives connected institutions in turn the opportunity to offer direct payments

⁶³ An amendment to the Act on Systems for Settling Obligations in the Financial Market (1999:1309) to also give payment institutions and e-money institutions the opportunity to take part in settlement systems such as RIX. The amendments are linked to changes in the Finality Directive and the EU Payment Services Directive and have been implemented in local legislation throughout the EU.

without having an account at all connected banks. No requirement is made in Sweden for the presence of a subsidiary for international e-money institutions when a Swedish national account number is issued. In most other EU states, a strict subsidiary requirement is applied as the lack of such a requirement impairs supervision and, in turn, increases vulnerability to enable it to be used for money laundering.

Compliance

Suspicious activity reporting to the FIU from an e-money institution has increased significantly, from 13 reports in 2020 to 560 in 2024. The increase can indicate increased awareness in obliged entities, which in turn is partially due to the risks being highlighted by the authorities.

The FSA's supervision has indicated that the prerequisites for managing risks are found within certain parts of the sector. But experience from supervision has found extensive and significant breaches in compliance with the AML regulations in certain companies within the sector. The breaches identified pertain to the general risk assessment, which has caused risk assessment to be unable to support the company's other measures to combat money laundering and terrorist financing. The observations emphasise the need for customised risk assessment and an understanding of the risks a company's own activities are associated with.

Significant breaches have also been found in customer due diligence procedures and the reporting of suspicious transactions. Poor reporting of suspicious transactions to the FIU have very probably impaired the changes of law enforcement authorities being able to investigate suspected crime and to safeguard money.

The FIU revoked the licence of one company within the sector in 2025.

Summarising assessment

The opportunity to transfer large amounts with many parties and jurisdictions involved, and the opportunity to use cryptocurrencies, impairs the traceability and the sector is exploited a large degree for money laundering by criminal actors. Supervision has found extensive and repeated breaches of compliance with the AML regulations.

In conclusion, the threat regarding vulnerability to money laundering in the sector is deemed to be high.

Risk scenario, including known approaches of terrorist financing

The same method as described in the section on money laundering applies to a large degree to terrorist financing. Foreign e-money institutions can be used to forward money in a transaction chain to finance terrorism, for example, from a bank account to an anonymous alternative outside Sweden. The services are also used for transactions and consumption in Sweden as a more anonymous alternative to transactions from a traditional bank account. The services make it possible to handle transfers and consumption with considerably less transparency than if conducted via a Swedish bank account.

Threat – terrorist financing

Scope

A wider selection on the Swedish market and the accessibility via mobile services are deemed to have contributed to the scope of suspicious terrorist financing growing in the sector. Obligated entities are primarily used that are not based in Sweden, but that are aiming at the Swedish market.

Threat actor capabilities

The user needs to be familiar with the use of mobile services, but otherwise, no special skills are needed to use financial solutions in this sector.

Anonymity

With regard to the chances of being anonymous, no assessment has been made other than that for money laundering.

Vulnerability – terrorist financing

The chances of detecting terrorist financing

The challenges facing foreign obliged entities with regard to customer due diligence for Swedish customers can offer the chances of detecting non-compliant transactions diminish. Opportunities for working with Swedish law enforcement authorities are impaired as a result.

Compliance

Concerning compliance when it comes to terrorist financing, no assessment has been made other than that for money laundering.

7.7 Fund operations

Overall sector risk:



Fund operations can be divided into two types of activity:

- administration of mutual funds
- administration of alternative investment funds (AIFs).

The two types are governed by different regulations which are linked, as to a certain extent, the activities are similar and a large number of the fund managers have licences for both types. Because the risks are also deemed to be similar, both activity types are dealt with together in this section.

General description of the sector and related products or activities

Fund management can be divided into the administration of mutual funds and of alternative investment funds, known as AIFs. Special funds are separately regulated AIFs, which are usually marketed to non-professional investors in the same manner as mutual funds. In contrast to special funds, the marketing of other AIFs is mainly to professional investors. Under certain conditions, they can also be marketed to non-professional investors; for example, if the shares in the fund are accepted for trading on a regulated market. Examples of other AIFs are venture capital funds, property funds and credit funds.

Fund management is governed by the Investment Funds Act (2004:46) and Alternative Investment Fund Managers Act (2013:561 – LAIF). In contrast to the management of mutual funds and special funds, – which always requires a licence – the management of other AIFs either requires registration or licence. Which is required depends on the size of the capital under management. The rules in LAIF only applied to a limited extent to registered managers of AIFs.

The fund manager is responsible for portfolio and risk management, among other things. Fund management that requires a licence is subject to a depositary being used. The depositary holds the fund's assets and controls the flow of money.

Funds are usually not a liquid assets such as shares, as they are traded at special times, e.g. daily, monthly, quarterly, annually and are otherwise closed, which means they cannot be traded before a preset date in the future.

Fund management is largely international, mainly within the EU/EEA. There are a large number of funds based in other member states but that are marketed and sold in Sweden. The large fund managers of mutual and special funds for capital under management are found within the big banking groups. These funds are often distributed through banking activities. They can also be distributed via fund platforms and sold via insurance companies, for example under the framework of unit-linked or deposit-linked insurance, and through the premium pension fund market. Fund shares can be manager registered, in which case it will be the manager (usually a bank or broker and not the actual investor) listed in the fund's register of shareholders.

Funds that offer their products to the general public often sell their shares through other actors (e.g. banks). These distributors are usually registered by the fund manager, are subject to anti-money laundering supervision and are that link in the transaction chain with the best possibility of monitoring the investors. In such situations, the customers of the fund are not the final investors, but the distributors selling fund shares to their customers.

Key figures	
Number of companies	341
Number of employees	3 156
Number of business connections established	1 302 528
Company balance sheet total	121 068 208 135
Capital under management	9 225 849 699 861
Company turnover	34 628 838 746
Total number of physical customers	1 277 986
Total number of legal customers	28 261

The figures in the table are a composition of mutual funds and AIFs.

Source: The FSA's periodic reports on money laundering, reference date 31.12.2024. The details are based on the reports of the institutions to the FSA and the table can, therefore, include data which deviates to some extent from the actual situation.

As shown in the table, financial assets (capital under management) held by the companies is very extensive and has increased significantly since the last sector assessment.

Money laundering – description of the risk scenario including known approaches

Funds can be used for money laundering

Because many funds offer their products to the general public through distributors such as banks, their customers are often a bank and not the private investor. This means that in such situations, the bank bears the primary responsibility for customer due diligence and transaction monitoring of the investors. But the fund manager does need to have adequate customer due diligence to manage the risk with the distributor and the distributor's risk exposure. This implies that risks linked to the final investors impact the fund, even if those investors are not customers of the fund.

Funds of various type can, for example, be used for money laundering in situations when illegal money has to be layered and integrated into the financial system. Because funds often manage a large capital flow, it can be a tempting channel for potential large scale money laundering. In addition, fund investments, in common with investments in most types of securities can yield returns and dividends. Placing in funds can therefore be a long term way of integrating criminal proceeds into the legal economy. Despite investments often being for the medium to long term, there are also opportunities within the sector to launder money within the short term.

Threat actors can use the sector's products

Threat actors can use the sector's products, for example, by buying and selling fund shares to layer or integrate funds originating from criminal activities. In such instances, funds are relatively liquid assets, especially when listed on a stock exchange, as trading takes place in real time. The opportunity to quickly buy and sell such assets can be part of the layering phase in a money laundering scheme, for example. If disbursement of crime proceeds from a fund is made to another account than that where the money originated, it can also be part of the layering phase. Through disbursement of liquid assets from the sale of a fund, the recipient can give the appearance of money originating from crime coming from accumulated capital gains in a fund instead.

Straw men

Using straw men, for example when relatives to the criminal are listed as owners of a fund account, distance can be obtained from the money to reduce the risk of detection and possible forfeiture of criminal proceeds.

Deposits to another person's fund account

The fund account can be used to layer money by threat actors depositing it in another person's fund account, or if relevant, a liquid account. The fund manager can check that disbursements only go to the account that belongs to one customer, but does not always have the same opportunities to check when deposits are made. This means that large values can accumulate from many different depositors. When the money is later disbursed, the recipient bank only sees that the money originates from the customer's fund account, which gives an apparent legitimate explanation as to its source. It is also possible to move fund shares between the fund accounts of different people, and this procedure can also be used as part of money laundering.

Threats – money laundering

Scope

Money laundering within the sector can be hard to assess in a Swedish context, as suspicions reported to the FIU regarding fund investments are relatively few. The assessment is therefore based on the risk associated with the products and services the companies in the sector provide. Based on the total fund assets at the end of 2024 comprising SEK 8,355 billion⁶⁴ there can be a significant risk of money laundering. But this is not reflected by suspicions reported, which means that under-reporting of money laundering may be possible.

Factors which cause certain funds to be more exposed to money laundering include:

- investment strategies aimed at hard to value non-liquid assets
- complex, multilayered structures that include a large number of intermediaries
- transparency on the issue of owners
- limited capacity to conduct customer due diligence and financial incentives to tempt wealthy investors whose profile could indicate pronounced risk of money laundering.⁶⁵

The likelihood of the large amounts of money that could potentially be laundered through fund investments is deemed to be high, as funds usually have the capacity to absorb large sums. However, criminal proceeds that could end in funds are often already integrated in the legal economy, which means that funds do not comprise the first link in a money laundering scheme. Meanwhile, there are difficulties for the fund managers to trace the source.

Small funds such as those intended for a limited number of investors, can have a greater risk of money laundering, as it is more likely that the investors can exercise control over the fund assets than they can in funds intended for a wide range of investors. If the investors exercise control over the assets, the funds become personal solutions for asset management. This is a circumstance highlighted as a factor which indicates potential higher risk of money laundering in annex III of Directive (EU) 2018/849 of the European Parliament and of the Council.

Threat actor capabilities

A certain degree of specialist skills and a large amount of capital are required to use the sector for money laundering. These criteria reduce the risk of money laundering amongst the general public. But the access to individuals with high financial skills increased amongst criminals, including through access to PMLs. This makes more complex and in some instance more anonymous investment within the fund management sector possible. In many instances, the sector also offers simple digital solutions with no volume requirement, which make it easier to use the sector for money laundering.

⁶⁴ The fund manager's form of association, *Årsrapport: Fondsparandet 2024*.

⁶⁵ https://knowledgehub.transparencycdn.org/helpdesk/AIFs-in-Europe_ML-and-corruption-risks_Final_10.10.24.pdf

Anonymity

Managers of AIFs can invest in physical assets such as property or infrastructure, for example. If highly capable criminal actors collaborate with fund managers, they can create such a fund and thereby control the assets, whilst maintaining their anonymity externally. Another means of attaining anonymity is to use straw men when registering a fund account with a financial company, to deceive the checks made by obliged entities and the authorities. Such anonymity can also be a risk factor when the customer is a company, a trust or other legal construction with low transparency, and when fund shares registered with a manager when the actual shareholder is unknown. The threat profile grows more if any of these structures are also established in a jurisdiction associated with the increased risk of money laundering.

Summarising assessment

The sector is deemed to be attractive to threat actors with a lot of capital, high skills level and the capability to execute complicated schemes. Having said that, a simpler *modus operandi* can be used as access to the fund sector is open, including through online banks, apps and digital investment solutions. This means the volumes in some instance can be large, but smaller amounts can also be laundered within the sector, in some instance through relatively quick transactions.

In conclusion, the threat regarding money laundering in the sector is deemed to be significant.

Vulnerability – money laundering

The chances of detecting money laundering

Cash is very rare in the sector, which as a rule contributes to good traceability. The overall assessment is that transactions are traceable to a large extent, and that users of the products and services are identified to a large degree.

Fund-related transactions conducted in the sector usually take one or more days to execute and are deemed to be relatively easy to track. The more complex schemes are deemed to take longer, as the funds can involve hard to value and illiquid assets. Complex schemes can also consist of several layers of entities and involve multiple jurisdictions. These can have less transparency, which can reduce the traceability of the transactions conducted.

But it is possible for a person to deposit large amounts in someone else's fund savings without it being seen where the money comes from, which is a vulnerability. Third party deposits of this kind are associated with high risk of money laundering, as they can represent money transfers in practice.

Several funds are marketed internationally, which implies that money can be easily placed abroad through the purchase of fund shares. For example, a wide range of foreign AIFs are marketed in Sweden. When a fund manager or a fund is based outside the EEA, but has a licence to be marketed in Sweden, the risk of inadequate customer due diligence procedures grows if the fund does not use distributors within the EEA, such as banks. This is a vulnerability that can facilitate money laundering in turn.

Compliance

Fund managers rarely report suspicious activities regarding money laundering. The FIU received only two SARs from fund managers and seven from AIFs in 2024. These statistics indicate under-reporting to the FIU.

There are signs that the institutions do see breaches in the sector reports on compliance. The smaller companies are not deemed to have adequate resources to guarantee an effective control system, and therefore face the same problems as other sectors with poor organisational conditions. It is reasonable to assume that larger companies have more employees and should be better equipped. Smaller companies still need to ensure that they have adequate resources to be able to comply with the regulations. Bank-owned fund managers are deemed to have risk control functions in place, and can apply the systems and tools also used for banking activities.

The sector earns money based on the size of the capital managed and therefore has a major interest in receiving investments from customers. That interest should be able to influence the assessment of fund managers of the risk of their company being exploited for money laundering. The licenced fund managers are also subject to high requirements for compliance and impartiality for their control functions.

Summarising assessment

A large element of the sector is comprised of bank-owned fund managers deemed to have a relatively well-functioning control system. Other fund managers with a licence have also developed control systems. When investments are made via manager-registered companies, the fund managers become dependent on those companies having a well-functioning control system. However, the fact that it is possible for a person to deposit large amounts in someone else's fund savings without it being seen where the money comes from is a vulnerability. Reporting of fund transactions to the FIU is low, not least when compared to the sector's size. The smaller companies have fewer resources and control functions, and their compliance is deemed to have room for improvement.

In conclusion, vulnerability in the sector is deemed to be significant.

Risk – terrorist financing

There is no known method by which the sector is used for terrorist financing in Sweden at this time. No international surveys have been conducted. The sector's risk of terrorist financing has therefore not been assessed.

7.8 Payment institutions

Overall sector risk:



Payment institutions are obliged entities that offer licenced payment services.

General description of the sector and related products or activities

A payment institution is a limited liability company or economic association licenced to provide one or more of the eight payment services defined in chapter 1, section 2 of the Payment Services Act (2010:751 – LBT).

The core activity of a payment institution is to execute payments from sender to recipient in various ways, such as through cash transfers, transfers via various forms of online services (e.g. apps) and transfers via Autogiro. The company must apply for a licence for each separate payment service it wants to provide. It is common for payment institutions to offer a combination of several of the services listed in chapter 1, section of the LBT. For example, there is a large market for account information services and payment initiation services. There are also payment institutions with various specialities. A payment institution is not licenced to take deposits from its customers and cannot therefore provide savings and deposit accounts. But they can receive funds to be used for future payments from their customers.

The Swedish payment institutions include forms of fine tech companies or neobanks, i.e. companies that, for example, offer payment services based on digital and innovative technologies. There are also a number of foreign actors on the Swedish market, running activities through agents or subsidiaries in Sweden. These are regulated by the laws of their own countries and Sweden's within anti-money laundering, and supervised by the FSA. But there are also a significant number of foreign payment institutions providing services on the Swedish market with no physical presence in Sweden. The FSA has limited opportunities to supervise these.

A number of payment institutions offer their customers fast digital bank-like services for payments. By entering into a collaborative agreement with other financial institutions, known as "white labelling" schemes, payment institutions can offer their customers a wider range of products than would otherwise be possible. For example, a payment institution can market a deposit account or credit to its customers under its own name. Although the infrastructure for deposit accounts or credit will lie with the financial institution collaborating with the payment institution, and which has the appropriate licence. Payment institutions often have a high degree of technical innovation making it possible to quickly become a customer.

Because the Payment Services Act was superseded by the Electronic Money Act (2011:755 – LEP) and the Banking and Financing Business Act (2004:297 – LBF), companies running activities covered by these acts can provide payment services.

Money transfers as payment services

Money transfer is a payment service involving the transfer of money from a payer to a recipient without opening a payment account in the payer's or receiver's name. The transfer is executed solely to transfer a sum of money, either to a recipient or to a payment services provider acting on the recipient's behalf. Payment transfers are commonly made abroad. The payment institutions providing services in Sweden are largely foreign, with an agent in Sweden. In principle, there are three large actors established in Sweden.

Given the risks associated with the money transfer service, there are certain commonalities with other payment services, it is partially described separately in the following risk assessment.

Amended legislation

Since the amendments came into effect on 1 July 2025, it is no longer possible to grant exceptions from the licencing requirement to provide other payment services than account information services. In brief, the amendments involve cash currency exchange only being provided by payment institutions, institutions for electronic money and credit institutions, as well as subsidiaries of corresponding foreign companies, and that anyone granted an exception from mandatory licencing or registered for providing cash currency exchange had to apply for a licence by 31 December 2025.

It also implies that the risks associated with currency exchangers and registered payment service providers will partially follow along in the payment institution sector. The amendments also state that a company granted an exception from mandatory licencing to provide account information services will now be covered by PTL.

In addition, the Finance Ministry has produced the white paper on Criminal Liability for anyone running financial activities with no licence or registration etc., in which the criminalisation is proposed of the provision of financial services with no licence or registration. The new⁶⁶ acts came into effect on 1 March 2026. Payment institutions are also covered by the proposal.

The threshold for running payment service and currency exchange businesses has been raised by the change in the law. It is important that the appropriate authorities follow developments and are aware of whether the risks associated with registered payment service providers continue in the remaining parts of the payment service sector.

Key figures	
Number of companies	56
Number of employees	3 280
Number of business connections established	6 684 772
Company balance sheet total	21 066 229 515
Company turnover	8 375 761 086
Total number of physical customers	13 591 549
Total number of legal customers	148 763

Source: The FSA's periodic reports on money laundering, reference date 31.12.2024. The details are based on the reports of the institutions to the FSA and the table can, therefore, include data which deviates to some extent from the actual situation.

Money laundering – description of the risk scenario including known approaches

Money laundering within the sector can occur when the obliged entity is unaware of being exploited for that purpose, is aware of but deliberately fails to take adequate measures or is directly involved in crime and acting as a PML.

Paying for illegal goods

Threat actors pay for illegal goods or services via payment services. Sometimes payments go to frontmen, who then transfer the money, or withdraw them to hand them over in cash, to the beneficial owner or some other link in the transaction chain (layering).

Money transfers

Income from crime is laundered through money transfers, e.g. to countries outside the EU/EEA zones. The transferer sends funds, e.g. from Sweden, via complex payment chains with a large number of intermediaries and jurisdictions involved. That makes it hard to track the source of the funds. In some instances, frontmen are used, and it is not unusual for the money transferred to lie under specific amount limits to avoid stricter monitoring and measures applied by the obliged entities.

⁶⁶ Act on Criminal Liability for Illegal Financial Activities (2026:56).

The operators in the payment chain sometimes pass payments through formal and informal payment systems, which further impairs traceability. The risk of money laundering is especially high when cash is sent. Criminal proceeds can also be paid into their own or a straw man's bank account through payment transfer services. Income from serious crime is placed in this manner in the financial system. Cash withdrawals via money transfer can be made to pay black wages, for example.

Payment service agents as facilitators and professional money launderers

Payment service agents act on behalf of payment service companies offering payment services such as money transfers and the like. Payment service agents are a commonly utilised channel within criminal circles, and the risk of money laundering is high. Money transfers are often offered as a secondary service under the auspices of a business. Examples include tobacconists, convenience stores, hairdressers, travel agents or currency exchange bureaux.

Criminal proceeds can be sent via payment service agents to recipients with no bank account, often with foreign destinations. Swedish kronor can be sent from someone via an agent in Sweden and received in another country in the local currency. Some agents offer the option of depositing cash in a Swedish bank account. Criminal actors can use such opportunities themselves or via frontmen to launder money.

There is evidence that owners and other officers of certain payment service agents conducting transactions for criminals and receiving transactions suspected as being part of a money laundering scheme. It is likely that several of these agents actively facilitate money laundering for others, and in exchange for payment. It is also likely that criminal actors start or take over such businesses with the primary purpose of laundering money.

Because payment services sometimes offer several various payment service systems for transferring in parallel, the possibility exists that criminal actors use multiple channels for laundering money. In that way, they can spread their transactions and stay under the relevant amount limits to minimise the risk of detection. Using multiple agents for criminal transactions also increases the risk of large volumes passing unnoticed through the monitoring system.

Payment services linked to online casinos

Payment institutions can handle payments for other services that have a high risk of money laundering, such as online casinos and crypto exchange platforms. Such services can also comprise a link in a layering scheme and thus impair tracing of the source of crime proceeds. There are vulnerabilities in payment service companies and gambling companies with regard to checking who owns an account, where money comes from and where it goes to. Using a payment service, threat actors can move money to and from online casinos where money is won or lost, sometimes between collaborating parties, for it then to be paid to a bank account.

White labelling schemes

The use of white labelling schemes has been identified as a risk in the sector. A white labelling scheme involves a company (the manufacturer) producing a product or service which is then licenced or sold under the band of another company (the reseller) instead of the manufacturer's. The scheme allows the institution to provide financial services through a collaborative agreement with other financial institutions. It can risk leading to confusion as to where responsibility lies for customer due diligence and transaction monitoring, for example.

Virtual IBAN

The use of virtual IBAN⁶⁷ makes it harder to detect money laundering, as it facilitates international payments that mask the identity of the main account, the executor and country of origin. In theory, there is no limit to the number of intermediaries between an institution and an end customer.

⁶⁷ A virtual IBAN (vIBAN) is a unique digital bank account number linked to an exclusive primary bank account instead of a separate physical account.

Threats – money laundering

Scope

Services are used to a relatively large extent for payment of illegal goods or services, and in layering schemes, where traces of the source of the crime proceeds must be erased. The sector is frequently used to launder money, and the various payment services are repeatedly exploited by organised crime. Because transactions of varying amounts can be executed frequently and to several different recipients, the overall volume is high. The sector is deemed to be exploited for money laundering to a large degree.

The number of SARs made to the FIU in 2024 from the payment institution category was 4,428, which is around 10% more than in 2020.⁶⁸

The number of payment institutions has increased by around 45% since the last sector-based risk assessment was written. It can be assumed that the increased number of actors also reflects the scope of money laundering in the sector.

Threat actor capabilities

The payment services offered by payment service institutions are often developed by companies active within fine tech and neobanking, and are often designed to have a high level of usability. No special skills are therefore needed by the user. Payments and transfers are also executed very quickly, which increases the attractiveness for money laundering in the sector.

Intelligence indicates that payment service agents are used repeatedly by criminal circles. In some instances, links have been found between the officers of payment service agents and criminal networks, mainly at local level where criminals exercise influence on businesses. It is not unusual for a company of this type to be owned by criminal actors, and it can be difficult for legitimate business owners offering payment services to operate in the exposed area. Criminal networks exert illicit pressure and use the companies for money laundering and storing drugs.

Anonymity

The chances of users initially being anonymous are relatively low. Threat actors therefore often use straw men to conduct transactions at one or more levels. That makes it hard to track the source of the funds.

Experience from supervision shows that payment institutions with fast digital payment services offer the opening of customer accounts remotely, without any physical attendance. Supervision also indicates that some institutions have less extensive customer identity checks compared to the traditional banks, which makes it possible for a threat actor to be partially anonymous through false identities or frontmen. A lower degree of checking thus leads to better chances of anonymity. The use by threat actors of companies as fronts for crime also increases the chances of remaining anonymous through false boards of directors and similar schemes.

Focus on money transfers

The money transfer payment service is simple to exploit as part of a money laundering scheme and for layering. No special level of skills is required. Transfers can be made almost immediately and cash is very common.

There are indications that threat actors use false ID documents, whilst a number of money transferers are unable or unwilling to undergo a thorough ID check and monitoring of non-compliant behaviour and transactions. Anonymity is also possible in the sector. Otherwise, obliged entities only need to perform customer due diligence for transactions that individually or collectively exceed €15,000 if there is no question of a business association. Threat actors can therefore make structured money transfers within certain amount limits to minimise the risk of detection and reporting. This possibility is deemed to increase the threat of money laundering in the sector.

⁶⁸ In 2020–2021, the category "Payment services" included both payment service providers and payment institutions. From 2022 onwards, the subcategories have been divided and reported separately. The number of SARs in 2024 from payment services companies was nine.

Summarising assessment

The sector is deemed to be systematically used to launder money, and the various payment services are repeatedly exploited by organised crime. In some instances, links have also been found between the officers of payment service agents and criminal networks. Because transactions of varying amounts can be executed frequently and to several different recipients, the overall volume is high. Payment services offered by payment institutions are often very user friendly, and transfers are often executed very quickly, which increases the attractiveness for money laundering. Establishing customer relationships is often remote, which increases the chances of using frontmen or false identities, which also contribute to the threat level in the sector.

In conclusion, the threat regarding money laundering in the sector is deemed to be high.

Vulnerability – money laundering

The chances of detecting money laundering

The payment volume and proportion of the international flow within the sector differs between different payment service providers. When digital solutions are concerned, transaction traceability is deemed to be good. But institutions licenced for money transfers be cash-intensive businesses. It is harder for some services for the payment receiving institution, e.g. a bank, to get information on who has initiated the payment. Such a risk is present when payment has been initiated by an officer of the TPP (third party provider) supplying the pay file. In such instances, the bank can see that the payment comes from the TPP. But it cannot see that the payment has been initiated by an agent. Procedures for customer diligence or transaction monitoring can therefore be impaired.

Transactions can be made instantaneously for several payment services. Another factor that increases vulnerability for money laundering is that a number of payment institutions offer their products and services via agents or collaborating company applications. The payment institution has to ensure that the agent lives up to the requirements set by the institution (through its management of third party risks) and the regulations for money laundering, which can imply a vulnerability. Money transfers involve a high volume of international transactions, which sometimes go outside the EEA. The use of cash by customers is common, which limits traceability.

There are also several foreign payment institutions on the Swedish market with no physical subsidiary in Sweden. These come under supervision of the supervisory authority in their own country. There is a risk that foreign payment institutions have poor knowledge of their customers' financial behaviour on the Swedish market, and have insufficient knowledge of Swedish conditions and what is regarded as risky behaviour in a Swedish context. This can make threat actors seek foreign institutions.

A complicating factor with regard to the chances of detecting money laundering within the sector is that the verification and customer due diligence process performed by payment institutions using fast digital processes for payments is purely digital, rather than physical. In some instances, the institution uses a verification process in which the customer is asked submit a certified copy of their ID card. Such a process means it is possible for a threat actor to use someone else's identity. The same applies to verification processes when e-ID is used to identify the customer.

The use of virtual IBAN can make it harder to detect money laundering, as it facilitates international payments that mask the identity of the main account, the executor and country of origin. The infrastructure allows a threat actor to spread their assets through multiple accounts and this complicate tracing of the money flow.

A notable vulnerability is the lack of transparency in transactions. Bank A does not inform recipient B if the transaction goes via a payment service. There is a risk of the information on a transaction chain being lost, as the transaction passes several obliged entities who have access to different parts of the chain. Furthermore, they have limited information on the customer.

Compliance

Risk awareness in the sector varies notably between companies in the sector. Some have their own analyses and good documentation, which indicates good awareness and knowledge of the regulations. Others use generic risk analyses and process documents that do not appear to be from their own business. They are not therefore adapted to their own business and are inadequate. There are also signs that the procedures and guidelines of some obliged entities for combating money laundering are not fully implemented within the business, or are hard to implement in practice.

Because the number of payment institutions has grown considerably, there is a risk that the many newly-established companies have not achieved the same regulatory maturity of better established companies, and thus do not have the same prerequisites to detect and combat money laundering.

Experience from supervision concludes that the sector's degree of maturity with regard to compliance and risk understanding could be better. Supervision has also shown that some companies in the sector fail to comply with regulations with regard to general risk assessment, risk classification of customers, procedures for customer due diligence and monitoring. The general risk assessment performed by companies often do not differentiate risks linked to money laundering and risks linked to terrorist financing. There are several fine tech companies within the sector. They usually focus heavily on growth, digital solutions and low costs. There is therefore an inherent risk that they do not allocate sufficient resources for practical implementation of control functions and processes.

Their control systems differ considerably, which affects vulnerability to money laundering. Those that are fine tech companies usually have automated business models with few manual processes and decision-making for individual transactions. Among money transferers are agents for foreign payment institutions. Policies and IT systems for such payment institutions are often found at group level. The agent must also adapt these, but can lack sufficient knowledge of the risks and which customer due diligence procedures are necessary.

The actual payment service agent is not obliged to report, as the payment institution is obliged to report suspicion of money laundering to the FIU. Given that the payment agent is often active within the local community, they can be particularly exposed to influence from criminal actors. It is therefore not certain that the agent's knowledge of its customers comes to the attention of the payment institution.

Many agents are small and locally-based and their reporting of suspicious transactions to the payment institution is usually made by personnel with direct customer contact. Because there are customers within the sector given to violence, there is a risk that obliged entities fail to report suspicious transactions due to the fear of reprisals. Overall, this leads to vulnerability to money laundering. There are also many smaller actors in the sector who are likely dependent on repeat business.

The reporting by payment institutions to the FIU mainly concerns the customer who made the transaction. Reporting on the agent, who is partially the party that can facilitate or actively participate in criminal schemes, is less common.

Summarising assessment

Vulnerability to money laundering in the sector varies according to business types, but supervision generally indicates weaknesses in compliance with regard to general risk assessment and customer due diligence. The majority of companies only have digital business models, which means that traceability is good, but that it may also be possible for a threat actor to exploit someone else's identity, or circumvent checks in the customer due diligence processes. Institutions licenced for money transfer can be cash-intensive with international transactions, which increases vulnerability to money laundering. Some payment institutions offer their products and services via agents or collaborating company applications. It is then the payment institution that has to ensure that the agent lives up to the requirements set by the regulations for money laundering, which is not done to an adequate extent. A number of improvements have, however, been seen that help reduce vulnerability in the sector, such as changes in the law that mean it is no longer possible to grant exceptions from licencing for certain services, and the criminalisation of providing financial services without a licence or registration.

In conclusion, vulnerability to money laundering is deemed to be significant.

Risk scenario, including known approaches of terrorist financing

Money transfer via payment institutions is a common method of financing terrorism. The entire chain for terrorist financing is rare within the sector, but the vital link – getting money out of Sweden – can be provided by payment institutions. Transactions to payment institutions can be conducted via transfers, card purchase or cash.

The sector includes Hawala activities, which can also be used for terrorist financing. There are good chances of conducting transactions anonymously and to send money to conflict zones. Hawala also provides the opportunity to send money to jurisdictions subject to sanctions or that have no agents for the large payment institutions, and to war zones with poor electricity supplies and technical infrastructure.

Threat – terrorist financing

Scope

The services of the payment institutions are easily accessible, offer fast digital solutions and are represented by a large number of agents with spread over a wide geographical area. It is therefore possible to send money to a large number of countries, many of which are in war zones and other high risk areas. Because the services of the large payment institutions work similarly throughout the world, they are perceived as easily accessible when travelling between countries. They are a frequent occurrence in transaction chains with the final objective of financing terrorism.

Conducting a transaction to conflict zones and inaccessible areas can be difficult, which is where Hawala is one of the alternatives. A large part of Hawala activities run in Sweden are not deemed to be registered with the FSA and therefore not under supervision by the authorities. This makes the total scope of Hawala hard to assess. However, the Hawala network is deemed to be exploited to a large degree to provide money for the purpose of terrorist financing.

Threat actor capabilities

In common with money laundering, no special abilities are needed to use the services of the payment institutions. With Hawala, only knowledge of who is running the activity and to where money can be transferred to is required.

Anonymity

The chances of anonymity vary between and within payment institutions. False ID is sometimes used when sending or receiving money, to ensure the transaction does not reveal the true sender or recipient. Furthermore, responsibility for performing the correct ID checks lies with the local agent, which does not always perform them. The anonymity of the sender and recipient are therefore maintained to a large degree.

There are good chances of conducting transactions via Hawala anonymously, making it attractive for actors intending to finance terrorism.

Vulnerability – terrorist financing

The chances of detecting terrorist financing

The problems for the sector as described in the section on money laundering are relevant, including for issues on terrorist financing. Because payment institutions operate globally, they have a good overall view of international transaction flows and the opportunity to detect deviations in those flows, or to follow a method used for terrorist financing. This also gives payment institutions opportunities to detect parties of international significance.

With regard to money transfers via a payment institution and Hawala, the problem to a large extent is separating legal transactions to relatives and family in conflict zones or in areas with no stable payment infrastructure, from transactions intended to finance terrorism. The opportunities the large payment institutions have to see global patterns should, to some extent, make it possible to differentiate.

The opportunity to conduct transactions in cash also helps make it hard to follow money through the entire transaction chain.

Compliance

With regard to compliance, the same actual circumstances as described in the section on money laundering apply to the issue of terrorist financing. As previously mentioned, the large payment institutions have a good overview of global transaction flows. But they interpret their reporting obligation as only having to report transactions to and from the relevant jurisdictions and that they do not have to take responsibility for the full intelligence profile. This limits the chances of getting a full picture of a complete transaction chain.

7.9 Registered payment service providers, account information services

Overall sector risk:



As from 1 July 2025, the sector only comprises suppliers of account information services.⁶⁹ Prior to 1 July 2025, registered payment service providers were institutions offering payment services according to the definition in chapter 3, section 3 of the Act on Payment Services (2010:751 – LBT), but granted exceptions from mandatory licencing according to chapter 2, section 3 of the same act.

Account information services are third party services that gather and compare information with the customer's consent from the payment accounts of various banks to give a general overview of the customer's finances. They can be provided, for example, via apps or online services, normally to help customers manage their finances.

The approaches previously associated by threat and vulnerability assessments associated with the activities run by registered payment service providers are described in section 7.8 Payment institutions.

A transformed sector

The Coordination Function considered the risks of alternative payment systems being used for money laundering and terrorist financing in a national risk assessment in 2022.⁷⁰ In the risk assessment, currency exchangers and registered payment service providers such as money transferers were deemed to have a key role to play in reinvestment by criminal networks in criminal activities and the laundering of crime proceeds. The suggestion was therefore made that statutory reporting for natural and legal persons operating activities such as money transfers and currency exchange should be replaced by statutory licencing. Natural and legal persons providing payment services in the form of account information services were exempted from the proposal.

The changes were introduced to the Act on Payment Services and came into effect on 1 July 2025, and after 31 December 2025, it is no longer possible for registered payment service providers to continue their activities. All registered payment service providers who wanted to continue operating as a payment institution therefore had to apply to the FSA for a licence. The cost of an application is SEK 400,000. The obliged entities who only provide account information services were allowed to continue as registered payment service providers. They are covered by the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

The threshold for running payment service activities has been raised by the change in the law. It is important that the appropriate authorities follow developments and are aware of whether the risks associated with registered payment service providers move to the remaining parts of the payment service sector.

⁶⁹ Chapter 1, section 2(1), para. 9 of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

⁷⁰ The Swedish Police Authority/the Coordination Function, *National Risk Assessment 2022 – Hawala: value changes in the alternative payment system*. Ref. no. A243.461/2023.

Risk – money laundering

The providers of account information services do not perform any financial transactions and are therefore not deemed to be associated with any real risk of money laundering. No approaches are known.

In conclusion, the threat regarding money laundering in the sector is deemed to be low.

In conclusion, the threat regarding vulnerability to money laundering in the sector is deemed to be low.

Risk – terrorist financing

There is no known method by which the sector is used for terrorist financing in Sweden at this time. No international surveys have been conducted. The sector's risk of terrorist financing has therefore not been assessed.

7.10 Consumer credit operations

Obligated entities in the sector offer or broker loans and account credits to consumers. Since 1 July 2025, such services can only be provided by banks or credit market institutions. The Act on Certain Activities with Consumer Credit (2014:275) ceased to apply on that date. Companies who want to continue their activities with consumer credit must apply for a licence according to the Banking and Financing Business Act (2004:297) by July 2026. Until their applications have been fully processed, exemptions from statutory licencing apply to those who want to continue their activities.

The sector has not been quantitatively risk assessed as it will cease to exist. But the risks associated with consumer credit have been considered in the assessments of the sectors that will continue to provide the service.

Money laundering – description of the risk scenario including known approaches

Information from decrypted communications between criminal actors clearly shows the need to introduce money from crime into the legal system through various forms of credit schemes. They include embezzlement and money laundering through loans granted on false grounds. A threat actor can, for example, get an unsecured loan paid into their account. The loan can have been granted on false grounds, for example, through incorrect personal details. The money disbursed can then be used for such things as buying large capital goods or for other types of investment. The money can also be moved to other bank accounts, including abroad, via so-called layering, which can be considered as money laundering as the amount loaned has been acquired on false grounds. By then amortising the loan using money from other criminal activities, such as drugs-related crime, another step is completed in the money laundering scheme. The lender or a third party can amortise the loan. Individual payments from persons other than the lender can be involved, or the loan can be paid off completely through deposits made by someone else. Lenders have also been known to deviate from the expected amortisation plan and make sporadic extra instalment payments. In all the above, the loan is paid off with money from criminal activities.

Lending with the help of a straw men

Loans can be taken out by other lenders than the criminal actors themselves, for example, using straw men. The funds disbursed can be transferred to the criminal actor's account, or to another straw man's account controlled by the criminal actor. In such instances, amortisation and repayment are made by the criminal actor transferring the proceeds from crime to the lender, who then makes payments to the credit provider. There are also examples of payments being made by other people completely, who do not have any apparent connection to the lender.

Facilitators and professional money launderers are used

Loans can be taken out in parallel with several credit providers to increase the total amount (which are thus amortised for money laundering). The individual amounts laundered are thus relatively small and the various credit providers gain no overall picture of the extent of the scheme. Loan documents from the credit institutions can also be used to provide apparent legitimacy for transactions when the money itself originates from crime. Employees within credit institutions have been known to associate with criminal actors within organised crime. Information indicates that such employees facilitate schemes for money laundering or fraud. Granting loans and high lending ceilings on false grounds can be involved.

Many small and quick transactions

Certain consumer credits linked to payment services or virtual cards can be used to quickly transfer money between different accounts, and thus circumvent traditional controls. By using credit via virtual cards or digital payment solutions (such as Swish), criminal actors can make fast, small transfers that can total large amounts.

Consumer credit to finance car purchases

Some types of consumer credit can be used to finance car purchases, with the car used as security for the loan. A majority of credit institutions that offer such loans have collaborative agreements or partnerships with car dealers. The buyer can be offered financing direct from the credit institution at the time of purchase. A wide range of criminal schemes can be facilitated through such financing:

- Car dealers over-value cars to be able to increase the amount of credit disbursed by the credit institution. This in turn means that larger amounts can be laundered through the criminal actor amortising the loan.
- Criminal actors finance car purchases using credit they apply for via a car dealer. The cash deposit for the car is paid directly to the car dealer. Normally, that payment must comprise at least 20% of the car's value. Criminal actors can pay the deposit with crime proceeds. Cash payments of more than 20% have also been known. This in turn allows criminal actors to launder money through continuing to amortise the rest of the credit amount.
- The same car is financed through loans several times. This means that larger amounts can be laundered through amortising the loan.
- The officers of the car company participate in fraud given that cars are sold to straw men who finance them through credit. The straw men have no intention of repaying the loan before leaving the country. The car is sold abroad by the car company which then gains another income. The straw men are paid an amount by the car company for their participation in the crime. The credit company makes a loss.

Illegal funds for legitimate incomes

Credit can be used to start or finance a company which is then used to convert illegal funds into legitimate income. By starting small companies and use credits to run the company, criminal actors can create a facade of legitimate income.

Risk scenario, including known approaches of terrorist financing

Consumer credit can be abused for financing terrorism. Because it is possible to lend from various credit providers, the amount can be large in comparison to the low transaction amounts otherwise involved in terrorist financing. Different procedures are used when applying for credit. Some take one or a few large credits, some take a large number of small credits and stay under the ceilings set to avoid enhanced checks by obliged entities. The money can then be sent abroad, often via a payment institution or payment provider to finance terrorism. By making one or a few amortisations, regardless of whether it is the lender or others that does so, the risk of detection is reduced.

Consumer credit has also been taken out in the name of themselves or relatives to finance travel to countries in or near conflict zones, in some cases to join terror organisations in the area with no intention of returning to Sweden. This procedure can also be used by "lone wolf" terrorists for planning attacks, for example.

Credit cards are also used, sometimes via direct applications or linked to a credit purchase of goods when a higher credit limit than the value of the goods is given. This makes it possible to make card payments to, for example, payment institutions and to make cash withdrawals in Sweden or abroad, to be used for financing terrorism. Amortisations made by others than the credit-taker are also known for the use of credit cards.

7.11 Mortgage lending business

Overall sector risk:



Activities involving mortgage lending entail the commercial provision of consumer credit, credit brokerage and advice for questions on housing credit issues.⁷¹

General description of the sector and related products or activities

The Swedish Housing Credit Activities Act (2016:1024)⁷² and others apply to so-called mortgage lending institutions running commercial activities with credit provision, brokerage and advice on mortgage lending issues and bridging loans to consumers. This sector can be broadly divided into two categories of companies: those that provide consumer loans for buying a home, and the so-called housing loan brokers⁷³. The sector mainly comprises smaller actors on the Swedish housing loan market and not credit institutions and banks.

When a consumer applies for a new home loan or to move an existing home loan, it is usually done via the company's own sales channels or those of a collaborative partner online. The companies finance their lending in different ways. They can set up home loan funds or similar structures in which financing is provided by investors outside the banking sector, such as insurance companies or pension funds.

Home loan brokers provide a service in which the consumer's application for a home loan is brokered to several home loan companies. The consumer can then choose among the credit providers that granted the consumer a loan, and the broker gets commission from the credit provider.

Key figures	
Number of companies	9
Number of employees	587
Number of business connections established	619 909
Company balance sheet total	7 025 233 562
Company turnover	1 463 916 894
Total number of physical customers	302 134
Total number of legal customers	1 033

Source: The FSA's periodic reports on money laundering, reference date 31.12.2024. The details are based on the reports of the institutions to the FSA and the table can, therefore, include data which deviates to some extent from the actual situation.

⁷¹ Chapter 1, section 2(1), para. 11 of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

⁷² Chapter 1, section 1 of the Housing Credit Activities Act (2016:1024). See also chapter 1, section 2 of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

⁷³ See chapter 1, section 6 of the Housing Credit Activities Act (2016:1024) and section 48 of the Consumer Credit Act (2010:1846).

Money laundering – description of the risk scenario including known approaches

Threat actors can conceal and invest earnings from crime through property investments. Earnings from crime are used for deposits, repayments or early repayment of the assets.

Money laundering through false documentation and home loans

Criminal schemes involving home loans and documentation can involve people with such low incomes that they would not normally be regarded as being sufficiently creditworthy to be granted a home loan. Such applicants falsely claim in their applications that they have started a new, full-time job in the current year and provide false employer documentation as proof. In such instances, the companies involved can be exploited by offering creditworthiness to people working black or in some criminal activity. In many instances, the lenders have a relatively weak connection to Sweden. Companies cited as employers are few and many lenders claim they work for the same company. In most instances, a home is also acquired after a loan has been granted. Interest payments and amortisations are often made without comment, but are paid from criminal proceeds.

Facilitators and professional money launderers

Employees of home loan institutions can act as facilitators by granting home loans to criminal actors on false grounds, which can also involve them accepting bribes. This procedure is often linked to a money laundering scheme, as the loan is repaid from criminal proceeds. An over-valuation of the home can also be made, and the home loan can be used as a method of legitimising higher turnover of money than that actually required for the purchase.

Threats – money laundering

Scope

A scheme involving home loan credits is generally deemed to be attractive for money laundering. As there are few companies in the sector, their turnover in relation to total lending for homes is low, and because most are engaged in brokering loans and not credit provision, it is hard to assess how exposed the sector is to money laundering. The following description of threats and vulnerabilities therefore concerns home loan credits in general.

Money laundering via property in Sweden involves large amounts, and can take place in all sectors offering this type of product. The transactions in SAR reports related to property comprised over SEK 5 billion in 2022.⁷⁴ The number of SARs from the sector to the FIU continues to be low, there were eight in 2024 and twelve in 2020. There can be an undisclosed number, given that complex schemes are involved. The intelligence from the FIU also indicates that the problem can be more widespread than indicated by reporting.

Threat actor capabilities

Exploiting home loan credit for money laundering requires a well-organised economy or enough knowledge to understand the product. Some approaches require the threat actor to also produce complex and false documentation, which often involves organised crime. Third parties (frontmen) can also be involved in the scheme.

When a threat actor comprises facilitators at a home loan institution or bank that grant loans for example to criminal actors on false grounds, the threat actor is deemed to be highly capable.

Anonymity

The chances of being anonymous when using home loan credits are very limited.

⁷⁴ Swedish Police Authority (2024) *Professional money launderers – Sectors, approaches and links to criminal networks*. Ref. no. A154.174/2024.

Summarising assessment

The services offered within home loan credits are generally deemed to be attractive for money laundering. Assessments made in other sectors with similar products show that risks include false loan applications, the use of complex financial structures, identity fraud and repayments made using illegal funds, which complicate the traceability of the source of the money. In conclusion, the products within home loan credits are deemed to be attractive for money laundering.

In conclusion, the threat regarding money laundering in the sector is deemed to be high.

Vulnerability – money laundering

The chances of detecting money laundering

The sector is only aimed at private customers and only mainly gives loans for the purchase of Swedish homes, but international transfers of funds also occur. The obliged entities within the sector are web-based, which makes it harder to discern whether false or stolen identities are used, for example.

Various types of obliged entities are involved, including in several countries, which means that money laundering schemes can be hard to detect. Obligated entities in the sector only see a limited part of their customers' private finances and transactions, which means it can be hard to get a full overview.

Compliance

Obligated entities in the sector are generally deemed to be aware of the risks of money laundering. Traceability within the sector is deemed to be high, as turnover rate for transactions is regarded as low.

Summarising assessment

Home loans involve several types of obliged entities, which implies a risk of the necessary checks falling between two stools. The lack of an overview of customer transactions and engagement can represent a problem for the obliged entities to detect suspected money laundering.

In conclusion, the vulnerability to money laundering in the sector is deemed to be significant.

Risk – terrorist financing

There is no known method by which the sector is used for terrorist financing in Sweden at this time. No international surveys have been conducted. The sector's risk of terrorist financing has therefore not been assessed.

7.12 Crowdfunding services

Overall sector risk:



Providers of crowdfunding services provide platforms to bring together project owners seeking financing from investors. Suppliers of crowdfunding services thus provide a brokerage service.

Since 10 November 2021, the Crowdfunding Regulation⁷⁵ and its supplementary provisions⁷⁶ has been in effect. In conjunction with it coming into effect, a supplement was made to the Anti-Money Laundering Act⁷⁷ and providers of crowdfunding services became obliged entities as defined in the act. The supplement concerns legal persons established in Sweden with activities as defined by the Crowdfunding Regulation. Providers of crowdfunding services are defined as companies providing a platform on which project owners and investors can meet for the purpose of alternative financing for small and medium-sized companies. Risk assessment of the sector is based on the definition made in the regulation regarding the term "providers of crowdfunding services".

General description of the sector and related products or activities

The sector is small in Sweden and only involves a few companies. Crowdfunding is used as a form of alternative financing for startups as well as small and medium-sized companies, which usually rely on small investments. It represents a type of brokerage services via which a provider of crowdfunding services – at no risk to itself – runs a digital platform that is open to the general public to match, or support the matching of, potential investors or lenders with companies seeking funding. This form of funding can be in the form of loans or acquisition of negotiable securities, or other authorised instruments for crowdfunding.

Crowdfunding is regarded by the European supervisory authorities as a form of capital acquisition from the general public for a specific project via the internet, by such means as:

- Detection of debtors. Loan-based funding entails financiers acting as lenders and expecting to earn interest on their money. This category is subject to licencing according to the Crowdfunding Regulation.
- Issuing debt instruments. Share-based crowdfunding makes it possible for investors to buy shares in a company in return for shares in that company. This category is subject to licencing according to the Crowdfunding Regulation.

⁷⁵ Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937.

⁷⁶ Act with Additional Provisions to the EU Crowdfunding Regulation (2021:899).

⁷⁷ Chapter 1, section 2(1), para. 12 of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

Key figures	
Number of companies	4
Number of employees	28
Number of business connections established	7 904
Company balance sheet total	42 070 915
Company turnover	42 435 291
Total number of physical customers	13 751
Total number of legal customers	2 018

Source: The FSA's periodic reports on money laundering, reference date 31.12.2024. The details are based on the reports of the institutions to the FSA and the table can, therefore, include data which deviates to some extent from the actual situation.

Money laundering – description of the risk scenario including known approaches

Description of the risk and approaches is based on intelligence. Because crowdfunding according to the Crowdfunding Regulation is mainly used by small and medium-sized companies, it is likely that mainly unlisted companies use the services. These are regarded as having relatively low transparency compared to listed companies. This opens up the opportunity for telling a false story with regard to investment in such a company. Crowdfunding can therefore represent a channel for fraudsters to give misleading information and risks making the brokerage service vulnerable to fraud and money laundering.

Crowdfunding services can also be vulnerable to exploitation for money laundering through project owners to create fictitious or exaggerated projects on platforms for crowdfunding as a cover for channelling and legitimising illegal funds. This can be done through investors collaborating with a project owner and "investing" money in a project that is then withdrawn or "fails" in a manner that makes it hard to track the source of the funds. It should also be noted that a platform offering crowdfunding risks being exploited for money laundering as it is either a payment service provider itself or collaborates with one to be able to execute payments. This can allow criminals to move illegal funds between different jurisdictions without being detected.

Fraud and tax crimes through crowdfunding

Crowdfunding can also be exploited to commit fraud. Examples include companies that finance property projects through crowdfunding where persons have been tricked into investing in something that does not exist. The problem is amplified if such companies do not use an approved or authorised auditor, which is possible as it is no longer a requirement for all limited companies. This implies that external insight and investigation of the project and the transactions related to it can be missing.

Crowdfunding can also be exploited for tax crime when company profits are sent to the provider of crowdfunding services under the pretence that they will be invested in a project when the money is diverted to a private person. The money is actually earnings but is disguised as dividends or the like from the supplier of the crowdfunding service.

Facilitators for criminal networks

Criminal networks can exploit crowdfunding services in money laundering schemes if the network has a facilitator at the provider of the services who guarantees financing to the company the network controls. A possible scenario could also be that the actual supplier of crowdfunding services is controlled by criminal actors.

Examples of such approaches:

Criminal network A transfers money from criminal proceeds to the provider of the crowdfunding service where the network has a facilitator. Large amounts are concerned and the transfers can be made from foreign bank accounts. Two companies controlled by network A apply for, and get, financing from the provider of the crowdfunding service. The laundered money is used to build property, which also generates an increase in value when sold. The laundered money is also used pay for labour.

Threats – money laundering

Scope

The sector is very small with only a few relatively well-established companies, which makes it hard to assess how exposed it is to money laundering. But it is believed that schemes involving crowdfunding are generally attractive various forms of fraud and money laundering. The following description of threats and vulnerabilities therefore concerns products and services generally associated with the sector.

Threat actor capabilities

In the same way as threat actors are increasing their technical skills regarding cryptoassets, among other things, the skills required for crowdfunding platforms are also deemed to be on the increase. As described earlier, criminal networks could be able to exploit crowdfunding services for money laundering. This can be done either through a facilitator at the provider of the services who guarantees financing to the company the network controls, or through criminal actors controlling the provider of crowdfunding services. Such money laundering schemes require a certain level of capability of the threat actor.

Anonymity

Because the sector is relatively new, there is a risk that there is insufficient experience and understanding of the regulation and the context. This makes it possible for threat actors to remain anonymous by exploiting the identities of others. The fact that payments can be made via payment services makes detecting suspected transactions and behaviour difficult. Providers of crowdfunding services can also have few opportunities to identify financiers, which can also contribute to those difficulties.

Summarising assessment

The sector comprises only a few companies, but they, in their turn, have a large number of business associates. The awareness of threat actors of platforms for crowdfunding services is expected to grow.

In conclusion, the threat regarding money laundering in the sector is deemed to be significant.

Vulnerability – money laundering

The chances of detecting money laundering

Because the sector is relatively new, there is a risk that there is insufficient accumulated experience and understanding of the regulation and the context. This means that there can be a built-in vulnerability that reduces the chances of detecting money laundering. Providers of crowdfunding services can also have few opportunities to identify financiers, which makes it possible for criminals to exploit the services to give their proceeds of crime an apparently legitimate source.

Compliance

The providers of crowdfunding can be less aware of the law in effect, especially if run by small and newly-established actors. This can lead to the provisions of the AML regulations not being complied with in full, including with regard to general risk assessment, customer classification, customer due diligence and transaction monitoring.

Summarising assessment

Given that the companies are relatively newly-established, the sector can have a lower regulatory maturity, which could lead to problems with compliance with the AML regulations.

In conclusion, the vulnerability to money laundering in the sector is deemed to be significant.

Risk scenarios, including known approaches of terrorist financing

Many countries do not have adequate regulation and collaboration to be able to manage the risks of crowdfunding. This makes terrorists can exploit the differences between different transactions and use international crowdfunding platforms to finance terrorism.

Terrorist groups and violent extremists use social media and encrypted messaging apps to spread donation campaigns and recruit followers. By sharing links to crowdfunding platforms or giving direct payment instructions, terrorist groups and violent extremists can reach a global public.

Threat – terrorist financing

Scope

Given the low number of crowdfunding platforms found on the Swedish market, and the fact that the sector did not exist as a natural part of the Swedish financial landscape until recently, the scope of terrorist financing through these platforms is deemed to be low.

Threat actor capabilities

In the same way as threat actors are increasing their technical skills regarding cryptoassets, among other things, their knowledge of crowdfunding platforms is also deemed to be on the increase. However, the sector is not deemed to be prioritised for use with terrorist financing yet, and the ability to do so within the sector is deemed to be low.

Anonymity

No other assessment than that made for money laundering is made on the issue of anonymity in the present field.

Vulnerability – terrorist financing

The chances of detecting terrorist financing and regulatory compliance

The same assessment made as for money laundering is made in the issue of terrorist financing.

7.13 Cryptoasset service providers

Overall sector risk:



Cryptoasset service providers are legal persons whose employment or business consists of professional provision of cryptoasset services to customers.⁷⁸

General description of the sector and related products or activities

Cryptoasset service providers have been regulated through the MiCA regulation (Markets in Crypto-Assets Regulation) since 30 December 2024. Only legal persons run the activity according to MiCA and the companies are obliged entities in the meaning of the AML act.

The MiCA regulation is intended to establish a uniform and harmonised regulation for cryptoassets within the EU. The regulation includes a new expansion of the definition of cryptoasset service providers (CASPs). Cryptoasset service providers are also covered by the EU Transfer of Funds Regulation (TFR) in Sweden. TFR regulates the kinds of information on sender and recipient that must accompany transfers of funds to avoid such transactions being conducted anonymously. The EU regulations create the prerequisites for cryptoasset activities to be controlled.

To run such activities as a cryptoasset service provider requires a licence from the FSA. According to MiCA, certain institutions do not need to apply for a new licence if they already have one that covers similar services. For example, if a bank wants to start offering cryptoasset services, simply informing the FSA will be sufficient. A cryptoasset service is defined as some of the following services and activities regarding some cryptoassets:

- a) provision of the safeguarding and administration of cryptoassets at the customers' expense.
- b) operating a trading platform for cryptoassets
- c) exchange of cryptoassets for money
- d) exchange of cryptoassets for other cryptoassets
- e) execution of orders regarding cryptoassets at the customers' expense.
- f) placing of cryptoassets
- g) receiving and transferring orders regarding cryptoassets at the customers' expense.
- h) provision of consultancy on cryptoassets
- i) provision of portfolio management of cryptoassets
- j) provision of the transfer services for cryptoassets at the customers' expense.

⁷⁸ Chapter 1, section 2(1), para. 13 of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

Transformed sector

Cryptoasset service providers have been subject to the MiCA regulation since 30 December 2024. Companies that were previously registered with the FSA according to the Act on Currency Exchange and Other Financial Activities had to apply for authorisation according to MiCA during a transition period to 30 September 2025. These companies came under the sector of currency exchangers and other financial activities in the previous sector risk assessments, but have now been classed in their own sector once the EU regulation on markets for cryptoassets came into effect.

Because the sector was first defined in 2025, it has not been possible to report exact key figures for 2024.

Money laundering – description of the risk scenario including known approaches

Cryptoassets are being used to a much greater degree in the context of money laundering.⁷⁹ A large number of cryptoasset exchangers are illegal actors operating without the necessary permit, or legal, foreign companies offering their services to persons in Sweden. The following descriptions concern legal cryptoasset service providers that are Swedish companies. The approaches described are not exhaustive.

Large scale exchange of cash to cryptoassets is, for example, intended to divert criminal proceeds abroad. Apart from cryptoassets being used as a means of laundering money, they are used by criminals to invest in new crimes and as a means of payment for various criminal services. Cryptoassets are commonly used, for example, within online drugs trading, in certain types of fraud, extortion and cybercrime.

The proceeds from all types of criminality can be laundered using cryptoassets. Money laundering can be conducted through fiat currencies⁸⁰ in digital form exchanged for cryptoassets and then layered, i.e. cash or other assets are exchanged for cryptoassets or cryptoassets come direct from the crime to then be laundered.

Simple money laundering schemes can consist of transfers between wallets and exchange on trading platforms or between private individuals. More advanced money laundering includes steps such as exchange between different cryptoassets, mixers⁸¹, the use of gambling platforms, purchase of goods and gift vouchers, non-fungible tokens (NFT)⁸² and decentralised finance platforms (DeFi). New tools and approaches to conceal tracking continue to be created and refined.

There are different types of fraud with cryptoassets, something that comprises a predicate offence to money laundering. Examples include investment fraud, pyramid trading or "pump-and-dump". Criminal actors use "pump-and-dump" to manipulate the value of newly-created or existing small cryptoassets through inflated transactions and liquidity spoofing. The cryptoassets are then used to launder money through quick purchases and sales.

The use of so-called stablecoins has increased in money laundering schemes. Stablecoins are a type of cryptoassets expected to maintain a stable value over time, for example, through them following the price of a national currency. The increased use is due to such factors as actors want to ensure that fluctuations in cryptoasset values mean that criminal proceeds lose value. Stablecoins, in common with cryptoassets in general, can be used to conceal money from the authorities and to pay for black labour.

⁷⁹ Europol (2025), *European Union Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime*, Publications Office of the European Union, Luxembourg.

⁸⁰ "Fiat currencies" are traditional currencies issued by a central bank, such as Swedish kronor or US dollars.

⁸¹ "Mixers" or "tumblers" are services designed to merge and mix cryptoassets from multiple users in a wallet, to then pay out the cryptoassets minus a fee to one or more other addresses than the original. The objective is to conceal the link between the input and output addresses.

⁸² NFTs can be associated with a certain digital or physical asset or a licence given a unique digital fingerprint. An NFT is a unit of data saved on a block chain and that can be sold or transferred. NFTs thus act as proof of ownership for a unique object. An NFT can, for example, be used for digital art, images or collectables, music or videos and to represent material assets such as proof of ownership to property.

Threats – money laundering

Scope

Several international sources indicate increased use of cryptoassets in a criminal context, not least for the purpose of laundering money.⁸³ The rapid technological development and growing social acceptance of cryptoassets have created new opportunities for laundering money. An increase in the number of individuals learning about and understanding the products and services means that demand for cryptoassets for money laundering is likely to increase further. A large part of that demand is likely met by PMLs, who offer illegal crypto exchange (see chapter 5, General risks), but money laundering also occurs within the regulated sector. For example, illegal exchangers can, in turn, use legal crypto platforms for their transactions.

Threat actor capabilities

The use of cryptoassets is generally usually higher up in the criminal network hierarchy, regardless of type of crime. Threat actors have developed the ability to use cryptoassets to conceal transactions and finance illegal activities.

Anonymity

Cryptoassets are often linked to the opportunity to remain anonymous. For each new transaction, a new block is created in a block chain, and new information is saved in the chain. It implies that the block chain grows and that all transactions are visible in it. The transaction is not strictly speaking anonymous, in common with cash, the transfer leaves a lasting track in the block chain. Each transaction has a history of where the asset came from and where it goes. On the other hand, the owner of an address is unknown to the general public, which means there is a question of pseudoanonymity.

The MiCA regulation gives a certain prohibition against the provision of anonymous cryptoassets, known as "privacy coins", which is why many regulated platforms no longer permit them. Privacy coins are designed to give a higher degree of anonymity, which means it is hard to trace the transactions and makes them attractive to use for money laundering. Even if cryptoasset service providers in the EU do not provide anonymous cryptoassets, privacy coins are often part of a money laundering chain which has links outside the EU.

Summarising assessment

Cryptoassets are pseudoanonymous, easily accessible and internationally viable. That means they are in demand for laundering criminal proceeds. The ability of criminal actors to use cryptoassets is deemed to have increased successively in recent years, and created an even greater demand for criminal purposes.

In conclusion, the threat regarding money laundering in the sector is deemed to be high.

Vulnerability – money laundering

The chances of detecting money laundering

The integration of cryptoassets in the traditional finance system via quick, digital financial services offered by certain actors on the finance market, can lead to criminal actors being able to use those companies to transform cryptoassets into fiat currencies or vice versa, which facilitates faster and difficult to trace transactions.

Transactions with cryptoassets are subject to international regulations. There is also an inherent pseudoanonymity in transactions of this type, as the sender and recipient are anonymous even if the transaction can be traced. Transactions with cryptoassets can be conducted quickly, which increases the vulnerability to money laundering in the sector.

The technological developments and growth of more advanced functions has forced a change towards more anonymised cryptoassets. This, in common with the use of decentralised platforms, makes it harder to detect and trace transactions, which, in turn, makes it harder to detect and investigate money

⁸³ See for example, Europol (2025), *European Union Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime*, Publications Office of the European Union, Luxembourg.

laundering. Traditional monitoring methods are often inadequate to deal with these new technologies. Special tools, such as block chain analysis, have been developed to facilitate tracing cryptotransactions, and to identify suspected activity.

To deal in cryptoassets usually requires that, in some instances, there is an exchange from fiat currency to a cryptoasset. The same applies when someone wants to convert a cryptoasset to a fiat currency. In the event of certain predicate offences, for example drug sales, it is possible that the crime is committed with the help of cryptoassets, which implies that the value can be transferred from one party to another without the use of traditional financial services. This in turn limits insight into the transaction. It is therefore only when exchanging between fiat currencies and cryptoassets that it becomes possible to learn anything about the content of cryptoassets. Companies that provide such services are therefore key to the ability of criminals to transact and conceal criminal proceeds, as they act as a bridge between the ecosystem for cryptoassets and the traditional financial system. This makes companies especially vulnerable to being exploited by criminal actors.

Compliance

The introduction of MiCA marks a major change in the regulation of the cryptoasset sector within the EU. For Swedish actors, it means that they are no longer only subject to the AML regulations, but must also comply with requirements for consumer protection, transparency and operating standards. The requirements include obligations to provide detailed information to consumers, set up safety measures and to follow specific guidelines for marketing and information provision.

This enhanced regulation is expected to lead to greater transparency within the sector and to improved regulatory compliance among the actors. By introducing harmonised rules at EU level, a more predictable market is created for consumers, and it becomes harder for shady actors to operate. This can in turn contribute to strengthening trust in the cryptoasset market.

Despite the introduction of new regulations to combat money laundering within the crypto sector, there are still problems with regulatory compliance. The decentralised global trade with cryptoassets makes it hard to ensure uniform compliance within the entire sector, which opens up opportunities for circumventing the regulations and using cryptoassets for illegal purposes. A general vulnerability that will likely increase is continued movement towards peer-to-peer transactions (purchase and sale directly between users with no centralised intermediary) and decentralised platforms, which is not addressed by the TFR regulation (see chapter 5, General risks).

Inadequate customer due diligence procedures practiced by crypto actors are exploited. Some actors within the finance market offering digital financial services and with less strict checks can permit criminals to open an account with false or stolen identities to conduct transactions related to money laundering.

Summarising assessment

The decentralised and global trade in cryptoassets makes it hard to ensure that cryptoassets are not used for illegal purposes. Experience shows that the customer due diligence processes and control systems found in the sector can be circumvented to conduct transactions in cryptoassets as part of money laundering.

In conclusion, the vulnerability to money laundering in the sector is deemed to be significant.

Risk scenario, including known approaches of terrorist financing

There have been occurrences of obliged entities offering trading in cryptoassets being exploited to finance terrorism, and both legitimate Swedish and foreign cryptoasset service providers and unregistered actors are active in this context.

Trading in cryptoassets can be part of a transaction chain with the aim of financing terrorism. They can also concern transactions made directly to cryptoaddresses controlled by terror organisations or individuals connected to them. Requests to conduct transactions in cryptoassets directly to terror-related organisations or individuals are often made on social media, and can therefore have global reach.

Threat – terrorist financing

Scope

In line with services for trading in cryptoassets becoming much more accessible and easy to use, the scope of trading is deemed to have increased, also linked to terrorist financing. Given that cryptoassets are global and digital, fast international transactions are possible.

Threat actor capabilities

To trade in cryptoassets requires that users are familiar with using digital services and have some knowledge of the phenomenon.

Anonymity

Regarding anonymity in this sector, the same factors as for money laundering are decisive for terrorist financing.

Vulnerability – terrorist financing

The chances of detecting terrorist financing

When it comes to trading in cryptoassets, there are certain possibilities of traceability if analysis at several points along the chain is possible. The obliged entity can gain a unique overview of the entire transaction chain, in contrast to, for example, traditional banks who have to take into account confidentiality. If the use of untraceable cryptoassets increases, it will be likely that the possibilities of detecting and investigating transactions that can be part of terrorist financing will diminish.

Compliance

Concerning compliance when it comes to terrorist financing, no assessment has been made other than that for money laundering.

7.14 Registered estate agents and estate agencies

Overall sector risk:



The sector encompasses the activities of registered estate agents and estate agencies.⁸⁴ Estate agents provide services such as brokerage, documentation and valuation.

General description of the sector and related products or activities

"Estate agents" are defined as natural persons running professional brokerage of properties. Brokerage involves them in funding and bringing together two parties. Estate agents also provide services such as valuation and documentation. Estate agents and estate agencies have to be registered with the Swedish Estate Agents Inspectorate. Lawyers and certain types of housing rental agency are exempted from the registration requirement, even if deemed to be professional brokerage. The exception for housing rental agencies concerns the brokerage of leasing rights with a monthly rent of less than eur 10,000 and if there is a question of municipal brokerage or leasing rights for leisure purposes. "Estate agencies" are defined as legal persons in which one or more estate agents run professional brokerage of properties. Individual firms, legal firms and certain types of companies within rental agency are exempted from the registration requirement.⁸⁵

The actual title of estate agent is not protected in law. That means that anyone can call themselves an estate agent with no requirement for registration with the Estate Agents Inspectorate.⁸⁶ But to actually practice estate agency according to the Estate Agents Act requires registration.⁸⁷ There are actors who broker objects without registration despite being subject to the obligation to register. Unlicensed estate agency is regulated in the Estate Agents Act and can result in fines or prison for up to six months.⁸⁸

The provisions concerning the activities of estate agents are regulated in the Estate Agents Act. Since the last sector-based risk assessment, a new Estate Agents Act (2021:516) has come into effect. The new act means that estate agencies are now subject to the registration requirements, supervision by the Estate Agents Inspectorate and the AML regulations. The introduction of the new act has allocated responsibility regarding obligations under the AML regulations between the estate agents and estate agencies.⁸⁹ Estate agencies with estate agents employed are responsible for the general risk assessment of how the business could be used for money laundering or terrorist financing, along with procedures and guidelines regarding measures for customer due diligence, monitoring, reporting and for processing personal data. Estate agents are responsible for customer due diligence in individual cases. The new act divides the registration category of rental agencies between registration for rental brokerage and special registration for rental brokerage. Registration for rental brokerage mainly concerns brokering contracts for rental properties and space with a monthly rent under eur 10,000. Special registration is required when monthly rent is at least eur 10,000, which usually concerns commercial premises or company sales in which such premises are included. Estate agents registered in the category of special estate agency are also subject to the AML regulations.

⁸⁴ Chapter 1, section 2(1), para. 14 of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

⁸⁵ Chapter 2, section 2, Estate Agents Act (2021:516).

⁸⁶ Magnus Merlin, the Estate Agents Act. A comment, p. 61, published 06.01.2025 (the author and Nordstedts Juridik AB).

⁸⁷ Chapter 1, section 2, para. 1 and 2, chapter 1, section 1, Estate Agents Act (2021:516).

⁸⁸ Chapter 4, section 18, Estate Agents Act (2021:516).

⁸⁹ Chapter 4, section 1, Estate Agents Act (2021:516), chapter 1, section 2, para. 14 and chapter 2, section 16, the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

An estate agent must discharge their duties responsibly and always observe best practices. The agent must represent the buyer and the seller's interests and act as an impartial intermediary. Within the framework of the requirements that best practices apply, the agent must especially safeguard their client's (usually the seller) financial interests.⁹⁰ Best estate agency practice includes an agent being obliged to comply with any other applicable legislation.

Apart from the more traditional services, some agents provide a simplified service for documentation, which becomes relevant in cases when buyer and seller are already in contact with each other and agreed the terms of a sale. Documentation mainly involves the estate agent completing the necessary documents for the sale, such as transfer of deed. Estate agents can sometimes produce documentation for an object, as it is often required by the banks. Documentation is a quick process in which the agent does not need any marketing skills.

Key figures	
Number of registered estate agents	7 529 ¹
Number of registered estate agencies	2 257 ²
Sales value (home market)	SEK 543 bill. ³
Industry turnover	over SEK 9.7 bill. ⁴

¹ Estate Agents Inspectorate's register of estate agents, 31.12.2024.
² Estate Agents Inspectorate's register of estate agents, 31.12.2024.
³ Based on data from Svensk Mäklarstatistik (Swedish estate agent statistics).
⁴ According to data from UC. The total industry earnings in 2024 comprised about SEK 9.7 billion (SEK 9,723,975,000). That is an increase of around 15.4% compared with 2023. The data come from UC and should be regarded more as an indication than an exact figure. The reason is that there can be companies in UC's statistics that do not run home brokerage on the private market. Neither are UC's figures complete, which means it cannot be presumed that companies in the franchise structures are included in full in the statistics.

Estate agents are obliged to hold money and other assets separate from their own.⁹¹ They do so by using trust accounts. Their trust accounts are mainly used depositing down payments paid by the buyers when buying a property or transferring deeds handled by the agent. It is common for agents to handle down payments by depositing them in their trust accounts.

Money laundering – description of the risk scenario including known approaches

Money laundering in the estate agency sector is deemed to be large scale, as transactions in property can generally reach very large amounts. There are a number of approaches in which estate agents can participate in money laundering. They concern situations in which the agent is either unaware of money laundering being involved, is aware of but chooses to ignore it, or is directly involved and acts as facilitator such as a PMLs in a criminal scheme.

Professional money launderers

Examples are found in intelligence and investigation of PMLs in the estate agency industry recruited by, or in some other way collaborating with criminal networks, mainly local networks with considerable influence on the local community. There are estate agents who are relevant in money laundering aspects who are related to leading actors in criminal networks. To follow is an anonymised example of links between a PML and a criminal network.

90 Chapter 3, section 1, Estate Agents Act (2021:516).
91 Chapter 3, section 4(2), Estate Agents Act (2021:516).

Estate agent H has been laundering money for network criminals for some time through his agency H-hus AB. H also has links to a foreign estate agency. H-hus AB provides false purchase contracts that criminals can use for bank transactions. Via the foreign estate agency, properties can be bought for cash, and then sold again. Very expensive objects are involved. H has statements of account privately and through his agency that belong to members of a criminal network with organisational skills and that is known to be violent, without any reasonable explanation.

Trust accounts used as fronts for crime

Trust accounts are intended to hold down payments until all terms and conditions are fulfilled and the purchase becomes binding. Using their trust accounts, estate agents can act as an intermediary, for example when Swedish banks will not receive a deposit payment from abroad in the seller's account with regard to the risk of money laundering. In such instances, the estate agent will receive the money in its trust account instead, and in turn will transfer the money to the seller. Trust accounts can also be used to funnel money to legitimise the transactions or conceal its source. Down payments already received have also been refunded to the same account or a different account to that they came from. A so-called better fortune clause can also be used, which involves including a clause in the sales contract which invalidates the purchase if the terms of the clause are not met.

Fabricated contract or awareness of over or under-valuation

A fabricated contract for a property purchase is used as documentation for the banks to allow transactions or legitimise the source of the money. Money laundering also occurs through an estate agent knowingly over or under-valuing a property. In the event of over-valuation, the owner can take out a bigger loan, which is then amortised with money from criminal activities. In the event of undervaluation, the buyer can compensate the seller with a cash payment alongside the official transaction.

Property bought with the help of frontmen

There are several reasons for using a straw man or front man in connection with money laundering via a property purchase. Someone who has bought a home moves in or is registered as a resident of the new address before the home is sold again.

Another situation when a straw man facilitates money laundering is when a buyer wants to conceal the source of the money and therefore is not named on the deeds of the property, for example for circumventing financial sanctions from countries subject to restrictions.

A straw man can also be used when money needs to be laundered via the renovation of a property before selling it on, often in combination with over or under-valuation. The renovations are financed using criminal proceeds.

Estate agents give legitimacy to property transactions

The documentation service increases the risk of an estate agent being exploited as part of money laundering. Without even having visited a property or met either the buyer or seller, the estate agent risks being party to money laundering in connection with an object description, valuation or a handover agreement being produced.

The document from the estate agent risks in turn contributing to false legitimacy and reassurance given to, for example, an intended lender who depends on the agent's information. The service risks being exploited as part of money laundering when it is a discrete service with limited insight that does not need to be marketed. The estate agent's own checks according to the AML legislation are ignored extensively in this type of scheme. The estate agents usually has less contact with the parties as the relationship is often quite short and the scheme is not as extensive as a regular brokerage job. In a situation when the threat actor has contacts with various facilitators at various credit providers, it is easy to produce the documents needed for the facilitator to be able to approve, recommend or grant a housing loan. The estate agent provides apparent legitimacy and can produce the data an official at a credit provider will not usually query and can approve. Criminal actors and networks systematically use facilitators from various companies and industries to acquire properties through using criminal proceeds for payment.

Threats – money laundering

Scope

The property industry is deemed to be an attractive sector for money laundering. Large amounts can be laundered through the buying and selling of properties. The trust accounts of estate agents can be used incorrectly for property transactions to disguise transactions with criminal origins. This happens in Sweden and abroad, and there are estate agents and other professionals in the property sector who knowingly participate in money laundering schemes. Regardless of whether it concerns an individual criminal who wants to launder criminal proceeds by buying a home, or others who more systematically launder money through buying and selling properties, facilitators are needed to provide contracts, fabricated personal data or able to help with bank transactions.

Large amounts can be involved for individual transactions and at the aggregated level. The FIU's analysis of SARs related to properties showed, for example, that the reported transactions were worth SEK 5 billion in 2022. Despite the risks referred to, estate agents continued to submit few SARs to the FIU, even though an increase occurred in 2024.

Threat actor capabilities

Estate agents are a critical resource for threat actors, thanks to their access to trust accounts and the ability to create and legitimise various types of fictive documents. Demand is high, which is why the risk of threats and extortion is rising. To execute a money laundering scheme with the help of estate agents requires some knowledge, but threat actors have enhanced their knowledge of how to manoeuvre in the financial landscape. The estate agents themselves can also be threat actors and act as PMLs.

Anonymity

The sector can be exploited for money laundering by natural and legal persons, but the majority of customers are comprised of natural persons. Straw men can be used to remain anonymous, but normally there will be access – often long-term – in their own name or that of a close relative. Property can also be bought and sold through companies where the crime actor themselves is not registered as an officer or board member, but can control the company's activities through straw men. Vulnerability in the sector is usually high, as all transactions are made via bank transfers, even though the estate agents themselves have limited opportunities to follow the transactions. This makes demands of the internal procedures and guidelines of estate agents and estate agencies to be able to fulfil their monitoring and reporting obligations, if, for example, counterpart details are missing from the bank.

Summarising assessment

The property industry is deemed to be a high risk sector for money laundering. Money laundering within the sector can either be conducted when the agent is unaware of money laundering being involved, is aware of but chooses to ignore it, or is directly involved and acts as a PML. Estate agents comprise a critical resource for threat actors in that the sector has the capacity to launder considerable amounts. Demand is high, which can increase the risk of threats and extortion. Estate agents are known to set up trust accounts with the purpose of providing legitimacy for transactions, and to set up different types of false or misleading documentation that is then used as part of a money laundering scheme.

In conclusion, the threat regarding money laundering in the sector is deemed to be high.

Vulnerability – money laundering

The chances of detection

Risk awareness and knowledge vary within the industry, but are generally deemed to be relatively low. A relatively large part of the profession is young and inexperienced, which sets high requirements for guidance and support from the estate agencies employing new agents. The Estate Agents Inspectorate also sees a need to overhaul estate agent training to give new estate agents sufficient skills to help combat money laundering and terrorist financing. The relatively low knowledge level combined with a largely commission-based industry means greater vulnerability. Reporting to the FIU from the sector is limited, but has grown a little.

The assessment is that awareness of abuse of trust accounts has increased in many banks, which has likely made it harder to use them for criminal purposes at several levels. But there are business-related incentives for banks to tone down the risks to avoid damaging lucrative business relationships with estate agents. Estate agencies often collaborate with, or are sometimes owned by, a bank able to assist with transfers and to market housing loans.

To increase the chances of detecting PMLs, it is extremely important that banks state the names of estate agents in the money laundering reports that concern property transactions. Examples of estate agents being accused of money laundering or losing their licence have considerable signal value, not just to encourage a tightening of the industry, but also for banks. The estate agencies can play a key role here by helping to increase risk awareness amongst the estate agents and of the AML regulations.

Given the new opportunities for collaboration according to chapter 4a of the AML, the chances of detecting money laundering have increased.⁹²

Compliance

5 SARs were submitted to the FIU in 2020 from the sector, 92 were submitted in 2024.⁹³ That is a substantial percentage increase, but seen in the number of registered obliged entities, reporting from the sector remains low. The low degree of reporting can have several reasons. It can be due to certain estate agents not being aware of the low degree of suspicion required for reporting. It can also be due to there being estate agents who consciously fail to report to the FIU despite there being a suspicion. And yet another reason can be the risk understanding and ability of the estate agents to risk classify their customers. If the industry classifies the risks of money laundering in its business relationships incorrectly to a large degree, it will mean that the estate agents do not perform adequate checks to identify the risks that exist. Another reason could be reluctance to be perceived as inquisitive towards buyers and sellers, especially in periods of low demand or when competition is high.

Within the framework of the Estate Agent Inspectorate's supervision, recurring failures with customer due diligence and documentation of customer due diligence procedures by estate agents are identified. Risk awareness in estate agents generally needs to increase, information acquisition within the framework to achieve basic customer due diligence and their ability to perform adequate risk profiling of their customers must be improved. Furthermore, better customer due diligence procedures need to be adopted and documented to a greater extent.

The Estate Agents Inspectorate has also identified weaknesses in the work done by estate agencies to combat money laundering. An improvement has occurred since the last sector-based risk assessment, but there are still general risk assessments, procedures and guidelines that do not fulfil the requirements of the AML act. The Estate Agents Inspectorate has produced a report⁹⁴ highlighting the weaknesses in estate agencies. An estate agency needs to ensure that it has excellent general risk assessment, procedures and guidelines, understands the purpose and problems of the regulation and helps and supports its agents employed.

The Estate Agents Inspectorate seeks to ensure that the right estate agencies are registered. Part of its registration procedure therefore is testing honesty and suitability. To support its assessments, the inspectorate obtains register extracts from police crime records. The inspectorate currently has no legal right to obtain details on a number of crimes, such as drug-related and smuggling. This implies an enhanced risk of persons committing various forms of crime being granted registration despite otherwise being deemed unsuitable and therefore denied registration if such crimes were known to the authorities. The inspectorate makes annual checks via extracts from criminal records of the honesty and suitability of registered estate agents, but these checks also do not provide the opportunity of detecting certain forms of crime that could have been committed by an estate agent.

⁹² Collaboration according to chapter 4a of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

⁹³ The category "Estate agents" includes "Estate agencies" as they have been under an obligation to report since 2021.

⁹⁴ The Estate Agents Inspectorate, *Tematisk tillsyn – Kartläggning av mäklarföretagens arbete mot penningtvätt*, Ref. no. 22-2557. (In Swedish).

The Estate Agent Inspectorate's supervision has identified failures with customer due diligence and documentation or that such procedures have been completely ignored. The inspectorate has stated that estate agents have the same responsibility when undertaking documentation to risk classify and conduct customer due diligence checks as for normal brokerage activities according to the AML act. Supervision has also shown that documentation is performed and that estate agents can, for example, produce an object description without even visiting the property.

Summarising assessment

Reporting to the FIU has increased in recent years, but remains low. Estate agencies often collaborate closely with banks and the business-related incentives for banks can cause conflicts of interest. Risk awareness and knowledge is deemed to generally be low within the industry and estate agents are not always aware of where or who transactions come from. There are often weaknesses in their procedures to avoid being exploited for money laundering. Such weaknesses combined with a largely commission-based industry means greater vulnerability to money laundering.

In conclusion, the vulnerability to money laundering in the sector is deemed to be significant.

Risk – terrorist financing

There is no known method by which the sector is used for terrorist financing in Sweden at this time. No international surveys have been conducted. The sector's risk of terrorist financing has therefore not been assessed.

7.15 The Swedish gambling market

Overall sector risk:



The sector covers gambling (for money) that is licenced, authorised or registered according to the Gambling Act (2018:1138).⁹⁵

General description of the sector and related products or activities

The Gambling Act contains seven different types of licences and permits:

- National gambling licence (chapter 5 of the Gambling Act) is mainly granted for slot machines and certain forms of lotteries. Such a licence is only granted to a directly or indirectly wholly state-owned limited company.⁹⁶
- The licence permits gambling for charitable purposes (chapter 6 of the Gambling Act) covering certain forms of lotteries. Such a licence is only granted to charitable associations or registered religious societies mainly established for charitable purposes.
- Licences for commercial online gambling and betting (chapter 7 and chapter 8 of the Gambling Act) are granted for the provision of online casinos, online bingo and computer-simulated slot machines and betting. They are open to application by market actors.
- A licence for land-based commercial gambling (chapter 9 of the Gambling Act) includes online casino gambling not played in a casino, playing on slot machines and card games in tournament format under certain conditions. Licences can be applied for by market actors.
- A licence for ship-based gambling in international traffic (chapter 10 of the Gambling Act) includes slot machines and casino gambling not online or played in a casino.
- Permit for gambling software. Anyone producing, providing, installing or modifying gambling software used for the provision of online gambling according to chapter 7 or chapter 8 of the Gambling Act must have a permit (chapter 11, section 6 of the Gambling Act).

The Swedish gambling market covers companies and organisations of varying sizes and character. It includes state-owned and controlled groups, international gambling companies turning over huge amounts annually and small, charitable associations running small-scale lotteries. Turnover for the various forms of gambling varies a lot. The same applies to the risks associated with the various forms and the way they are organised.

⁹⁵ Chapter 1, section 2(1), para. 15 of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

⁹⁶ Casino gambling under the national gambling licence was withdrawn on 1 January 2026.

Key figures	
Number of companies	374 licenced (plus 189 with a permit for gambling software)
Number of employees	4 200 ¹
Number of business connections established	No information
Company balance sheet total	No information
Company turnover	SEK 27,848 million ²
Total number of physical customers	5 946 593³
Total number of legal customers	0

¹ Permanent employees in Sweden. **Source:** Swedish Agency for Financial and Public Management

² Net turnover (bets placed minus winnings). **Source:** Swedish Tax Agency and Swedish Gambling Authority

³ **Source:** General Gambling Report 2024 and Swedish Gambling Authority

Money laundering – description of the risk scenario including known approaches

Probably the most common criminal activity within the gambling sector covered by the AML act is gambling paid with crime proceeds. The risk of gambling for money being exploited for money laundering is present in various forms of gambling. The risk of money laundering varies with the legal prerequisites for the arrangement, scope, distribution, anonymity, forms of betting or payment and disbursement of winnings. The risk is deemed to be highest for commercial online games and betting (online and land-based). This mainly depends on the chances of high bets, winnings and high turnover. The risk is influenced for online betting by players using player accounts, and for land-based betting by the fact that cash is involved.

Arbitrage gaming through betting

Laundrying criminal proceeds through betting usually implies a risk of the bet being lost and that the assets are therefore lost wholly or partially. Forms of gambling that offer high payout rates, i.e. a large element of the bets is repaid to the players, are deemed to be very attractive as the money is laundered by passing it through betting. High payouts of winnings therefore represent higher vulnerability to this form of gambling being used for money laundering.

The level of winnings payouts in most instances is predetermined, e.g. through a winnings plan, rules, machine or software settings, and differs between different forms of betting. Betting differs from other forms of gambling as the payout of winnings depends totally on the player's own choices and, to a certain extent, skill. By betting on safe matches with very low odds, a high rate of payout can usually be ensured. The player can also compare odds or use software services that constantly gather large volumes of odds from gaming companies and bet on all possible outcomes of a betting object, but with various providers. A win can be guaranteed in this way. This is called arbitrage betting, a way of winning money regardless of outcome in betting with odds. Arbitrage betting is often associated through rules, terms and conditions with European gaming companies. On markets with high turnover and high betting limits, it can be hard for gaming companies to detect individual players. The risk of detection is further reduced by parts of bets being spread on foreign betting markets.

Money laundering via online betting

Online betting offers the chance of high bets and winnings and requires no particular knowledge of complicated schemes to be exploited for money laundering. Several persons can make bets directly or indirectly in a betting account where the various obliged entities only see a small portion of the chain. Money is usually deposited in a betting account from an account at a payment institution. Withdrawals from betting accounts can be made in the same way. Laundered money thus passes through several sectors and putting it in a betting account and betting online is only part of the scheme. To follow are examples of approaches.

Rigged online poker

The Gambling Act does not permit transfers between betting accounts, but funds can be transferred between players, for example, via known losses in poker through the giving and taking of chips (chip dumping). Criminal funds are deposited into the bank accounts of one of more persons in cash, bank transfer or Swish and the deposited into the betting account. The players agree a time with yet another person and play at the same table online. During the time they play, they are in contact by telephone. They can thus ensure that the money is transferred to the latest arrival through rigged losses. That person can then make a transfer from their betting account to their bank account, whereupon the deposit becomes legitimate winnings. This can occur between players acting in collusion with each other or using illegally obtained legitimization.

Money held in a gambling account without being used

Money from criminal activities is deposited into a bank account in cash, by bank transfer or Swish. It is then deposited into a gambling account where it is held with no intention of being used to gamble. The money can either be transferred shortly thereafter back to a bank account, often another bank and can then be seen as legitimate winnings with obscure links between deposit and withdrawal. The money can also be held in a gambling account for extended periods. In such instances, the purpose is to conceal criminal proceeds from the authorities. Long-term holding is usually in large and medium-sized gambling companies where the risk of bankruptcy is deemed to be lower. Low level play on low risk gambling can be seen on the account to avoid bank monitoring systems⁹⁷.

Money processed through several different rounds of gambling

Criminal proceeds are deposited into a bank account in cash, by bank transfer or Swish. The money is then deposited into a betting account, for example, via a payment institution handling the transaction. The money can then be spent on several rounds of gambling to avoid being caught in the gambling company's monitoring. The crime actor can also opt to gamble on games with a high repayment percentage. Small gambling losses are accepted as the actor is left with a large part of the bet made and the sources of the money have been concealed. The actor can then transfer the amount left over to their bank account and the amount can be accounted for as winnings. The main purpose of this scheme is to create an explanation as to where the money came from, and to make it hard to follow the money as it has passed through several sectors with none of the individual obliged entities able to see the whole chain of transactions.

Money laundering via match fixing

Match fixing is basically a corruption crime. Crime proceedings can be used to bet on odds to conceal the source of the money. This procedure is also a money laundering scheme, as the proceeds can be laundered and increase in value. To follow are two examples of money laundering through match fixing.

A match is to be played between team A and team B, and several gambling companies offer odds on the match. The odds are calculated from the likelihood of a given match result. In this example, the odds are based on team A being expected to win the match – but the players in team A knowingly contribute to their team losing. The actor involved in this scheme bets on team A losing, which gives high odds. Team A loses the match and winnings are paid to the actor, meaning the amount of money bet is now laundered and increased in value.

Criminal networks can be involved in money laundering via match fixing by, for example, helping football clubs with funding. Talented players who play at a higher level than the opponent club are recruited, and offered large one-off bribes to sign for the club, along with bonuses to tempt them. The club then has a good chance of directing matches into wins and losses, the number of goals, etc., and criminal actors can benefit from that advance knowledge to derive winnings from the betting company. Winnings are disbursed and the money laundering process is complete.

⁹⁷ Gambling companies generally have good monitoring systems able to detect low account activity, i.e. they can detect money placed in an account without being used to gamble. But there are gambling companies who are not aware of this method and therefore do not detect such deposits. The Swedish Police Authority (2021), *Penningtvätt på spelmarknaden, via onlinespel, vadhållning och statliga kasinon*. Ref. no. A102.215/2021.

Transferring criminal proceeds

Criminal proceeds can be transferred by chips or winning tickets physically changing owner. A customer relationship conducted remotely with multiple payment methods can be used by criminals to exploit gambling companies and their gambling accounts as a service to transfer illegally acquired funds to other people.

Law enforcement authorities know that gambling accounts have been used to channel funds without the account holder gambling for money.⁹⁸ If the gambling company fails to verify that the recipient of a disbursement is the same as the owner of a gambling account, the account can be used to transfer to someone other than the account holder.

Reports made by banks and payment institutions to the FIU also indicate that several persons can make direct or indirect transfers to a gambling account.⁹⁹ For example, several persons can make deposits to a bank account via Swish, whereupon the account holder transfers the total amount to their own gambling account. The gambling company will find it hard to detect this, as it cannot see the full transaction chain.

Organised crime and facilitators

There are international examples of how groupings within serious organised crime used gambling companies to facilitate money laundering. One risk scenario is that organised crime infiltrates or owns a company licenced according to the Gambling Act in Sweden, with the aim of laundering money. Transactions of criminal funds can be concealed in the company's legitimate transactions. It can be a question of a legal gambling company where black money is laundered, or illegal gambling where the earnings can be regarded as criminal proceeds.

Exchanging for larger denominations

Exchanging criminal proceeds for larger denominations using the gambling market is possible when licenceholders allow cash bets. Because organised crime is becoming more and more international, the transportation of large amounts of cash across borders is a common feature of money laundering. If criminal proceeds consist of small denomination notes, they need to initially be exchanged for larger denominations to reduce the risk of attracting attention. Another method is for bets to be paid in small denominations but winnings to be paid in large denominations.

Threats – money laundering

Scope

Suspicious activity reports to the FIU from gambling service activities have increased from 907 in 2020, to 3,715 in 2024. The reports linked to gambling transactions from banks and payment institutions are witness to a range of approaches being used to deposit money in gambling accounts, which can be part of money laundering. Suspicious activity reports made by gambling companies are often due to a pooled or individual assessment of criminal history, low income in relation to the deposits made and the lack of response from the customer in the event of stricter customer due diligence procedures.

Only natural persons can gamble for money. This means that legal persons are excluded from being able to launder money within the sector. Criminals can own or infiltrate gambling companies to use them for money laundering. The possibility of laundering money in the sector is deemed to be relatively high. Commercial online gambling is accessible 24 hours a day for anyone who wants to gamble and launder money. The range of platforms taking cash can run a high risk of being exploited for money laundering.

High bets and winnings and an industry with high turnover are very attractive for laundering money. Money can also be laundered quickly, as gambling companies offer fast transactions and registration of new gambling accounts.

⁹⁸ Swedish Gambling Authority, *Åtgärder för att motverka att spelkonton används för kriminell verksamhet*, 2024. (In Swedish).

⁹⁹ The Swedish Police Authority (2021), *Penningtvätt på spelmarknaden, via onlinespel, vadhållning och statliga kasinon*. Ref. no. A102.215/2021. (In Swedish).

Threat actor capabilities

To play commercial online gambling requires that the gambler is registered with the licenceholder in principle (chapter 12, section 1 of the Gambling Act), which presumes ID checks through reliable electronic identification or the like (chapter 12, section 2 of the Gambling Act). Logging in is then possible through simplified methods such as user name and password. Deposits in gambling accounts must also be made in Swedish kronor via an approved payment service provider. On the other hand, gambling companies can collaborate with payment service providers offering exchange from cryptoassets to kronor, which implies that gambling can be done in cryptoassets. It is rarely possible for a natural person with a gambling account to play with cash at a physical gambling venue, as this gambling must be done through a gambling account.

But it is possible to use someone else's identity to open and use a gambling account. No particular ability is needed for threat actors to launder money in the sector. One method observed in other jurisdictions is the use of bots, either in quantity on online casinos or in complex patterns for betting to minimise the risk. The existence of gambling with bots cannot be excluded in Sweden.

Anonymity

Customers are identified by the gambling company checking e-identification when a gambling account is registered online. Only natural persons resident or staying permanently in Sweden can be registered for online gambling. Requirements for identification and registration of visitors and gamblers also apply to casino gambling and land-based betting. Certain forms of gambling are exempted from the requirement for registering, for example, the sale of scrape lottery cards and bingo. But threat actors can also remain anonymous by exploiting the identities of others.

It cannot be excluded that receipts are used by someone other than the person who made a deposit for a game. It is therefore possible that money is paid into an account that does not belong to the actual player.

The Swedish Gambling Authority has also found persons playing using someone else's account. It is not unlikely that borrowed identities are used when registering a gambling account. Examples include players who cannot register an account using their own personal data for various reasons, or criminal actors using the identities of others to be able to play anonymously. There may be a risk of gambling accounts being registered using loaned identities being exploited for money laundering.

Summarising assessment

Suspected activity reporting to the FIU has increased, indicating different approaches. The possibility of laundering money in the sector is deemed to be relatively high, and requires no special abilities of threat actors. A threat actor may, however, need access to borrowed or stolen identities to be able to create and use a gambling account anonymously. Some games can be played with cash, such as casino and land-based betting, and online casinos are open 24 hours a day. High bets and winnings and an industry with high turnover are very attractive for laundering money. Money can be laundered quickly, as gambling companies offer fast transactions and registration of new gambling accounts.

In conclusion, the threat regarding money laundering in the sector is deemed to be high.

Vulnerability – money laundering

The chances of detecting money laundering

The Swedish Gambling Authority believes that gambling companies have developed systems to check their customers through internal monitoring which can detect gambling patterns that indicate money laundering and fraud. But certain gambling companies still use a reverse checking system in which it is relatively simple to deposit money in a gambling account, but harder to transfer it to a bank account.

There is also a certain degree of vulnerability in that online gambling companies rely on e-identification as the only form of legitimation when registering. It is therefore possible for a gambler to borrow or misuse someone else's e-identification and remain anonymous to a certain degree. Using false identity documents make it possible to open one or more gambling accounts. They can then be used to commit fraud or money laundering. Identity fraud is therefore a high risk when a new customer is registered by a gambling operator.

The Swedish Gambling Authority has found that certain gambling companies are poor at risk classifying customers and in checking the customer's risk profile, which indicates that a general increase in their skills level is needed, for example, in how the companies initially and regularly work with the purpose and nature of the business relationship. Among other things, small bets increase the risk of it taking time for a gambling company to suspect money laundering. Despite existing checking systems, there is in the nature of the business that risk increases in companies with many transactions and high turnover.

The opportunity to trace gambling money is limited, as several persons could have made deposits to the same gambling account. It is difficult to follow the money once it has been paid into a gambling account. The money can also be transferred to a foreign bank account. The Swedish Gambling Authority recommends that any disbursements should be made to the same account the deposit came from (closed loop transactions), but experience from crime investigations shows that the recommendation is not always followed. Swedish banks have shown a tendency to be more reluctant to welcome gambling companies as customers. There is therefore a risk that such companies choose banks outside the EU. If a gambling company is active in Sweden and uses a bank outside the EU, it becomes harder to trace money transfers. A gambling company established in Sweden has no obligation to use a Swedish bank.

The ownership structure of a gambling company can often be highly complex, and the parent company can be in a country outside the EU. Identities are checked and ensured of the actual beneficial owner, but frontmen are known to be used.

Online gambling companies are cross-sectoral and can market themselves on the ability of payment institutions to make rapid payouts of winnings. Apart from a gambling company, banks and a payment institution are also needed to complete money laundering. It is a challenge for the obliged entities and law enforcement authorities to understand and detect the transaction chain when money is moved between bank accounts via a gambling account. All gambling has to be conducted in Swedish kronor, but the money risks being quickly disguised upon deposit and withdrawal from a gambling account. Many gambling companies do have turnover requirements for money, which reduces the risk of a gambling account only being used to pass money on. If criminal actors form a gambling company themselves to launder money, the scheme can be more advanced and hard to detect.

Gambling accounts are not covered by the Act on Accounts and Safety Deposit Systems (and are therefore not in the Mekanismen). The final report on the Swedish Gambling Authority's commission (Fi2023/03186) will be submitted to the Government Offices where the issue currently lies.

Compliance

Gambling companies intending to trade and market themselves in Sweden must have a Swedish gambling licence since 1 January 2019. However, the range of online gambling outside the licenced market is extensive and relatively easily accessible to Swedish gamblers. If gambling online is subject to licence or is not governed by the Gambling Act and the so-called direction criterion. A gambling company cannot market (direct) itself to Swedish gamblers without this licence. The problems highlighted concerning applicability of the direction criterion imply, in practice, that there is a tripartite market (one licenced, one legal unlicensed and one illegal unlicensed). This is problematic and can be exploited by gambling companies who do not want to comply with the requirements set by the Gambling Act, which implies lower consumer protection and distorted competition. The current area of application also implies lack of clarity in the application and effectiveness of other regulations in the area, such as the opportunity of limiting the payment flow to gambling platforms with no Swedish licence. The Swedish Gambling Authority has assessed that the degree of channelling¹⁰⁰ was 85% in 2024. Even if the degree of channelling has increased since before the new regulation, extensive gambling continues in Sweden with companies that do not have a Swedish gambling licence.

According to the AML regulations, the Swedish Gambling Authority has no supervisory responsibility toward gambling companies with no Swedish licence. The Swedish gambling market is international to a high degree. Most gambling companies operating in Sweden with a licence are based in Malta. The rate of development within the gambling industry is also high, and many major changes have taken place on the market in recent years.

¹⁰⁰ "Degree of Channelling" means the proportion of gamblers gambling with companies with a Swedish gambling licence.

There is a risk that gambling companies have poor customer due diligence procedures, as some of them only perform checks when winnings are withdrawn and not upon registration and deposits into a gambling account. There is also reluctance to report suspicious activities for the most profitable customers, if the degree of suspicion is low.

Because the gambling market is a sector with a high risk of money laundering, effective and deterrent means of intervening are required. The penalties when a gambling provider breaches the AML act differ considerably from those for breaching the Gambling Act. The size of the penalties therefore risk being incorrectly interpreted as compliance with the provisions of the AML act was not given priority for licence and permit holders. The penalties were harmonised on 1 June 2024 and the penalty for breaching the AML act can reach the same amount as for breaches of the Gambling Act (chapter 18, section 21a of the Gambling Act).

Summarising assessment

Certain gambling companies still use a reverse checking system in which it is relatively simple to deposit money in a gambling account, but harder to transfer it to a bank account. The chances of tracing transactions are slim, especially as several persons could have made deposits to the same gambling account, and money can be moved between bank accounts via a gambling account. Traceability is also reduced because many gambling companies use banks within and outside the EU. There is also a risk that legal persons set up gambling companies with the aim of laundering money from criminal activities. Due to the lack of clarity on how the Gambling Act should be applied, gambling is extensive in Sweden via gambling companies with no Swedish licence, which means such companies fall outside the responsibility of the Swedish Gambling Authority. Some companies fail to risk classify their customers and there is a risk of poor customer due diligence procedures. There is even reluctance to report suspicious activities for the most profitable customers.

In conclusion, the vulnerability to money laundering in the sector is deemed to be significant.

Risk scenario, including known approaches of terrorist financing

The Swedish gambling market encompasses a number of different forms of gambling, and is subject to rapid development and high turnover of liquid funds. Given the various gambling forms, approaches can differ and no assessment has been made of terrorist financing other than that for money laundering.

Threat – terrorist financing

Scope

Terrorist financing through gambling companies is deemed to not be extensive, but the rise in turnover on the gambling market implies that there is a risk of more transactions being committed for terrorist financing. Otherwise, the same circumstances reported for money laundering apply.

Threat actor capabilities

No special abilities or knowledge are needed to exploit commercial online gambling, but to avoid being checked, some knowledge of the threshold limits or transaction patterns that trigger alarms is useful.

Anonymity

With regard to the chances of being anonymous when using commercial online gambling, no assessment has been made other than that for money laundering.

Vulnerability – terrorist financing

The chances of detecting terrorist financing

The same actual circumstances as described in the section on money laundering apply to the issue of terrorist financing with regard to the chances of detecting money laundering and traceability. But there is a difference when it comes to method of provision, transaction patterns for terrorist financing can be harder to identify. In case of terrorist financing, the transactions are rarely of the same non-compliant nature, which means they can be harder to catch. Given that transactions via gambling companies are part of a longer transaction chain with terrorist financing as the goal, it is also harder to catch an isolated transaction and understand its purpose.

Compliance

Concerning compliance when it comes to terrorist financing, no assessment has been made other than that for money laundering.

7.16 Merchants

Overall sector risk:



"Merchants" are defined as legal and natural persons trading professionally in goods.¹⁰¹ Transactions are or will be conducted in the business – or in parts of it (individual or connected) for which an amount is disbursed or received equivalent to eur 5,000 or more.

General description of the sector and related products or activities

Obligated entities within the sector can be in a range of industries, but often sell expensive goods, known as "rare goods". Examples include the sale of motor vehicles, parts for motor vehicles, scrap and metals, jewellery, watches, coins and antiques. The businesses involved range from individual firms with no employees to limited companies with a number of employees. Turnover for companies within the sector varies a lot, depending on their circumstances, for example a large car dealer compared to a small jewellery business.

On 31 December 2024, the Swedish Companies Register for money laundering listed a total of 1,082 companies, who stated that run cash sales of goods when they registered. Of these, about 690 (around 64%) stated that they only run reportable activities. The remaining 392 obliged entities in the register stated that they also run other activities under the supervision of the County Administration Boards. There is likely a large hidden number of obliged entities who could be classified as traders, and which are subject to the AML act, but are not registered with the Swedish Companies Register for money laundering. Determining how many obliged entities running reportable activities without being registered is hard to do, as there is no complete register of traders.

Money laundering – description of the risk scenario including known approaches

Apart from criminal proceeds used for consumer goods for own use, there are a number of approaches for laundering money through merchants. Money laundering within the sector can either be conducted when the obliged entity is unaware of money laundering being involved, is aware of but chooses to ignore it, or is directly involved and acts as a PML.

Goods converted to deposits in an account

Goods are bought for cash from criminal proceeds and then sold against a deposit in an account or via Swish, whereupon the actor can show that the money came from a sale. Another method is for actors to buy goods with cash from criminal proceeds, return the products and ask for the amount to be paid into a bank account. Varying large amounts of cash handled by the trader are a circumstance that can indicate that the trader is party to money laundering.

Gift vouchers as an intermediary

Gift vouchers for just under SEK 50,000 are paid for with cash from criminal proceeds. The amount is under the threshold (equivalent to eur 5,000) for when the obliged entity has to perform customer due diligence. Several gift vouchers are bought separately and then exchanged for expensive goods without the customer having to provide identification. The occurrence of several such gift vouchers at the trader can indicate money laundering.

¹⁰¹ Chapter 1, section 2(1), para. 16, of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

Cryptoassets are also used to buy individual gift vouchers, which are then used in stores, online or sold via auction platforms on the internet. Gift vouchers can also be used on various online gambling platforms.

Money laundering in wholesale trade

In common with other cash- and labour-intensive industries, there is an elevated risk of money laundering within wholesale¹⁰². The nature of the industry gives rise to a variety of potential ways of laundering money. Examples of money laundering approaches in wholesale trade:

Import and export

Laundering money via international trade, often referred to as "Trade-based money laundering" or TBML¹⁰³, is a method that allows large scale money laundering. Industries that trade in large volumes at low value, such as clothing and food, can be involved. Examples of approaches include over- and under-invoicing of goods and services, over- and under-delivery of goods and services, ghost deliveries (only money changes hands, not the goods). Import and export of goods mean international transactions. Criminal proceeds can be easily layered and integrated into the financial system via import and export of goods, without the authorities and reportable obliged entities suspecting money laundering.

Cash placings and false invoices

One way of laundering cash generated from crime is to place it in businesses where cash continues to be used to a large degree, such as wholesale. Cash originating from crime is simply mixed with legal earnings using the company as a front for the criminal activity. Cash placings are often combined with false invoices.

Luxury goods sold abroad – value bearers instead of cash

Exclusive capital goods such as bags, watches, expensive cars, jewellery and gold, are bought and sold as part of money laundering. The possibility of exchanging and refunding Swedish cash from dubious sources has been reduced abroad. The demand for alternative ways of laundering money through cash has therefore increased. To some extent, criminal proceeds are invested in sought-after luxury goods instead, and such goods are used as value bearers instead of cash, and they can be sold abroad. The goods can also be used in Sweden as a means of payment instead of cash, which means the second hand market for such goods can be of considerable interest.

Gold retains its value over time, and in some instances, it is reasonable to assume that criminal actors prefer physical assets that they can control to cryptoassets, for instance.

Money laundering through the auto trade

The auto trade has long been an industry in which several different areas are subject to enhanced risk of money laundering and other financial crimes. Companies in the industry are therefore an attractive and valuable front for organised crime. Examples of money laundering approaches in the auto trade:

Granting credit for car purchase

A car loan is usually taken from a bank or finance company the car dealer collaborates with. The loan may have been granted on false grounds (credit fraud) and repayments of the loan can be made with criminal proceeds. Common features are short agreement terms with high amortisation, and other people than the credit taker make payments to the credit provider. The cash deposit paid to the car dealer may also be paid with crime proceeds, including cash.

102 Wholesale trade involves large volumes of goods, known as trade goods. Wholesale trade is primarily conducted by wholesalers between manufacturing industry and retailers. Goods are not sold to private individuals.

103 Trade-based money laundering.

Trading with cars within Sweden and with other countries within and outside the EU

The auto trade is global and trade between countries offers additional opportunities for money laundering. Trade-based money laundering occurs within car trading, when criminal proceeds are moved through apparently legal transactions. A common method is over- and under-valuation of vehicles when the car changes owner.

Money laundering transactions disguised as car trades

Money laundering transactions can be disguised as transactions that indicate the buying or selling of a car, but when no change of owner has occurred or even when none of the parties have anything to do with the car at all.

Professional money launderers

There are goods traders who are PMLs and who assist professional criminal actors with money laundering. One particular example is watch dealers.

PMLs within the watch trade

The use of exclusive watches for money laundering has grown in Sweden over the last decade. Even though watch dealers in their capacity of goods dealers are obliged to report suspected money laundering to the FIU in the event of cash payments equivalent to eur 5,000 or more, very few reports are submitted from dealers buying and selling watches. But when the FIU investigates suspected transactions, transactions with watch dealers are relatively frequent occurrences. Transactions involving watch dealers also appear regularly in the explanations from banks as to why they suspect money laundering.

Information on suspected PMLs within the watch trade should be able to be reported to a greater degree by banks, for example, when circumstances permit. They can involve frequent transactions with individual watch dealers, when the purchase of exclusive watches does not equate to the economic circumstances of the customers in general, such as low or no income. The awareness of the banks of the circumstances surrounding a reported transaction with a watch dealer are of considerable interest to the FIU. If the obliged entity has obtained an agreement, an invoice or bill of sale from the reported customer when performing its investigations, they will be important documents.

Threats – money laundering

Scope

The merchant sector is easily accessible to most threat actors. The purchase of goods with known value such as motor vehicles, boats, gold and watches can be made with, for example, cash proceeds from crime. This allows threat actors to convert their illegally earned money into capital goods, that can be sold or pledged in turn in the next link. The scope of money laundering via this sector is therefore deemed to be extensive.

Threat actor capabilities

No particular ability is needed for threat actors to launder money in the sector. In some large-scale money laundering schemes, threat actors may need access to straw men to purchase and sell the goods. Money laundering within the sector can either be conducted when the obliged agent is unaware of money laundering being involved, is aware of but chooses to ignore it, or is directly involved and acts as a PML.

Anonymity

In cases when an obliged entity fails to perform checks of the customer's identity and source of funds, a threat actor can conduct a transaction anonymously. This obscures the traceability of the transaction. That makes it possible to use the sector to launder money with no major risk of detection in certain cases. A threat actor can also use straw men to remain anonymous.

Summarising assessment

The sector is easily accessible and facilitates the use of cash. This implies that transactions can be made very quickly while anonymity is high. PMLs are present in the sector.

In conclusion, the threat regarding money laundering in the sector is deemed to be high.

Vulnerability – money laundering

The chances of detecting money laundering

The FIU received 69 SARs in 2024 concerning professional trade with goods from the sector, which is a reduction from 2020 when 122 reports were received. In accordance with the AML act, traders must conduct risk assessments of their products and customers, along with customer due diligence, when dealing with a new customer whose transactions with cash total eur 5,000 or more. Measures must also always be taken when there is a suspicion of money laundering, regardless of the size of the transaction or whether it is conducted in cash or not. The chances of detecting money laundering in the sector are limited by transactions partially conducted with cash, which reduces the chances of showing that the money could have originated from crime. Another vulnerability is that the sector is diverse and is spread over large geographic areas.

More and more dealers of exclusive goods report that they no longer take cash. The use of cash at such dealers should be regarded as an indication of money laundering and a chance to detect PMLs.

Compliance

Awareness of risks, along with knowledge of the AML act is deemed to be low in the sector. Serious breaches in compliance have been detected by supervision by the County Administration Boards. Several obliged entities do not conduct general risk assessment at all, and have not considered all the risks that should be assessed. The obliged entities are thus generally regarded as not being aware of the requirements of the law stipulating that they must assess their own business. Neither is there any understanding for how their own business can be exploited for money laundering.

If an obliged entity reports suspected money laundering, the purchase can be denied, which can mean lost income for the owner of the business or for salespeople on commission. This can, in turn, lower the incentive to report suspected money laundering. Purchases and transactions mostly take place through a physical meeting with the customer, which means that threat situations can arise, making it harder to refuse the purchase or report it as suspicious to the FIU.

Summarising assessment

When cash is used within the sector, transaction traceability can be limited. There is also a risk of threat situations arising in conjunction with purchases, as transactions often take place physically in a shop, and the businesses concerned can be small, with only one or a few employees. This can imply that obliged entities are afraid to conduct the necessary customer due diligence to reduce the risk of money laundering. Exclusive goods can often be sold in the legal and criminal economies, which makes high demands of the obliged entities in their application of the AML act. But obliged entities within the sector are generally deemed to be aware of the AML act and the risks of money laundering, which is a considerable vulnerability.

In conclusion, the threat regarding vulnerability to money laundering in the sector is deemed to be high.

Risk scenario, including known approaches of terrorist financing

One method is that goods are used instead of money as a link in the transaction chain intended to finance terrorism, partly in recognition of the loss in value of the Swedish kronor and to increase anonymity and avoid checks. Luxury goods such as clothes, bags, watches, jewellery and precious metals are bought and taken out of Sweden by persons wearing them. Once out of the country, the products are sold and the money obtained used for terrorist financing.

Threat – terrorist financing

Scope

The merchant sector is easily accessible, but the approaches used to ultimately finance terrorism are deemed to be more complicated than those described for other sectors. But the sector is deemed to be exploited to some degree for terrorist financing.

Threat actor capabilities

Concerning the abilities of threat actors when it comes to terrorist financing, no assessment has been made other than that for money laundering. See above.

Anonymity

Straw men can be used for buying and selling goods to improve anonymity. When buying goods, it is also possible to pay an amount just under the threshold that will trigger more comprehensive checks. Some traders also accept payments in cash. These circumstances imply that the chances of anonymity in the sector are good.

Vulnerability – terrorist financing

The chances of detecting terrorist financing

The same actual circumstances as described in the section on money laundering also apply to terrorist financing linked to wholesale and retail goods. Furthermore, it is hard to determine whether the purpose of a purchase is to take the goods out of the country for resale and ultimately terrorist financing.

Compliance

Concerning compliance when it comes to terrorist financing, no assessment has been made other than that for money laundering. See above.

7.17 Pawnbrokers

Overall sector risk:



Pawnbrokers are a type of business that extends credit to customers against a pledge on the item¹⁰⁴.

General description of the sector and related products or activities

The provisions on pawnbrokers can be found in the Pawnbroker Act (1995:100). The act contains requirements on form of limited companies permitted for pawnbroking. If a foreign company does not want to form a Swedish subsidiary without becoming a foreign legal entity, the business must be run as a subsidiary according to the Act on Foreign Subsidiaries (1992:160).¹⁰⁵ A licence will only be given to foreign companies if they run a pawnbroking business and are subject to supervision by an official authority in the country where they are based.¹⁰⁶

Pawnbrokers must be licenced by the County Administration Boards.¹⁰⁷ Direct or indirect acquisition of shares in a pawnbroker that will lead to a qualified holding also requires authorisation.¹⁰⁸ Before a pawnbroker opens a new outlet, it must be reported to the County Administration Boards. They are also responsible for supervision of pawnbrokers.¹⁰⁹ Because pawnbroking requires a licence, pawnbroker companies cannot be registered in the Swedish Companies Register for money laundering.

Pawnbrokers must be run in a manner that maintains the trust of the general public, and can be regarded as sound. Linking the business with another business is prohibited, with the exception of selling unredeemed items¹¹⁰ repurchased by the pawnbroker. Such items must be sold by the pawnbroker over the counter.¹¹¹ There is nothing to prevent a pawnbroker from wholly or partially owning other companies running other forms of business, as long as that other business can be regarded as not having any negative effect from a consumer protection angle.¹¹²

Key figures

Number of companies	18
Total turnover	SEK 728 million

There are about 65 physical pawn shops in Sweden. The market is dominated by two large companies. These two account for around two thirds of all turnover in the sector, and for over half of all pawn shops.

¹⁰⁴ The legal definition of a pawnbroker does not exclude the traditional possibility of pledging securities. About 5% of the items held by pawnbrokers concern such loans. But this does not provide any opportunity for pawnbrokers to extend their business into the field of the normal credit market. See prop. 1994/95:178 p. 27, chapter 1, section 2(1), para. 17 of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

¹⁰⁵ 3(2) of the Pawnbroker Act.

¹⁰⁶ 4(2) of the Pawnbroker Act.

¹⁰⁷ 3(1) of the Pawnbroker Act.

¹⁰⁸ 23(1) of the Pawnbroker Act.

¹⁰⁹ 24 of the Pawnbroker Act.

¹¹⁰ An expired pawned item is something the customer has left with the pawnbroker as a pledge for a loan, but which has not been redeemed in time. When the loan period has expired and the customer has not repaid the loan and redeemed the item, it is regarded as expired. The pawnbroker can then sell the item to recover its money.

¹¹¹ 6 and 20 the Pawnbroker Act.

¹¹² Prop. 1994/95:178 p. 27, 42f.

Money laundering – description of the risk scenario including known approaches

Pawnbrokers can be used for laundering money without them actually being aware of it. Money can also be laundered by the pawnbroker being aware but choosing to ignore it, or actively taking part as a facilitator, e.g. as a PML.

Valuables from fraud or theft are sold

Criminal actors who have obtained, for example, jewellery, precious metals, precious stones and watches through criminal activities, such as defrauding the elderly or theft, can convert items to cash by pawning them. Anyone pawning an item receives a sum of money based on a valuation made of the object. The customer is also issued a pawn receipt which can then be used as apparent proof that the money is legal.

Criminal actors trade in crime proceeds.

Criminal actors can use the cash proceeds of crime to buy pawned items when the loan has expired, such as watches, jewellery and precious stones.

Items change owners, are pawned and redeemed to be sold again

One method can be compared to a loop, started by a threat actor buying goods, such as exclusive watches, at a pawnbroker's or an auction house through cash from criminal proceeds and given a pawn receipt. The objects are pawned to different pawnbrokers, and the apparently legal cash obtained is banked and the actor given a pawn receipt. More cash from criminal proceeds is then used to buy the objects back. They can then be sold at an auction house or other pawnbrokers, whereupon the cash from the sales is banked into a new account. By repeating this process and given that only a few objects are involved, large amounts of money can be laundered in total.

Documentation in the form of pawn receipts and notes along with packaging are important for the threat actor, as they can be used later to give the appearance of legitimacy.

Frontmen used for pawning and purchasing

People with or without a criminal background can be used as frontmen to pawn or buy goods, to come under the amount thresholds for customer due diligence and thus avoid traceability.

Facilitators

Intelligence indicates that some pawnbrokers actively facilitate money laundering for payment.

Threats – money laundering

Scope

The sector is deemed to be relatively easily accessible for threat actors. Even though the number of pawnbrokers is low and the individual amounts loaned are generally low, large amounts can be laundered through high frequency. Intelligence confirms that pawnbrokers are often used within certain money laundering schemes to move such items as gold, jewellery and exclusive goods further in the scheme. There is international demand for some pawnbrokers goods such as gold and diamonds.

How quickly a transaction can be done in the sector depends on the value of the goods and size of the loan. Buying a pawned item can be relatively quick.

Threat actor capabilities

No particular ability is needed to pawn or buy goods. Large amounts can be laundered through frequent buying and selling and large amounts can be laundered. Pawnbrokers can be used for money laundering without their knowledge, or by the pawnbroker being aware but choosing to ignore it. In some instances, the pawnbrokers can actively facilitate money laundering as a PML.

Anonymity

It is hard for a threat actor to be anonymous when laundering money. But frontmen have been used to reduce traceability.

Summarising assessment

The use of pawnbrokers is relatively common within certain money laundering schemes to move such items as gold, jewellery and exclusive goods further in the scheme. Such goods are also in demand internationally. By repeated buying and selling, the overall volumes are large, and the use of frontmen limits traceability. In some instances, it is deemed likely that pawnbrokers actively facilitate money laundering as a PML.

In conclusion, the threat regarding money laundering in the sector is deemed to be high.

Vulnerability – money laundering

The chances of detecting money laundering

Different pawnbrokers have different systems for customer due diligence, and risk awareness and knowledge levels vary within the sector.

Compliance

Breaches in compliance have been detected by supervision by the County Administration Boards.

The number of suspicious activity reports to the FIU is low. 12 reports were received in 2020, and 37 in 2024. The low degree of reporting may indicate that the obliged entities are not aware that they are obliged to report suspicions of money laundering, or that they actively avoid reporting. The generally low amounts loaned in the sector could be one reason, if the pawnbroker sees no risk of large scale money laundering. But the size of the amount should not influence whether reporting is done or not. One reason for the low level of reporting could be that the obliged entities are used to reporting to the police "goods watch".

Money laundering has been detected when suspicious activity reports received by the FIU from banks concerning transactions pawnbrokers have handled for their customers. A large number of suspicious activity reports concerning transactions made at pawnbrokers, yet pawnbrokers in their turn have not made any reports to the FIU. This indicates that the pawnbrokers in question either find it hard to detect such behaviour themselves or that they fail to act according to the AML act. Regardless of the reason, it represents a vulnerability in the sector.

Summarising assessment

There is a protective system in the sector to detect money laundering, but it is not complied with. The obvious vulnerability in the sector is exploited by criminal actors looking for new ways to launder money, not least when the monitoring systems used by banks are strengthened.

In conclusion, the vulnerability to money laundering in the sector is deemed to be significant.

Risk – terrorist financing

There is no known method by which the sector is used for terrorist financing in Sweden at this time. No international surveys have been conducted. The sector's risk of terrorist financing has therefore not been assessed. The sector is deemed to be in the risk zone for being yet another front for terrorist financing. There is a risk of young people with few financial resources beginning to use pawnbrokers to quickly realise cash and pass it on to terror organisations, or to travel abroad themselves to join a terror organisation.

7.18 Approved or authorised auditors or registered audit firms

Overall sector risk:



The sector includes businesses such as approved or authorised public auditors or registered accounting firms.¹¹³ It involves services such as accounting, other assurance assignments, auditor's statements and audit-related advice.

General description of the sector and related products or activities

In limited companies, only an authorised or approved auditor can act as auditor. At least one of the auditors for listed companies, large companies in terms of turnover, balance sheet or number of employees and many financial companies must be authorised.

Partnerships and limited companies providing auditing services can be registered as auditors under certain conditions. This includes that the actual company – as opposed to non-registered accountancy/audit firms – can be elected as auditors. An approved or authorised auditor must always be appointed as the principal auditor for each audit assignment. The principal auditor must sign the audit reports and state an opinion.

The provisions on authorised and approved auditors or registered audit firms can be found in the Auditors Act (2001:883). Since 2013, the title has been restricted to "authorised auditor", but auditors approved prior to that date can continue to work as approved auditors. In the following, authorised and approved auditors are collectively referred to as "auditors".

Audit assignments

Audit assignments can be divided into four categories:

- audits of historical financial information
- reviews of historical financial information
- other assurance assignments (apart from audits and reviews)
- review by special agreement.

Assurance assignments

The auditor expresses an opinion upon conclusion of the first three categories in the list on the degree of certainty – either reasonable or limited.

Auditing is the most common form of assurance assignment and is mainly governed by law.¹¹⁴ For audits, the auditor's task consists of auditing the accounts and the management, going into the detail required by best auditing practice.¹¹⁵ The auditor must achieve reasonable certainty through review that the financial statements do not contain material misstatements as a whole. This is required for the auditor to be able to express an opinion as to whether – in all material respects – the financial statements have been compiled according to the applicable rules.¹¹⁶ An audit does not examine every single transaction, but a selection, and the work is targeted to the areas where the biggest risk of misstatements

¹¹³ Chapter 1, section 2(1), para. 18 of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

¹¹⁴ For example: the Auditors Act (1999:1079), the Companies Act (2005:551), the Act on Financial Associations and the Foundation Act (1994:1220).

¹¹⁵ Section 5 of the Auditors Act. Similarly, according to chapter 9, section 3 of the Companies Act, chapter 8, section 3 of the Act on Financial Associations and chapter 4, section 9 of the Foundation Act also apply.

¹¹⁶ ISA 200 The independent auditor's overall objectives and conducting an audit according to ISA. International Standards on Auditing (ISA) are produced by The International Auditing and Assurance Standards board (IAASB).

exists and where possible errors could be material to the financial statements. Even though reasonable certainty is a high degree of certainty, there is no guarantee that an auditor always detects any material misstatements if they exist. It is possible for a company to be involved in unethical or illegal activities despite it being audited.

For a review of historical information, an auditor conducts a less detailed audit and expresses an opinion with limited certainty. For other assurance assignments, such as statutory reviews (e.g. non-cash issues, balance sheet for liquidation purposes or distribution at extraordinary general meetings), the degree of certainty can vary, depending on the circumstances.¹¹⁷ Neither is the auditor's review any guarantee that the company is honest or free of irregularities in these categories of assurance assignment.

Review by special agreement.

Review by special agreement is the most common type of review assignment in conjunction with support or assistance from authorities and organisations. Reporting for review by special arrangement does not include a conclusion, as the auditor only reports on observations made. The scope and direction of a review is agreed between the auditor and the client.¹¹⁸ As such, the auditor only reviews what falls within the scope of the assignment, not the business as a whole. Neither can this category of review, often based on a selection and documentation provided by the company, reveal hidden problems or irregularities.

Audit-related consultancy

Auditors often also offer consultancy within areas with a natural relationship to their work, such as financial management, accountancy and taxation. This type of consultation is called "audit-related consultancy".

Key figures	
Number of authorised auditors	2 772
Number of approved auditors	194
Number of registered auditing companies	244
Total number of authorised and approved auditors	2 966

Source: The Swedish Inspectorate of Auditors, register of auditors, 02.01.2025.

The number of auditors has fallen over the last two decades, but since 2020, the fall has slowed and bottomed out. Because the role of approved auditor was abolished in 2013, leaving only the role of authorised auditor, the number of approved auditors will continue to diminish due to retirements.

The number of registered audit firms has increased by almost 40% since 2020, mainly due to more accounting firms advocating choosing a firm (i.e. a registered audit firm which appoints a principal auditor for the assignment) rather than choosing an individual (choosing a single natural person) and that registered audit forms can also have other professional categories amongst their owners and management. But most audit firms are not registered as such, despite around 78% of all qualified auditors have a registered auditor firm as their employer. A registered audit firm is directly subject to supervision by the Swedish Inspectorate of Auditors, which non-registered audit firms are not.

117 For example, according to chapter 2, section 19, chapter 13, section 42, chapter 15, section 44, chapter 18, section 6, chapter 23, section 25 and chapter 25, section 15 of the Companies Act. These assignments are conducted according to the Swedish RevR 9 The Auditor's Other Opinions standard according to the Companies Act and the Limited Companies Ordinance.

118 The review is conducted according to the ISRS 4400 International Standard on Related Services according to separate agreement.

Money laundering – description of the risk scenario including known approaches

Auditor services can be used as a rubber stamp for financial reports on businesses used as part of a money laundering scheme.

Audit services can be used to legitimise illegal transactions, or to make false documents and invoices look correct. The auditor can be unaware of this occurring, ignore it – by ignoring disbursements made that have little to do with the business and payments received from shady sources – or actively participate as facilitator, e.g. as a PML.

Companies as fronts for crime

Companies are a major means of running more complex money laundering. They can also be used to generate criminal proceeds, via fraud and false invoices for example, to pay black labour or finance illegal activities.

Auditors often have assignments that cover a large number of companies and groups, contributing to their function and capability as potential facilitators and PMLs. They can legitimise the activities of several companies within the same criminal scheme knowingly or unknowingly. Given that they also possess sought-after financial expertise, they can also provide other services than those directly linked to audit assignments, such as setting up a company or advising on corporate structures.

Crimes involving layering between different accounts, often over several jurisdictions or that involve false invoices between companies that are part of the same criminal scheme, can be hard to detect for auditors and external investigators or authorities, as they take place within established corporate structures. An illegal activity is often mixed in with legitimate transactions and activities, which also obscure detection. It is also common that the company is only used for a short time and then put into liquidation, whereupon the principal starts a new company. This also makes it harder to spot irregularities, as history, relationships and links between actors and transactions can be concealed. Serial bankruptcies should be seen as a risk indicator.

Facilitators and professional money launderers assist criminal networks

Intelligence confirms that auditors act as PMLs in assisting criminal networks in money laundering schemes. An auditor can mistakenly approve a company's financial statements, thereby concealing money laundering transactions, or by accepting over-valuation of the company's assets by issuing an opinion. Auditors can also contribute with advice to support money laundering and other financial crimes. Payment for their services of this kind can, in some instances, be the assignment itself, permitted overcharging or concealed shares in the company. Auditors have also been known to have authorised access to accounts. Exercising such authority gives the auditor the right to make pure money laundering transactions that breach auditor rules and best auditing practice.¹¹⁹

Intelligence confirms that auditors collaborate with bookkeepers or executives in criminal schemes. Audits can be arranged to conceal illegal activities, such as through choice of which audit measures or sampling are to be applied. An indication of PMLs being involved is when the auditors rotate assignments between themselves, which is non-compliant.

To follow is a fictitious example of an auditor who is a PML with links to criminal networks.

The auditor has several audit assignments that can be linked to serious criminals and various criminal networks. He assists them with money laundering and other financial crimes through, for example, attesting false costs, which are then used as grounds for granting government support or different types of licences linked to activities. He also has contacts within banking through which the company can be granted loans on false grounds. He approves over-valuations of various assets and irregular transactions with family members in the audit, and ensures that apparently legitimate verifications and documentation for these activities exists.

119 See section 21a of the Auditors Act (2001:883) on non-partisanship and impartiality and, for example, chapter 9, section 17(4) of the Companies Act (2005:551) on disqualification.

Threats – money laundering

Scope

Because the need for audit services exists in all industries and because companies are a common front for large-scale and systematic money laundering, there is a considerable risk that money laundering transactions pass through the sector. The number of suspicious activity reports received by the FIU from the audit industry are few, but increasing, from 8 in 2020 to 84 in 2024.¹²⁰ The increase may indicate greater awareness or more inclination to make reports.

Threat actor capabilities

The extensive use of companies in criminal circles, the widespread variation in approaches and range of industry sectors amongst companies used show that threat actors possess considerable ability. But a relatively good understanding of finances, accounting and auditing methods is required to be able to exploit the sector as part of money laundering.

As mentioned above, intelligence confirms that auditors also act as PMLs in assisting criminal networks in money laundering schemes. In such instances, the auditor has been key to the crime, for example by selling criminal schemes and companies highly suited to money laundering to criminal actors. An auditor can also exploit schemes and companies personally. Given their expertise within accounting and finances, auditors who are also threat actors have considerable ability.

Anonymity

Complex and large scale money laundering schemes plus, for example, false personal data, stolen identities or straw men can mean that auditors find it hard to identify beneficial owners. Such difficulties exist as well when there are foreign owners and board members. That creates the possibility of actors remaining anonymous, even though it requires certain skills on their behalf.

Summarising assessment

Reporting to the FIU from the audit sector is limited, but has increased over time. Companies are often used in money laundering schemes. Intelligence confirms that auditors act as PMLs in assisting criminal networks. The need for auditors giving advice knowingly or unknowingly to enable a company to be exploited for money laundering, or hiding behind the company facade is not expected to fall moving forward. The threat of money laundering in the sector is deemed to be significant, and adequate risk assessment and customer due diligence are essential to avoid being exploited in money laundering schemes.

In conclusion, the threat regarding money laundering in the sector is deemed to be significant.

Vulnerability

The chances of detecting money laundering

An audit assignment involves reviewing a company's financial reporting and management. This requires the auditor to have good awareness of the individual customer's business, management and organisation. Auditors have no customer due diligence requirements pertaining to their customers, but to understand their business and risk assess them, they normally need to gain an understanding.

The sector often features long customer relationships, which give plenty of opportunity to detect non-conformist behaviour or activities. A key part of auditing is also the assessment of risks of irregularities linked to the financial reporting.

Compliance

The sector is heterogeneous with all sizes of audit businesses, and the understanding of and compliance with the AML regulations varies.

¹²⁰ Refers to the sector approved authorised auditors or registered accounting firms.

During 2023 and 2024, the Swedish Inspectorate of Auditors conducted a risk-based supervision project specially aimed at audit firms and the actions of auditors according to the AML regulations. In 61% of the cases within the framework of the project, the audit firm or auditor had ignored their obligations in this respect.¹²¹ During the same period, an auditor's approval was revoked after the authority's ordinary risk-based supervision detected him ignoring several of the basic obligations for obliged entities set out by the AML regulations in a very serious manner. Another auditor's authorisation was revoked following a large number of errors in his audit work and failure to fulfil his obligations according to the AML act. The choice of disciplinary action also reflected that the auditor had twice before been warned for such offences as failure to exercise professional skepticism and repeatedly recommended approval of the balance sheet and profit/loss accounts without good grounds to do so.

According to the AML act, obliged entities must report suspicions of money laundering and terrorist financing to the FIU without delay, and provide details at the request of the FIU. Reporting is handled through the goAML platform, via which the FIU also regularly distribute up-to-date information on various approaches and warning signals. The FIU has seen an increase in the number of auditors who have registered as obliged to report in goAML.

As can be seen above, the number of reports is still low, despite an increase in recent years. Because the sector features a lot of long-term customer relationships and an auditor's opinion has to be well founded, there can be reluctance to report suspected money laundering if the degree of suspicion is low. Such under-reporting to the FIU represents a vulnerability. Greater awareness is needed of under which conditions suspicious activity reporting should be made.

Despite the confirmed presence of criminal activity in companies over a long period, information on sufficiently specific circumstances is missing in many instances for auditors to initiate penal provisions or administrative measures. In court cases for example, proceedings have been taken against other actors than the auditor, despite clear indications being found that the auditor contributed to a criminal scheme.

Summarising assessment

Despite widespread use of companies for money laundering, few auditors report suspicions to the FIU. Audit assignments do not include the active seeking of crimes, but they can detect suspected money laundering in the course of their work. On the other hand, the companies audited are often only a link in a money laundering chain, and without the full picture it is hard to identify irregularities in individual companies. It is also common for money laundering to consist of small items in relation to an otherwise legitimate business. All-in-all, this means that the chances of an auditor detecting money laundering are limited, especially, for example, if a facilitator employed by an audit firm has helped to conceal the criminal activities.

Due to the difficulties above, it is probable that there is an expectation gap in that the ability of the sector to detect money laundering is believed to be better than it actually is, something that represents a vulnerability for society's defence against money laundering. The supervisory authorities may also find it hard to detect PMLs in the sector.

In conclusion, the vulnerability to money laundering in the sector is deemed to be significant.

Risk – terrorist financing

Auditor services can be used as a mark of quality for financial reports on businesses used as part of a terrorist financing scheme. A potential risk that false invoices can be used for terrorist financing.

But a relatively good understanding of finances, accounting and auditing methods is required to be able to exploit the sector for terrorist financing.

¹²¹ The Swedish Inspectorate of Auditors, verksamhetsrapport 2022-2024. Ref. no. 2025-0570. (In Swedish).

7.19 Accountancy and audit services

Overall sector risk:



Natural and legal persons providing professional accounting and audit services.¹²²

General description of the sector and related products or activities

Accountancy services include regular bookkeeping of business transactions, compiling annual accounts or annual reports, making tax declarations and signing off on declarations. Accountancy services in this chapter are regarded as those services not performed by an authorised or approved auditor (see also under section 7.18 Authorised or approved auditors or registered audit firms). The services include the provision of due diligence for business acquisitions, internal audits and statutory reviews of financial reports. The latter includes auditing regarding certain housing associations.

The title "accountancy and audit consultants" is not all-inclusive. It also applies to auditors who are not authorised or approved. It means that anyone can use these titles, regardless of training, experience or formal skills. There are two main trade associations within the accountancy and audit industry. An accountancy and audit consultant can opt to become authorised by one or both organisations and follow their recommendations. Accountancy and audit consultants have unique insight into their customers' transactions and can detect suspicious transactions, along with suspicious behaviour.

The Swedish Companies Register for money laundering had a total of 13,155 obliged entities providing accountancy and audit services as of 31 December 2024. Of those, 9,731 (74%) stated that they only run reportable activities. The remaining 3,424 obliged entities in the register stated that they also run other activities under the supervision of the County Administration Boards. Such activities can include tax advice. There is likely a large hidden number of obliged entities subject to the AML act, but who are not registered with the Swedish Companies Register for money laundering.

Money laundering – description of the risk scenario including known approaches

An accountancy and audit consultant can be used in a money laundering scheme, to provide false documentation and invoices, for example. The consultant can be unaware of this, knowingly ignore it or actively taking part as a facilitator, e.g. as a PML. Services from accountancy and audit consultants are regarded as easily accessible and can be a key function for criminal networks when they do not have such expertise themselves.

¹²² Chapter 1, section 2(1), para. 19 of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

Inadequate awareness encourages crime

Inadequate customer due diligence or failure to understand the customer's business can lead to accountancy and audit consultants not detecting transactions that ought to be suspicious and reported to the FIU. They can involve:

- money from criminal activities being booked as sales and then withdrawn as legal in the form of wages and dividends
- money comes into the company bank account for no reason. The company is asked to refund it (the payer cites accidental payment) but pays to another account than the one it came from
- the obliged entity observes a large transaction coming in to a customer's account without any documentation to indicate where the money comes from
- unknown payments from or to countries with high risk of money laundering
- false invoices
- reverse money laundering, in which legal money is made illegal through false invoices paid to the invoice beneficiary who then withdraws the money in cash to pay for black labour, for example.

Facilitators and professional money launderers assist criminal networks

Companies are a major means of running more complex money laundering. Persons providing professional accounting and audit services often have insight into a large number of companies and groups. This can contribute to their function and capability as potential facilitators and PMLs, as they can handle accounts for several companies within the same criminal scheme to conceal money laundering.

An accountancy and audit consultant acting as a PML can, for example, perform the regular bookkeeping or year end accounts for a company on false grounds, or create false documents that give a credible impression, such as convincing annual report. False invoices and documents used to verify a transaction can be used to conceal money laundering transactions or over-value assets, or in some other way support the activities of criminal networks. There are also examples of accountants or executives collaborating with auditors in criminal schemes. The information provided by the accountant means the audit and review of the company can be manipulated, for example, on the question of where random sampling is performed.

Trust accounts exploited

Audit firms and neobanks with accountancy services can offer trust accounts to their customers. The audit firm can hold the trust account instead of the company and its officers being named as the account holders. For example, there are neobanks with accountancy services and who offer trust accounts to their customers with other banks.

A combination of services offered

Some companies combine different services, making them attractive to risky customers. Examples of combined services:

- neobanks offering accountancy services
- integrated accounting and payment solutions, e.g. an accountancy firm with factoring¹²³ and payment services.

¹²³ Factoring is a financial service in which a company sells to or borrows against its invoices via a finance company or bank.

Threats – money laundering

Scope

The sector is the biggest under the supervision of the County Administration Boards. Because the provision of accountancy and audit services does not require a licence or authorisation, the range of people providing such services is wide and there is a risk of shady operators amongst them. It is also common that audit firms have customers within industries known for being more exposed to financial crime than others, such as the construction and catering industries.

The new Confiscation Act¹²⁴ which came into effect on 8 November 2024 gives law enforcement authorities a new means of confiscating the assets of criminal actors. This can lead to changes in approaches. The ability of the criminal actors to boost a legal income will be decisive. For example, the scope of false or forged certificates and documents could increase, along with false signatures and retrospective dates. Because this is something that facilitating accountancy or audit consultants can help with, the sector's service can be in demand to a large extent for money laundering purposes.

Threat actor capabilities

Some ability and capability is needed for money laundering in the sector. When accountancy and auditing consultants act as PMLs, they can contribute with criminal schemes and knowledge to conceal criminal activities in the accounts of their customer companies. This can make accountancy errors hard to detect retrospectively, and conceal money laundering transactions. PMLs with knowledge of the rules for accountancy and auditing can also react quickly to changes in the law, market dynamics and law enforcement measures.

Anonymity

Obligated entities in the sector obtain certain details on their customers when entering into a contract with them. Some transactions performed can be traced, making it harder to remain anonymous. Even though most obliged entities claim that they perform customer due diligence procedures, a large number of them do not. This implies increased risk of threat actors being able to act anonymously.

Summarising assessment

In summary, the threat of money laundering in the sector is deemed to be high, as accountancy and audit services can represent an important part of money laundering schemes. Accountancy and auditing consultants acting as PMLs can conceal criminal activities in the accounts of their customer companies – a significant function widely used by companies for large scale money laundering.

In conclusion, the threat regarding money laundering in the sector is deemed to be high.

Vulnerability – money laundering

The chances of detection

Many large companies are present in the sector, but smaller firms are also common. A number of obliged entities have long-term customer relationships and monthly contact with their customers.

Risk awareness and knowledge of the AML regulations is generally good within the sector. During 2024, the FIU received 140 SARs from accountancy and auditing services. This is a clear increase compared to previous years (six SARs were received in 2020), but there are still deemed to be relatively few reports in relation to the size of the sector.

Several obliged entities are not aware that they are subject to the AML act, which indicates that they lack awareness of the risks inherent in the sector and how their companies can be exploited for money laundering. Another vulnerability is that the sector is diverse and is spread over large geographic areas.

¹²⁴ See chapter 36 of the Swedish Criminal Code (1962:700).

Compliance

The County Administration Boards identify non-compliance in the majority of their supervisory inspections.

In a survey conducted in conjunction with the last sector report, almost half of the obliged entities in the sector stated that they had performed risk assessment of their business. The County Administration Boards can conclude from their inspections that few obliged entities considered all the factors in their risk assessment, and that they therefore do not fulfil the requirements of the act.

Summarising assessment

The sector has low awareness of which risks of money laundering there are, and has limited awareness of the AML act. The low number of SARs to the FIU reinforces this picture. Many obliged entities have also be found to conduct adequate or complete customer due diligence procedures, which is why vulnerability to being exploited for money laundering is increasing. There are also a large number of obliged entities who registered with the Swedish Companies Register for money laundering, and which therefore have low awareness of their obligations according to the act and how they can be exploited for money laundering schemes.

In conclusion, the vulnerability to money laundering in the sector is deemed to be significant.

Risk – terrorist financing

Accountancy and auditing firms are exploited as part of money laundering with the objective of terrorist financing. Corporate structures of varying complexity are used to issue false invoices and create false documentation. The problems described in the section on money laundering are therefore relevant, including for terrorist financing.

7.20 Tax advisers

Overall sector risk:



The sector covers natural and legal persons providing professional advice on taxes and duties.¹²⁵

General description of the sector and related products or activities

The provision of advice on taxes and duties includes, for example, calculating and reporting taxes that affect companies, owners and private individuals, along with analysing, interpreting and advice on tax rules.

There is one trade association for tax advisers. Tax advisers can opt to be authorised by their trade association, which means that the association's recommendations must be followed.

Tax advisers have a unique insight into customer transactions and corporate structures and ought to be able to detect suspicious transactions or suspected ownership structures. Tax advisers and others giving tax-related advice which is international must report to the Swedish Tax Agency in accordance with the Act on Reportable Arrangements (2020:434).

The Swedish Companies Register for money laundering contained 3,418 companies as of 31 December 2024. Of those, 74 (2%) have stated that they only provide tax advice. The remaining 3,444 obliged entities in the register stated that they also run other activities under the supervision of the County Administration Boards.

Tax adviser is not a protected title, and there is likely a large number of unauthorised practices. Assessment of the sector is also subject to a problem with limitation, as not only tax advisers provide tax advice. Tax advice is also a service included with other services and consultancy which can be offered by independent legal practitioners, auditors, accountancy consultants and lawyers, for example.

Money laundering – description of the risk scenario including known approaches

Tax advisers can be exploited under tax schemes in which money from criminal activities is fed into the legal system. Money laundering within the sector can occur when a tax adviser is unaware of money laundering being involved, is aware of but chooses to ignore it, or is directly involved and acts as a PML.

Creating complex corporate structures

Tax advisers can be involved in money laundering and tax schemes, but can also assist with tax planning. They can be involved and create complex corporate structures containing several companies with obscure activities, and postbox companies in low taxation countries. Examples include several similar companies with the same activities, which obscures the possibility of tracing the source of the money. There can be large groups engaged in a wide range of activities, etc. This cluster of companies is hard to analyse for the authorities, as a large number of companies, actors, straw men and accounts with different banks in different countries and registrations in low tax jurisdictions (tax haven) can be involved. "Front companies"¹²⁶ and their bank accounts are also involved (see also under section 7.1 Bank and financial institutions).

¹²⁵ Chapter 1, section 2(1), para. 20 of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

¹²⁶ Front companies are referred to as invoicing companies. Front companies can be used in different ways, such as money passing through their accounts, as an administrative function to issue invoices or certificates, or as agencies for temporary employment.

Central role in underground banking

Tax advisers are used in underground banking (see also chapter 2), in criminal schemes involving money laundering and tax avoidance in parallel.

Threats – money laundering

Scope

A tax adviser must have specialist knowledge of tax law, know how the Swedish Tax Agency's checks work and which countries it is strategically right to place money in. This type of expertise is attractive to threat actors who need large scale money laundering. Large amounts can be laundered through complex, international schemes that are hard for the authorities to investigate.

Threat actor capabilities

Threat actors laundering money with the help of the sector are natural or legal persons with capital and profits they do not want to be taxed in Sweden in whole or part. Threat actors may need some understanding of finances and the ability to create false documentation of various types to give an apparent explanation to transactions made to conceal tax avoidance. Tax advisers have also been found to act as PMLs, in criminal schemes involving money laundering and tax avoidance in parallel.

Anonymity

Customer due diligence procedures must be conducted before a business relationship can be started, but this is not always done. In such instances, the threat actor can act anonymously through legal persons with complex ownership structures, which makes it hard for obliged entities to identify the beneficial owner.

Summarising assessment

Using tax advisers, large amounts can be laundered through complex, international schemes that are hard for the authorities to investigate. The threat actor is likely a person with a lot of capital. The person has funds that need to be transferred through tax transactions at a low or zero tax rate. Tax advisers have specialist knowledge of tax law, know how the Swedish Tax Agency's checks work and which countries it is strategically right to place money in. Complex ownership structures can provide anonymity. The adviser's expertise is attractive to threat actors who need large scale money laundering. There are tax advisers who are PMLs and knowingly take part in criminal schemes involving money laundering and tax avoidance.

In conclusion, the threat regarding money laundering in the sector is deemed to be high.

Vulnerability – money laundering

The chances of detecting money laundering

In a survey conducted in conjunction with the last sector report, almost half of the obliged entities claimed that they had performed customer due diligence in issues concerning their customers. The fact that customer due diligence and checks of the financial circumstances of customers is not performed on all their customers reduces the chances of detecting money laundering and thus increases the risk of money laundering in the sector.

Compliance

The fact that a large number of obliged entities do not perform any customer due diligence procedures indicates inadequate understanding of the requirements of the law. This implies increased vulnerability to being exploited for money laundering. It can also mean that obliged entities do not report suspected money laundering to the FIU, as reflected in the low number of SARs received from tax advisers. Four SARs were received by the FIU in 2024, which is the same number as in 2020. Some tax advisers are likely aware of the duty to report, but deliberately opt to not report suspected money laundering.

Summarising assessment

There is a lack of awareness of the requirements set by the law. This can increase the risk of obliged entities being exploited for money laundering and that they do not report suspected money laundering. Only a handful of SARs are received annually by the FIU from tax advisers, which indicates a lack of awareness or deliberate avoidance of reporting. Because the title of tax adviser is not protected, and given that it is not only tax advisers offering tax advice, the chances of adequate supervision are affected. It also becomes harder to direct information to and increase awareness and knowledge level in the sector.

In conclusion, the vulnerability to money laundering in the sector is deemed to be significant.

Risk – terrorist financing

There is no known method by which the sector is used for terrorist financing in Sweden at this time. No international surveys have been conducted. But it should be mentioned that a potential risk is that false invoices can be used for terrorist financing.

7.21 Lawyers and law firms

Overall sector risk:



Lawyers and law firms are covered by the AML act when they perform certain services.¹²⁷ For example, when a lawyer acts in a client's name for financial or property transactions. It can also concern planning or execution of transactions at a client's expense.

General description of the sector and related products or activities

Supervision by the Swedish Bar Association

The Swedish Bar Association is obliged to effectively monitor and take the necessary measures to ensure that the law is followed. The supervisory function has to ensure compliance with the law, and that lawyers and law firms have the training, administration and procedures required. For example, procedures must be in place at law firms covered by the law for customer due diligence, reporting, retention of details and documents, internal audits, risk assessment, risk management and communication.

The Swedish Bar Association strengthened its supervisory function in 2024 according to the AML act by setting up a special supervisory unit which is organisationally separate from the rest of its activities. Investigation of the compliance of lawyers and law firms with the AML regulations has been separated from other proactive supervision and is managed separately. The setting up of the special unit has meant that the range of lawyers and law firms that have become the object of money laundering supervision has grown. The investigations are now made from an even more risk-based perspective, which means supervision is aimed at the areas and activities where the risk of money laundering is deemed to be highest.

In contrast to other supervisory authorities, the Swedish Bar Association has no obligation to inform the FIU if circumstances are detected that could be assumed to be linked to or could comprise money laundering when checking a law firm or in some other way.¹²⁸

Monitoring authority over the Swedish Bar Association's money laundering supervision

According to the EU's sixth money laundering directive, supervision conducted by a self-regulating body must be monitored by an authority in the future. A researcher was tasked with providing suggestions as to which authority should be given monitoring authority over the Swedish Bar Association's money laundering supervision. The investigation, entitled Money Laundering Investigation 2022¹²⁹ proposed that the Attorney General should be appointed as this authority. The Attorney General is to check that the Swedish Bar Association looks after its money laundering supervision function and can notify the association if the authority detects breaches. The investigation also suggested that the Attorney General should inform the FIU if the authority detects breaches that comprise crimes in the execution of its duties. The new law will come into effect in three years from the date on which the directive comes into effect.

127 Chapter 1, section 2(1), para. 21 and section 4(1) of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

128 According to chapter 4, section 4 of the AML, supervisory authorities shall inform the police (the FIU) if they detect during inspections or in some other way identify circumstances that could be assumed to be linked to or could comprise money laundering or terrorist financing. However, the obligation to inform only covers authorities and not the Swedish Bar Association as a private law supervisory body.

129 New regulations to combat money laundering and terrorist financing, SOU 2024:58.

Key figures	
Number of law firms	1 988
Swedish associate lawyers at law firms	2 656
Active Swedish lawyers (excluding 23 so-called "EU lawyers", who practice in Sweden under the title of their homeland)	6 694

Source: The Swedish Bar Association

Money laundering – description of the risk scenario including known approaches

Services provided by lawyers can be used as part of a money laundering scheme. A lawyer can be unaware of this, knowingly ignore it or actively taking part as a facilitator, e.g. as a PML.

Fictive reasons for transactions

In some instances, fictive reasons for transactions have been used to conceal the real background to a money flow. For example, a corporate structure is fictitious within the framework of an otherwise legal and "normal" structure. In such instances, it is important that the lawyer understands each transaction, measure or circumstance within the framework of the assignment to be able to prevent the business being exploited for the purpose of money laundering.

Fictive legal disputes

A fictive legal dispute is used as the reason to obtain a judgement or ruling that means money can be claimed and moved from one actor to another through the auspices of the authorities. The transfer then appears to be legitimate and the money launderer can demonstrate the source of the money.

Money laundering through corporate structures

Large scale money laundering often arises from corporate structures and threat actors can use lawyers to create such structures, which are then used for money laundering or to conduct transactions that seem legal. It is also possible that lawyers sitting on boards of directors represent a new risk scenario. A lawyer could be appointed to a board of directors to prevent criminal investigations, as a lawyer's duty of confidentiality can, in some circumstances, prevent the police and prosecutors from conducting house searches and telephone bugging relevant to the company documents held by the lawyer.

An anonymised example of a lawyer's role is described below.

The lawyer has been a board member in several companies involved in various money laundering schemes. He has opened a trust account for one company through his law firm which received about SEK 60 million from a foreign company. The money was then forwarded to companies in other countries via the trust account.

Facilitators and professional money launderers

According to Europol, criminal networks exploit legal structures – such as shell companies and startups – to a large extent to conceal assets and launder money. In some instances, professionals, including lawyers, play a role in helping to set up or maintain such structures.¹³⁰ Sweden is no exception.

Intelligence confirms that lawyers act as PMLs serving organised crime in money laundering schemes. An anonymised example of a lawyer's role as a PML with links to criminal networks is shown below.

A has been popular and highly-regarded as a lawyer. He is deemed to be an integrated part of the Swedish gang underworld, and criminal networks have used his services for criminal purposes. A has handled pre-investigation assignments and laundered money via cryptoassets. A has been active in several industries and has sat on several boards.

¹³⁰ EU Socta 2021 – *Serious and Organised Crime Threat Assessment. A corrupting influence: The infiltration and undermining of Europe's economy and society by organised crime.* Europol, 2021.

Trust account

A lawyer is obliged to keep money and other assets belonging to a client or beneficial owner separate from the company's own funds using a trust account. Client funds are only used for disbursements to the client or on the client's behalf to cover expenses and for fees. The account can be opened in the name of the lawyer or the client.

According to the guidelines of the Swedish Bar Association, lawyers and law firms are instructed to avoid using trust accounts as far as possible. If it is necessary for the execution of an assignment, there must be clear procedures concerning their use to check transactions and deal with risks. However, the use of trust accounts by lawyers still represents a risk factor and is a known method used in money laundering. Trust accounts can be used to conceal criminal proceeds, but can also be a means of integrating them into the legal financial system through complex legal corporate structures and complicated transactions that are hard to detect. Client confidentiality entails that lawyers cannot provide information to a bank on to whom the funds in a trust account belong without the client's consent. Client confidentiality is a circumstance that makes lawyers attractive as possible PMLs.

An anonymised example of how a lawyer has used a trust account for property-related transactions in a money laundering scheme is described below.

A lawyer at a large law firm is responsible for a trust account that belonged to a number of Swedish companies in the property market, controlled by a Swedish citizen. The account has been used to receive transactions from foreign companies. The transactions are then forwarded to an account abroad that belongs to the Swedish citizen. The same Swedish citizen also owned the foreign companies.

Trust account risk indicators

Risk indicators of a trust account being used for money laundering:

- transactions to and from high risk countries or tax havens
- property-related transactions, especially when linked to high risk countries or tax havens
- transactions refunded to the sender shortly after being deposited, which can indicate a deliberate part payment to create legitimacy.

It is imperative that the bank knows which type of industry the lawyer or law firm is active within, to be able to understand how much money can be expected to be reasonable in the trust account. The lawyer must naturally also be alert when transactions are requested via the trust account, and transactions that alone or collectively look unreasonably large in relation to their purpose and nature, or in relation to the depositor's financial resources, should be investigated or denied.

Threats – money laundering

Scope

Europol has highlighted the problem of lawyers helping criminals with advice on money laundering and creating legal structures. Such structures can create the preconditions for large scale money laundering, but the total scope in the sector is hard to assess.

The Swedish Bar Association does not have any dedicated reporting or information obligation to the FIU. Only lawyers and law firms have that obligation. As stated above, the Money Laundering Investigation 2022 also suggested that the Attorney General should inform the FIU if the authority detects breaches that comprise crimes.

The number of SARs made to the FIU from lawyers is very low. Two reports per year were received between 2020-2024. Similarly, very few SARs come from banks on issues concerning lawyers' accounts. The very low level of reporting to the FIU bears no comparison to the high risk of trust accounts held by lawyers being associated with the flow of intelligence, for example. According to the Swedish Bar Association, there are natural reasons for the low reporting frequency from lawyers.

Anonymity

Lawyers have an obligation to conduct detailed investigations for adequate customer due diligence before starting on the main parts of an assignment. According to best legal practice, a lawyer must not accept an assignment if there is a conflict of interest or realistic risk of the same. This implies that the lawyer must conduct detailed disqualification testing before accepting the assignment, obtaining information on the client, the counterpart and the assignment. These circumstances, combined with the close relationship between client and lawyer, along with the special legal skills of lawyers, mean that it is deemed to be hard for actors to remain anonymous. But for complex and large scale money laundering schemes, it can be difficult to exclude that a highly capable threat actor can still conceal the actual client.

As mentioned earlier, the use of trust accounts can imply better chances of anonymity through the bank.

Threat actor capabilities

The approaches of organised crime to infiltrate the legal structure have been refined and are harder to detect. The majority of criminal networks have access to companies and structures in which the upper levels of the hierarchy have the ability to plan, initiate and complete complex transactions to conceal the source of the money. Highly capable threat actors can approach lawyers and get help with legal advice or assistance. Examples include setting up a complex corporate structure which can then be exploited for extensive money laundering.

The risk of threats and other unauthorised influence from organised crime with a lot of capital makes the sector vulnerable. Given the close relationships between client and lawyer, there is a risk that lawyers decide to ignore any suspicions of conduct transactions on their clients' behalf.

Summarising assessment

The approaches of organised crime to infiltrate the legal structure have been refined and are harder to detect. This development makes higher demands of alertness and risk preventive measures. The skills and services the sector can offer are attractive to criminals who need to handle and launder money from large scale criminal activities. Given the risk of violence within organised crime, the sector risks being exposed to pressure. Intelligence also confirms that lawyers actively act as facilitators for money laundering.

In conclusion, the threat regarding money laundering in the sector is deemed to be significant.

Vulnerability – money laundering

The chances of detecting money laundering

One explanation for why the sector detects and reports money laundering to such a low degree, can be that sophisticated actors are involved with advanced approaches that are hard for lawyers to spot. Money laundering in the sector is deemed to mainly occur in large and complex business transactions, which are extensive and complicated by their nature. Multiple companies or legal persons are often involved. The reasons for the transactions and question of the beneficial owner can be complicated to assess. But lawyers also have good chances of detecting irregularities of varying types, thanks to being legal experts.

Unless adequate customer due diligence procedures are in place, the chances of detecting money laundering are reduced. Lawyers must therefore investigate who is the beneficial owner and analyse the actual objective of the assignment. If they fail to conduct these checks and analyses adequately, they can represent a vulnerability.

Another reason for the low degree of reporting from the sector can be that in certain instances, lawyers are exempted from reporting according to the AML act. The reason for the exemption is the independent, loyalty and statutory duty of confidentiality lawyers have in relation to their clients.¹³¹ Something else that could affect the degree of reporting, is that there is no express requirement to report to the FIU if an obliged entity refrains from entering into a business relationship due to a customer

131 SOU 2016:8 p. 299.

failing to pass customer due diligence procedures, even though reporting must then be considered. On the other hand, if the lawyer has reason to suspect that the client intends to use his services for such purposes, a report should be made.¹³²

There can be instances of money laundering not being reported to the FIU despite it being known to the lawyer. This is deemed to be the biggest vulnerability in the sector, as information on non-conformity is not passed on to the law enforcement authorities who can act on it. This reduces the chances of combating money laundering.

In its role as the supervisory body, the Swedish Bar Association is not obliged to report suspected money laundering to the FIU, which is a vulnerability in itself. That is why the reporting of suspicions by bankers, auditors and other obliged entities about trust accounts held by lawyers is extra important. Few lawyers are the subject of SARs made to the FIU.

Breaches of the AML act can lead to various types of intervention. The disciplinary board of the Swedish Bar Association can, if it has reason, pass on a case to the County Administration Boards for considering a fine.¹³³ Between 2016-2024, the Swedish Bar Association started 431 cases which also included ethical requirements and other legal requirements pertaining to lawyers.¹³⁴ In the same period, the Swedish Bar Association submitted no cases to the County Administration Boards.¹³⁵ Three cases were submitted to the County Administration Boards in 2025.

The Swedish Bar Association plays a key role in detecting irregularities and combating participation by lawyers in money laundering. It is vitally important that the association's supervisory function is adapted to the risks the industry is associated with.

The fact that the association is not an authority, compared to other supervisory functions, does imply certain limitations, including the issue of information sharing. For example, the possibility of collaboration according to chapter 4a of the AML act.

Compliance

The duty to report conflicts with the core values of lawyers, namely the duty of loyalty. Loyalty to the client is the primary duty of lawyers. It can only be broken by the law, for example the obligation to report according to the AML act and best legal practices. But there is nevertheless a risk that lawyers fail to report despite the AML, with reference to their duty of loyalty.

If a lawyer has reported suspicious activity regarding a client to the FIU, he is obliged to immediately relinquish the case.¹³⁶ This is the business interest that affects the refusal to report.

With the introduction of the supervisory unit and increased resources, the number of investigations conducted has increased considerably. That implies greater chances to detect breaches that can be corrected or lead to disciplinary action, and can contribute to increased compliance in time. Five cases were referred by the Disciplinary Board regarding alleged infringements in 2024. Investigations by the Swedish Bar Association in 2024 showed that most law firms had established and working procedures for combating money laundering. A requirement also developed at a general level, especially amongst small and medium-sized firms, to increase awareness of the risks that can arise in the business, and to strengthen the systematic and integrated work of managing them.¹³⁷

Summarising assessment

Despite lawyers being exploited for money laundering, few SARs were received by the FIU from the sector. This can partially be due to sophisticated criminals and complex schemes being involved, encompassing many legal persons. It can be hard for lawyers to perceive the intention of transactions and who is the beneficial owner. The low degree of reporting can also be due to lawyers being exempted in some instances from the duty to report with regard to their obligation to be independent, loyal and confidential. Neither are there any express requirements to report in instances when a lawyer

¹³² Prop. 2016/17:173 p. 292.

¹³³ Chapter 7a section 6(2) of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

¹³⁴ The Swedish Bar Association, obtained 09.01.2024.

¹³⁵ County Administration Boards, obtained 03.02.2025.

¹³⁶ This is pursuant to the Legal Rules on Ethics (3.4.2, fourth paragraph *Recommended Rules on Best Legal Practice*).

¹³⁷ <https://www.advokatsamfundet.se/for-vara-ledamoter/tillsynsenheten2/nyheter-tillsynsenheten/advokatsamfundets-tillsynsenhet-har-granskat-hur-advokatbyraer-efterlever-penningtvattslagen/>

has refrained from entering into a business relationship due to inadequate customer due diligence. Yet another vulnerability is the fact that the supervisory body does not have any obligation to report suspected money laundering to the FIU. This vulnerability will probably be less important if the proposal that the Attorney General should control the Swedish Bar Association's supervisory function is adopted.

In conclusion, the vulnerability to money laundering in the sector is deemed to be significant.

Risk – terrorist financing

In contrast to other supervisory authorities, the Swedish Bar Association's supervisory function has no obligation to inform the FIU if circumstances are detected when checking a law firm or in some other way that could be assumed to be linked to or could comprise terrorist financing.¹³⁸

There is no known method by which the sector is used for terrorist financing in Sweden at this time. No international surveys have been conducted. The sector's risk of terrorist financing has therefore not been assessed.

¹³⁸ According to chapter 4, section 4 of the AML, supervisory authorities shall inform the police (the FIU) if they detect during inspections or in some other way identify circumstances that could be assumed to be linked to or could comprise terrorist financing. However, the obligation to inform only covers authorities and not the Swedish Bar Association as a private law supervisory body.

7.22 Independent lawyers

Overall sector risk:



This sector covers the independent lawyer activities of independent lawyers who are not lawyers or who have a law firm. The title of independent lawyer is not protected. It implies that who may call themselves an independent lawyer is not regulated by law.¹³⁹

General description of the sector and related products or activities

The profession includes services involving acting in a client's name for financial transactions or property transactions. It can also concern helping when transactions are planned or executed (at a client's expense) when buying or selling properties or businesses. Other services can include administering a client's money, securities or other assets, opening or administering bank, savings or securities accounts, obtaining the necessary capital to form, run or manage a company and to form, run or manage a company, association, fund or trusts and similar legal constructions.

The Swedish Companies Register for money laundering had a total of 941 obliged entities stating that they provided "legal services" as of 31 December 2024. Of those, 298 (approx. 31%) stated that they only run reportable activities. The remaining 643 obliged entities in the register stated that they also run other activities¹⁴⁰ under the supervision of the County Administration Boards.

Money laundering – description of the risk scenario including known approaches

With the help of financial transactions, an Independent lawyers can contribute to money laundering by moving illegal funds and getting them to seem legitimate. This can involve a range of more or less complicated money laundering schemes. An independent lawyer can be unknowingly exploited in a money laundering context, be aware of what is happening but deliberately ignore or actively partake in money laundering by acting as a professional money launderer (PML). According to Europol, independent lawyers help criminals with fraudulent schemes and advice on how to set up shell companies and startups, for example, to launder money.¹⁴¹ Sweden is no exception.

Knowledge of financial regulations and legal structures

An independent lawyer can contribute knowledge of financial regulations and legal structures to legitimise criminal money, or create corporate structures to conceal money laundering. Setting up corporate structures in Sweden, starting offshore accounts or funds, advising on how complex transactions can be conducted can all be involved.

Trust account

Independent lawyers can have trust accounts to conduct transactions on a client's behalf, e.g. for financial transactions or property transactions, or to administer funds during a dispute. These accounts can be used to conceal criminal proceeds, but can also be a means of integrating them into the legal financial system by transferring them to the final recipient via the trust account. This conceals the original sender and tracing of the transaction is made harder.

¹³⁹ Chapter 1, section 2(1), para. 22 of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

¹⁴⁰ Including as trust managers, as the opportunity to register in this category only became available from the Swedish Companies Register in August 2023.

¹⁴¹ EU Socta 2021 – *Serious and Organised Crime Threat Assessment. A corrupting influence: The infiltration and undermining of Europe's economy and society by organised crime*. Europol, 2021.

Conciliation as an apparent explanation

Independent lawyers can take part as a representative in disputes, and can, for example, propose conciliation between two parties. The parties can then opt to have the conciliation settled in court. In this way, a transfer that seems legitimate and the ratified conciliation give an apparent explanation for the transaction. The transaction can, in fact, be the result of some other crime, such as extortion, but can also be a money laundering transaction. Conciliations are often subject to confidentiality by the parties to further obscure insight.

Threats – money laundering

Scope

The title of independent lawyer is not protected, and many independent lawyers offer other services, such as accountancy and auditing, tax advice or company formation.

SARs from the sector to the FIU are low, six were received from paralegals in 2024. When an independent lawyer is the threat actor themselves, it is the responsibility of the banks and other obliged entities to submit an SAR. Despite the risks of trust accounts being used for money laundering, very few independent lawyers are reported to the FIU for suspected transactions from their trust accounts.

Intelligence confirms that independent lawyers act as PMLs. But in common with PMLs, little information is available and there is a large unknown number. It is therefore hard to detect to what extent the sector is exploited for money laundering.

Threat actor capabilities

No major capability is needed for money laundering in the sector. An independent lawyer is often cheaper to use than a lawyer. It was also reported in the last sector report that a significant proportion of independent lawyers do not investigate where their clients' money comes from. There are no indications of the situation having changed. Independent lawyers can thus be unknowingly exploited in a money laundering context, or deliberately ignore what is going on. Intelligence also confirms that independent lawyers are actively acting as facilitators and assisting clients in money laundering schemes, for example, by giving advice on how to set up a shell company and foundations to launder money. Such PMLs can be highly capable.

Anonymity

Obliged entities in the sector obtain certain details on their customers when entering into a contract with them. Even though most independent lawyers claim that they perform customer due diligence procedures, a large number of them do not. This implies increased risk of threat actors being able to act anonymously.

Summarising assessment

Intelligence confirms that there is considerable demand from criminal actors for legal skills and that money laundering is facilitated in the sector to a much larger extent than what reporting to the FIU indicates. Independent lawyers can thus be unknowingly exploited in a money laundering context, but also actively assist criminal networks in money laundering schemes.

In conclusion, the threat regarding money laundering in the sector is deemed to be high.

Vulnerability – money laundering

The chances of detection

Awareness of the risks and knowledge of the AML regulations was deemed to be low in the sector in the last sector report. It was reported that a significant proportion of paralegals do not investigate where their clients' money comes from. There are no indications of the situation having changed.

Independent lawyers have generally not considered all the risk factors in their standard risk assessments. It can therefore be stated that many independent lawyers are not fully aware of the requirements and obligations of the law.

Another vulnerability is that the sector is diverse and is spread over large geographic areas. Furthermore, independent lawyers are sometimes engaged in cases that also involve other professional categories, which makes supervisory responsibility less clear and risks that they fall between two stools. This is an obvious vulnerability.

Compliance

The County Administration Boards identify non-compliance in the majority of their supervisory inspections. However, the scope of their supervision has been limited. The hidden number of independent lawyers not on the Swedish Companies Register for money laundering is deemed to be high. There can therefore be independent lawyers running legal businesses but who do not believe they are subject to the AML act, or are not aware that they are.

Independent lawyers have also stated previously that the low number of SARs submitted to the FIU is due to uncertainty on whether suspected transactions really do concern money laundering. This indicates that their awareness of what is required for reporting is generally low.

Summarising assessment

Adequate customer due diligence along with awareness of risks and approaches are key factors for adequate monitoring. The sector has low awareness of which risks of money laundering there are, and has low awareness of the AML act. Several independent lawyers do not perform any comprehensive risk assessment of their business, nor do they apply adequate customer due diligence procedures. Such failures comprise considerable vulnerability and enhanced risk of the sector being exploited for money laundering. Suspicious activity reporting is very low.

In conclusion, the vulnerability to money laundering in the sector is deemed to be significant.

Risk – terrorist financing

There is no known method by which the sector is used for terrorist financing in Sweden at this time. No international surveys have been conducted. The sector's risk of terrorist financing has therefore not been assessed.

7.23 Trust Administrators

Overall sector risk:



The sector includes obliged entities running activities regarding services such as trust management or similar legal constructions.¹⁴²

General description of the sector and related products or activities

A trust implies that someone administers a property at someone else's expense. It is a legal construction in which the founder's right of ownership is transferred to an administrator in a prescribed manner. The administrator is obliged to handle and control the property according to the provisions in trust deed. Administration is exclusively conducted to the benefit of the beneficiary who has the right to use the property. Remuneration for administration expenses comes from the property or the returns it generates.

Trusts do not have any legal capacity (the benefit of rights and duties) and are a phenomenon mainly found within the Anglo-Saxon countries. Trusts are not found for legal purposes in Sweden, but can be used in the country.¹⁴³ The Swedish regulations apply to international activities run by Swedish companies or foreign companies established in Sweden.

The services can be offered professionally by natural and legal persons. The administrator is often a limited partnership in which the administrator is the general partner with unlimited liability. The general partner manages the trust's assets, which are often placed via offshore accounts¹⁴⁴. The assets can be anything from cash funds and securities to properties and cryptocurrencies.

There are no exact statistics for how many businesses are run under the definition of trust manager. The Swedish Companies Register for money laundering had a total of 25 obliged entities stating that they were trust managers as of 31 December 2024. But some of the sector's obliged entities can be found in the Swedish Companies Register for money laundering category of legal services instead. This is due to the possibility of reporting the business as a pure trust manager only became available in August 2023.¹⁴⁵ There were 98 limited partnerships listed under the group of legal services in 2024, that were found to manage trusts, foundations and the like when compared to the register of businesses.

Money laundering – description of the risk scenario including known approaches

There is no information on known approaches used.

Threats – money laundering

Opportunities for running money laundering in the sector

A trust has no legal capacity and is not found for legal purposes in Sweden. Trust managers can be found in Sweden – above all, the trust's address can be in Sweden – and therefore comes under the supervision of the County Administration Boards. The actual trust is always abroad. This is one of several reasons why

¹⁴² Chapter 1, section 2(1), para. 23 and section 4(2), para. 4 of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

¹⁴³ Prop. 2016/17:173, Additional Measures against Money Laundering and Terrorist Financing, p. 459.

¹⁴⁴ An offshore account is a bank account opened in a country or jurisdiction different to where the account holder is resident or runs their business.

¹⁴⁵ The number of trust managers concerning obliged entities who reported their activities to the Swedish Companies Register after August 2023, when the opportunity to specifically state trust management as a business was introduced. There can also be obliged entities who registered before August 2023, but under other categories.

the authorities' knowledge of the sector is very low. Another reason is that the area has not had adequate supervision and that the FIU has received no SARs from the sector's obliged entities. But it is evident that high specialist skills are needed to run money laundering within the sector.

To start a money laundering scheme takes time, as the setup is advanced, but once in place, assets can be rapidly transferred. Legal persons are exclusively required to conduct money laundering in the sector, and the presence of cash funds is very low. Assets are transferred usually via bank transfer and obliged entities state that payment can also be made in electronic currencies.

Anonymity and traceability

Threat actors can be highly anonymous in this sector. Anonymity is often cited as a benefit in materials marketing the trust as a legal construction. The County Administration Boards have found it hard to contact the officers when background checking them, as they are often resident abroad.

Summarising assessment

The limited knowledge the authorities have of the sector, along with the opportunity to remain anonymous, mean that the threat of money laundering is deemed to be high.

In conclusion, the threat regarding money laundering in the sector is deemed to be high.

Vulnerability – money laundering

Risk awareness

The obliged entities in the sector state that they have general risk assessment in place, and that they do conduct customer due diligence procedures. The obliged entities state that they gather information on the financial circumstances of customers, and that they provide training to their employees to a large extent. They also believe that their general knowledge level is good and that the sector is rarely exposed to money laundering. The lack of information the authorities have on the sector makes it hard to assess risk awareness. This represents a vulnerability.

In conclusion, the vulnerability to money laundering in the sector is deemed to be significant.

Risk – terrorist financing

There is no known method by which the sector is used for terrorist financing in Sweden at this time. No international surveys have been conducted. The sector's risk of terrorist financing has therefore not been assessed.

7.24 Art dealers

Overall sector risk:



Art dealing as a sector applies to professional businesses regarding the selling, storage or trading works of art, if it can be assumed that transactions are or will be conducted within the business or parts of it, individually or that can be assumed to have some connection, that involve an amount disbursed or received equivalent to eur 10,000 or more.¹⁴⁶

Art dealers were first included in the AML act in 2020 and the sector was therefore not assessed in the last sector report.¹⁴⁷

General description of the sector and related products or activities

There are various types of obliged entities within the sector, such as artists, auction houses and galleries. Trading is conducted through the buying and selling of artworks via galleries, auction houses, fairs and online platforms. Intermediaries are often used. "Artworks" are defined as paintings, serial-produced artworks, sculptures, antiques and NFT¹⁴⁸ (digital art). The definition of artworks in Swedish law is stated in the preparatory work for the AML act. It states there that artworks should concern two or three-dimensional works with artistic input and uniqueness, usually in the form of paintings or sculptures in material such as marble, plaster, bronze, ceramic, glass, silver, gold, fabrics and wood. Serial-produced artworks are also included. There are no general, widely accepted definitions of the types of objects handled within this sector at this time.

Many art dealers work with valuation and expertise around artworks, and it is common for them to have contact with collectors and artists. The art trade has a culture of discretion with regard to the identities of buyers and sellers. The industry can be international, with transactions and objects moving across borders. There is no specific regulation or authorisation for art dealers. There are a number of trade associations within the sector.

The Swedish Companies Register for money laundering had a total of 177 obliged entities stating that they provided "sales, storage and trading in artworks" as of 31 December 2024.¹⁴⁹ Of those, 148 (84%) stated that they only run reportable activities. The remaining 29 obliged entities in the register stated that they also run other activities under the supervision of the County Administration Boards. There is likely a large hidden number of obliged entities who could be classified as art dealers, and which are subject to the AML act, but are not registered with the Swedish Companies Register for money laundering.

An estimate of how many obliged entities running reportable activities without being registered is hard to do, as there is no complete register of art dealers.

¹⁴⁶ Chapter 1, section 2(1), para. 24 of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

¹⁴⁷ The Coordination Function's awareness of the number of exploited art dealers in a money laundering context is limited. The data concerning money laundering is mainly based on information from the FATF (FATF Report on Money Laundering and Terrorist Financing in the Art and Antiquities Market. February 2023).

¹⁴⁸ An NFT (Non-Fungible Token) is a unique digital access that represents ownership of a specific object, such as digital art, music or a video clip. It is registered on a block chain, which creates a digital certificate of ownership that cannot be copied or replaced. NFTs are used to verify the genuineness and ownership of digital assets, and they can be traded on digital marketplaces.

¹⁴⁹ Art dealers were included in the register in 2020.

Money laundering – description of the risk scenario including known approaches

The businesses selling high value artworks risk being exploited for money laundering. Money laundering within the sector can either be conducted when the art dealer is unaware of money laundering being involved, is aware of but chooses to ignore it, or is directly involved and acts as a facilitator.

Several of the approaches involved in art trading generally apply only to art dealers, but with the difference that art is something on which an arbitrary value can be placed.

Artworks are resold

Threat actors buy art and pay with illegally obtained funds. The art is then sold, for example to a retailer, auction house or private individual, and the money paid into an account. Artworks are goods that can be expensive and therefore consume large proceeds of crime, whilst they can be simple to store and transport. Because payment is made accessible in the threat actor's account, the money can then be converted in the legal system.

Artworks bought with the help of others

A threat actor buys artworks with the help of, for example, a family member or agent. The threat actor gives the funds to a third party and can conduct the transaction without having to reveal their identity in connection with the customer due diligence process.

Exploiting purchase on approval

An artwork is paid for in cash from criminal proceeds. The art dealer offers purchase on approval and after a few days, the work is returned. The art dealer pays the amount received into the threat actor's account or another account stipulated by the threat actor. The source of the funds is therefore concealed.

Manipulated prices

Manipulated prices involve the threat actor buying an artwork, at an auction for example, for a much higher price than seems reasonable given the value of the artwork. In such instances, it can be an indication that the purchase of the artwork is intended to transfer money between buyer and seller in a money laundering scheme.

Fake art auctions

False valuations, false art auctions or sales and international transactions are known to occur. False auctions occur when a threat actor offers art for sale at an auction, and a co-conspirator buys it using criminal proceeds. The seller of the art then received payment in their bank account via the auction house. Art dealers have been known to take part in this scheme. Postbox companies¹⁵⁰ and intermediaries are used to obscure the true owners through false documentation, false invoices, etc.

Reverse money laundering

Reverse money laundering involves a threat actor who needs cash selling artworks to dealers who pay in cash. The cash funds the threat actor gains can, for example, be used to pay black labour.

Threats – money laundering

Scope

The art trade is a sector that threat actors with a lot of capital and knowledge have access to. Money laundering in the sector can involve large amounts, as art often has high value and there are good opportunities for transferring money between countries without raising suspicion. Buying art means that the item has an existing value and that the purchase is made in cash. This allows threat actors to convert their illegally earned money and can later demonstrate that the money comes from a sale. Money

¹⁵⁰ A postbox company is registered in one country but has its main activities and management in another. They often have no physical presence such as an office and employees, and are only found as a registered entity with a postal address (a "postbox").

laundering in the sector can happen quickly, as the transactions can be performed in cash. It is also easy to move artworks across borders. But the process can also be slow, due to an artwork not always selling quickly, which limits the attractiveness of the sector for some actors.

Threat actor capabilities

Threat actors using art dealers for money laundering often have access to large sums of money and cash within the art world. This requires a certain degree of knowledge for threat actors to be able to launder money in the sector. They may need to know how to manipulate the art market and use false documents to conceal the source of the money. In some large-scale money laundering schemes, threat actors may need access to straw men or agents to purchase and sell the artworks.

Anonymity

Threat actors can conceal their identity by using intermediaries or postbox companies as buyers and sellers of artwork. It is common that complex ownership structures make it hard for art dealers to identify the actual beneficial owner behind the transactions.

A threat actor can make a cash transaction anonymously, which obscures traceability. In other words, a threat actor can use the sector to launder money with no major risk of detection. A threat actor can also use straw men to remain anonymous. Certain parts of this market customarily deal with wealthy customers, for whom integrity and discretion are expected. The importance of integrity and discretion on the market can be regarded as an important obstacle to effectively detecting money laundering.

Summarising assessment

Threat actors are likely to be an individual or organisation with considerable financial resources. Money laundering can involve large amounts, as art often has high value and there are good opportunities for transferring money between countries without raising suspicion. Art dealing is a sector with the opportunity to trade in cash, which entails that transactions can be made very quickly and the threat actor can remain anonymous. Threat actors can also conceal their identity by using intermediaries or postbox companies. Complex ownership structures make it hard for art dealers to identify the actual beneficial owner behind the transactions.

In conclusion, the threat regarding money laundering in the sector is deemed to be significant.

Vulnerability – money laundering

The chances of detecting money laundering

Because art dealing was only included in the AML act in 2020, supervision of the obliged entities has only been in effect for a short time. This affects the level of knowledge. Customer due diligence procedures vary within the sector, and some art dealers do not follow the regulation in full to prevent money laundering. One vulnerability can be that it is hard to verify the origin and value of an artwork.

When agents are involved, it is hard to check the identity of the agent or the customer, for example, identity documents or documents to prove income can be in foreign languages or copies, and therefore hard to verify. The fact that customers will not meet the seller in person also makes it harder to conduct customer due diligence procedures.

Compliance

Some art dealers are not fully aware of the requirements set by the AML act. 12 SARs were submitted to the FIU in 2024 from the sector, which is deemed to be low.

Summarising assessment

The sector is deemed to be highly vulnerable to money laundering due to breaches in customer due diligence and compliance. The high degree of anonymity and difficulty in determining the actual value of an artwork makes detection of suspicious behaviour hard. International transactions and cash payments further increase vulnerability. Not all art dealers are fully aware of the requirements set by the AML act and few SARs are received from the sector.

In conclusion, the threat regarding vulnerability to money laundering in the sector is deemed to be high.

Risk – terrorist financing

There is no known method by which the sector is used for terrorist financing in Sweden at this time. No international surveys have been conducted. The sector's risk of terrorist financing has therefore not been assessed.

7.25 Company formation agents and business brokers

Overall sector risk:



The sector covers natural and legal persons who offer services such as forming legal persons, selling newly-formed limited companies and brokerage for Swedish or foreign legal persons.¹⁵¹

General description of the sector and related products or activities

Company formation agents offer services such as forming legal persons, selling off-the-shelf companies (companies started with purpose of being sold on) without acting as brokers buying or selling Swedish or foreign legal persons to order. Business relationships for company formation agents are deemed to mainly be short term and occur only a few times.

A business broker deals in legal persons, not off-the-shelf companies or established companies. Business brokers can be found during the entire acquisition or disposal process from company analysis and valuation, to setting up a transfer agreement.¹⁵² The sales process of a company broker lasts usually for 6-12 months. There is a trade association via which company brokers can be authorised under certain conditions.

The Swedish Companies Register for money laundering had a total of 1006 obliged entities stating that they provided company brokerage or company formation services as of 31 December 2024. Of those, 193 (19%) stated that they only run reportable activities. The remaining 813 obliged entities in the register stated that they also run other activities under the supervision of the County Administration Boards.

There is likely a large hidden number of obliged entities who could be classified as company formation agents and business brokers, and which are subject to the AML act, but are not registered with the Swedish Companies Register for money laundering.

Money laundering – description of the risk scenario including known approaches

Company formation agents and business brokers can be exploited in money laundering schemes as facilitators, either knowingly or unknowingly. They can also actively take part as PMLs.

Both offer to wind up companies quickly, but instead of winding them up, they are sold again as established companies. Established companies are companies that have been sold by their previous owners but have no activities or sales. The advantage of these companies for criminal actors is that they can be used as fronts directly, in principle, as they may still have their credit rating, approval for corporation tax, bank account, employer and VAT registrations.

This allows criminal actors to avoid new customer due diligence procedures from banks and the Swedish Tax Agency's checks for tax registration, as buying an established company requires no renewal of corporation tax approval. High risk persons with bad payment records, debt with the Swedish Enforcement Authority or previous bankruptcies gain access in this way to a functioning company, with credit rating and the necessary registrations, which can then be used for criminal purposes.

¹⁵¹ Chapter 1 section 2(1) paragraph 23 and section 4(2), paragraph 1 of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

¹⁵² Company brokers also need to take into consideration the Act on Prohibiting Legal or Financial Assistance in Certain Cases (1985:354).

Threats – money laundering

Scope

Despite there being few reported obliged entities in the Swedish Companies Register for money laundering, it is possible to launder large amounts in the sector. A purchase can be made through a single transaction, which means money can be laundered relatively quickly.

Threat actor capabilities

A threat actor can be a facilitator themselves, be helped by one or a PML and needs a good understanding of how money can be moved without obliged entities detecting any non-conformity or suspicious transactions. They also need an understanding of company acquisitions and valuations.

Anonymity

The sector handles no cash but there is a risk of money laundering upon transfer of the purchase price. If several small amounts are transferred from various bank accounts, it can be hard to detect the source of the money.

To reduce the risk of money laundering, company formation agents and company brokers need to adopt customer due diligence procedures. Out of the businesses the County Administration Boards have investigated, most of the obliged entities fail to obtain information on the customers' financial circumstances or on where the money comes from. This implies that the AML act is not being complied with in the sector.

Summarising assessment

For advanced money laundering schemes, the threat actor must have skills within several areas or the help of a facilitator. The sector is deemed to be attractive to threat actors who can remain anonymous through the acquired business. The sector allows threat actors to acquire a front in the form of a new or established company relatively quickly and at acceptable cost, which is often a prerequisite for large scale criminal activities, including large volume, advanced money laundering schemes.

In conclusion, the threat regarding money laundering in the sector is deemed to be high.

Vulnerability – money laundering

The chances of detecting money laundering

A large majority of obliged entities only adopt customer due diligence procedures occasionally, and several obliged entities concede that they do not always know where the money comes from.

During 2024, the FIU received 13 SARs from the sector, which is more than previously but still very few. The low number of SARs can partially be due to company formation agents stating another principle business, as most of them run businesses within several different areas. Many believe that there is nothing to report. One explanation for this can be lack of awareness of the approaches and risks within the sector.

Compliance

The County Administration Boards assess that many obliged entities in the sector are not sufficiently aware of the AML act, and the responsibilities they have as obliged entities. This assessment is made based on information that many obliged entities do not adopt adequate customer due diligence procedures, do not ask for information on the source of the money or take into account all the factors required to perform risk assessment of their business.

The County Administration Boards conclude from their supervision that risk assessment performed by obliged entities does not fulfil the requirements of the act.

Summarising assessment

A number of obliged entities are not aware of their responsibilities according to the AML act, and very few SARs are sent to the FIU. This implies increased risk of the obliged entities being exploited for or participating in money laundering.

In conclusion, the vulnerability to money laundering in the sector is deemed to be significant.

Risk – terrorist financing

There is no known method by which the sector is used for terrorist financing in Sweden at this time. No international surveys have been conducted. The sector's risk of terrorist financing has therefore not been assessed.

7.26 Business centres and postbox service companies

Overall sector risk:



The sector covers natural and legal persons running professional services and offering a registered office or postal address, along with cohesive services to natural or legal persons.¹⁵³

General description of the sector and related products or activities

There are obliged entities within the sector who offer company addresses with or without a physical office for a fee. The most common customer is small businesses and employees of, for example, subsidiaries without their own office. Postbox businesses can offer "digital postboxes". This entails post received being scanned and forwarded to an email address given by the customer. A postbox can provide a certain form of anonymity, which many letterbox businesses use in their marketing.

The Swedish Companies Register for money laundering had a total of 94 obliged entities stating that they provided shell offices or letterbox services as of 31 December 2024. Of those, 61 (65%) stated that they only run reportable activities. The remaining 33 obliged entities in the register stated that they also run other activities under the supervision of the County Administration Boards. There is likely a large hidden number of obliged entities who could be classified as shell office or letterbox companies, and which are subject to the AML act, but are not registered with the Swedish Companies Register for money laundering.

Money laundering – description of the risk scenario including known approaches

When threat actors want to be anonymous, they need office and postal addresses that cannot be linked to themselves. They use office and postal addresses to give the appearance of a legal business. There is therefore a risk that obliged entities providing postboxes and shell offices can be exploited as part of a money laundering scheme by threat actors who want to remain anonymous.

Threats – money laundering

Scope

There has been an increase in the use of digital postboxes since the last sector report, but the increase does not necessarily arise from criminals using them to any greater extent. The obliged entities in this sector can be used and are interesting to threat actors such as those that need an address in Sweden to register a company, to obtain certain benefits from the state or to open a bank account.

Threat actor capabilities

No special knowledge is required by the threat actor. A straw man can also be hired to provide an address.

Anonymity

How anonymous a threat actor can be depends on how thoroughly an obliged entity has executed its customer due diligence procedures on the person renting the postbox or office.

¹⁵³ Chapter 1 section 2(1) paragraph 23 and section 4(2), paragraph 3 of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

Summarising assessment

The obliged entities in the sector are attractive to threat actors who want to remain anonymous, and no special knowledge is required from the threat actor. The obliged entities can form part of a money laundering scheme, knowingly or unknowingly.

In conclusion, the threat regarding money laundering in the sector is deemed to be significant.

Vulnerability – money laundering

The chances of detecting money laundering

The last sector report revealed the majority of obliged entities claimed that they had performed risk assessment of their business. But the County Administration Boards have found that few have performed risk assessment in the manner prescribed by the AML act. Many obliged entities state that they do use the information and training provided in the AML regulations. But because there is a general lack of awareness of this, the County Administration Boards believe that the training done is inadequate. There are no indications of the situation having changed.

Compliance

The last sector report revealed that half of obliged entities stated that they know their responsibilities according to the AML act. But the majority do not implement customer due diligence procedures, ask about the source of the money, train their personnel or consider all the risk factors in their risk assessments. This indicates that the obliged entities do not understand the requirements imposed by the act. There are no indications of the situation having changed.

Summarising assessment

The obliged entities are an attractive target for threat actors and the sector can be used for complex schemes in which large amounts are laundered. The fact that the obliged entities do not have sufficient knowledge of the requirements imposed by the act, do not risk assess their business according to the act and do not adopt adequate customer due diligence procedures means significant vulnerability to money laundering.

In conclusion, the vulnerability to money laundering in the sector is deemed to be significant.

Risk – terrorist financing

There is no known method by which the sector is used for terrorist financing in Sweden at this time. No international surveys have been conducted. The sector's risk of terrorist financing has therefore not been assessed.

7.27 Board representation and nominal shareholders

Board representation and nominal shareholders are covered by the AML act, but these services are not compatible with Swedish company law and cannot therefore be offered in Sweden. The sector has therefore not been threat or vulnerability assessed within the framework of this national risk analysis.

Board representation

Board representation involves natural or legal persons holding the office of board member, being responsible for company law, a partner in a limited partnership or some other similar position in relation to other legal persons.¹⁵⁴

Nominal shareholders

Services in this sector also involve natural or legal persons as nominal shareholders at someone else's expense, or measures intended to ensure someone else has such a function, with the exception of when a legal person is listed on a regulated market.

General description of the sector and related products or activities

Board representation

The obliged entities concerned in this sector are purely those persons holding office on the behalf of a third party and on commercial grounds. It entails that the those appointed as "normal" board members in a company or association are not included.¹⁵⁵

Given that board representation is not compatible with Swedish law, Swedish obliged entities can only offer these services in other countries. The Swedish Companies Register for money laundering had a total of 30 obliged entities stating that they were active within board representation as of 31 December 2024. This is a notable reduction compared to the previous national risk assessment, when the corresponding number of around 900. The difference is due to a large number of companies deregistering when made aware that they were not covered by the regulations.

Nominal shareholders

A nominal shareholder is intended to conceal the real owner of a shareholding.

¹⁵⁴ Providing that the obliged entity is not covered by chapter 1, section 2(1), paragraphs 17-21 of the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

¹⁵⁵ The same ought to apply to the function of partner in a limited partnership.

7.28 Currency exchange

Overall sector risk:



Currency exchange is a financial service that can be provided by a credit institution, an institution for electronic money, payment institution and subsidiaries of similar foreign companies. It was previously thought sufficient that currency exchange was covered by a duty to register according to the Act on Currency Exchange and Other Financial Activities (1996:1006) (LVA) instead of being licenced (prop. 1995/96:216 section 6.3). Under the LVA, the service could be provided by natural and legal persons. Since 1 July 2025, currency exchange has required a licence instead of registration (the Currency Exchange Act (2025:250)).

General description of the service

Currency exchange can be run within the framework of various licence and registration types. Which licence or registration is necessary depends on which actual services the company will offer. The business of currency exchange can, for example, be run by banks and payment providers. There are also foreign companies offering money transfer. This requires the business to be established in Sweden through an agent. The agent can offer currency exchange parallel with money transfers when registered with the FSA. Because currency exchangers have different licence or registration types, some key figures and assessments can overlap with other sectors in this risk assessment. The term "currency exchange" only applies to the exchanging of cash for cash.

Amended legislation

It was previously thought sufficient that currency exchange was covered by a duty to register according to the LVA instead of being licenced (prop. 1995/96:216 section 6.3). But since 1 July 2025, currency exchange has required a licence instead of registration (the Currency Exchange Act (2025:250)). The background to this is that currency exchangers handle cash to a large extent, and the risk of such businesses being exploited by criminals is high. It has also become apparent through intelligence and a number of court cases that currency exchanging plays a key in reinvestment by criminal networks in criminal activities and the laundering of crime proceeds (prop. 2024/25:67). Consequently, it no longer seemed reasonable that currency exchange should only be covered by a duty to register. The purpose of the proposal for licencing was to raise the threshold for running currency exchange to make it harder for criminals to exploit businesses under the FSA's supervision.

As from 1 March 2026, the Act on Criminal Liability for Illegal Financial Activities (2026:56) also made it a criminal offence to run a financial business without an FSA licence or registration.

The key figures below are for currency exchangers and certain financial businesses jointly as of 31.12.2024, as the sectors were previously regulated by the same act (the Act on Currency Exchange and other Financial Activities). Compared with the previous sector assessment, providers of crowdfunding services and of cryptoasset services have been removed, and deposit brokers are no longer under supervision.

Key figures	
Number of companies	316
Number of employees	6 580
Number of business connections established	884 420
Company balance sheet total	309 205 123 296
Company turnover	50 401 186 902
Total number of physical customers	1 693 764
Total number of legal customers	167 181

Source: The FSA's periodic reports on money laundering, reference date 31.12.2024. The details are based on the reports of the institutions to the FSA and the table can, therefore, include data which deviates to some extent from the actual situation.

Money laundering – description of the risk scenario including known approaches

The exchange of cash from criminal sources can be done through exchange bureaux, where exchange is executed from one currency to another. A common method is for Swedish kronor to be exchanged to euros or US dollars. Exchange bureaux can also take bank transfers, including mobile payments through payment services, and then exchange them for cash to launder crime proceeds. Exchanging reduces the chances of tracing the money back to the crime, making laundering of criminal funds possible.

Facilitators and professional money launderers

Exchange Bureaux often offer a range of different financial services, such as exchanging cash and providing payment services, with legitimate and illegal money flows. Transactions can also be offered through informal payment systems such as Hawala, despite the business not being licenced to do so.

The links between exchange bureaux and criminal networks are generally substantial. Several of the criminal networks in Sweden have one or more exchangers they use to handle their criminal proceeds. A PML can be an individual employed by a currency exchange company, or an entire business set up as a PML organisation which systematically launders money for criminals for a fee. In many instances, it is not just money laundering or transferring money to other countries that are made possible by criminal activities, they also offer holding and selling of cash criminal proceeds in various currencies. The currency exchange sector is by its nature cash-intensive, which is attractive for money laundering schemes. Criminal proceeds can be exchanged from Swedish kronor to another currency, often euros, to finance drug crime or to integrate money into the financial system abroad.

Several exchange bureaux act as financial hubs, offering a range of financial services to criminal actors. Such bureaux are, in turn, a prerequisite for the extensive illegal flow of money within the parallel economy. An anonymised example of such a financial hub is described below:

Actor W ran a currency exchange bureau in a large Swedish city regarded as a hub for large scale money laundering. The actor helped criminal networks in Sweden to move criminal capital into Europe. Hundreds of millions of kronor were involved.

Threats – money laundering

Scope

Currency exchange bureaux are often easily accessible and transactions are conducted immediately. The sector has a low number of physical premises, with a few local exceptions, and a relatively simple and easily accessible product range. As previously mentioned, currency exchange bureaux have been infiltrated by or can be linked to actors within organised crime. Large volumes can be systematically exchanged and converted to legitimate assets in this way. The scope of the illegal flow within this sector is deemed to be very large.

Because financial actors within cash handling on the international markets are forced to comply with applicable rules to combat money laundering, Swedish kronor have become harder to dispose of abroad. In practice, this has led to the laundering of criminal proceeds from Sweden being limited when it comes to cash, and that criminal actors in Sweden need to exchange euros and US dollars before moving money abroad.

Threat actor capabilities

Businesses within currency exchange are important channels for criminal actors and networks within organised crime. Criminal proceeds from large scale money laundering and cash often pass through some form of currency exchanger. Systematic laundering of criminal proceeds through currency exchange is performed at exchange bureaux and within other types of businesses, and exchange can also be run in private homes, for example. The businesses act as legitimate facades to mislead the authorities. Other services are also offered illegally within the sector, such as couriers, payments through the Hawala system and depositing of cash. As a rule, no particular ability is needed for threat actors to exploit currency exchange to launder money.

A threat actor running an exchange bureaux himself will need a certain level of expertise and ability. The thresholds for setting up and running a currency exchange business have been relatively low in Sweden for a long time. The new legislation that came into effect on 1 July 2025 was designed to tighten up the possibilities for shady actors within the sector.

Anonymity

Currency exchange conducted over the counter requires a physical visit to the exchange bureau, which reduces the chances of anonymity, providing an identity check is performed. But it is possible for threat actors to use couriers and straw men for exchanging to avoid detection, or to leave and collect the money from somewhere other than the exchange bureau. The biggest threat in this context is currency exchange businesses run for criminal purposes. The illegal transactions of a currency exchanger can be conducted and booked outside ordinary procedures alongside legitimate activities, and leaving no visible trace in the official documentation.

An obliged entity has to perform customer due diligence according to the AML act when dealing with a new customer, or for transactions that individually or collectively exceed the equivalent of eur 15,000. But threat actors can make structured currency exchanges within certain amount limits under that threshold to avoid detection and reporting, known as "smurfing".

As a rule, currency exchange bureaux handle large amounts of cash, which implies less traceability of the source of the money and increased anonymity for the threat actor. There are also ways for currency exchange businesses to systematically merge legitimate money with criminal proceeds. Overall, this leads to increased risk of money laundering.

Summarising assessment

Large scale money laundering and conversion of cash criminal proceeds have often passed through some form of currency exchange, and businesses operating within currency exchange have been important channels for criminal actors and organised crime. Several of these businesses take active part in money laundering schemes. Without such exchange bureaux, organised crime in Sweden would likely find it harder to convert its criminal proceeds. Thanks to extensive cash handling, the sector provides the chance of anonymity. The scope of the illegal flow within this sector is deemed to be very large. Consequently, the law was changed in 2025. Businesses with currency exchange now require a licence and will continue to be supervised by the FSA. It is now also a criminal offence to conduct financial activities without a licence or registration. The change is expected to make it harder for criminals to exploit this activity.

In conclusion, the threat regarding money laundering in the sector is deemed to be high.

Vulnerability – money laundering

The chances of detecting money laundering

The legitimate currency exchange customers are mainly private individuals exchanging holiday money, but there can also be high risk customers. Exchange for the purpose of laundering money can, for example, occur through exchanging Swedish kronor to or from another currency, or by exchanging between different Swedish denominations. Because cash is used less and less within the Swedish financial system and society in general, businesses within currency exchange may especially be exposed to threat actors using their services for money laundering. The fact that the sector is cash intensive, and that transactions can be executed quickly, means poor traceability, which implies that businesses within the sector are vulnerable to being exploited for money laundering. Small businesses within the sector are deemed to have fewer resources to protect themselves from being exploited for criminal schemes, and the application of current rules to combat money laundering is deemed to be less effective for smaller actors. There is therefore a risk of threat actors focusing on such businesses. In some instances, threat actors use frontmen or false ID to conduct exchanges or other transactions that amount to money laundering.

The vast majority of small actors running an exchange business do not report suspected money laundering to the FIU, despite being obliged to do so. That means that important information on suspected transactions risks never reaching the relevant authorities. Exchange bureaux are also known to only report a certain number of suspected transactions to the FIU, but those transactions usually do not concern the systematic money laundering that can be linked to actors within organised crime. In conclusion, these circumstances mean that the sector is deemed to be especially vulnerable to money laundering.

In those instances when criminal actors run exchange bureaux themselves, the chances of detecting money laundering are limited due to active and systematic concealment. Currency exchange is sometimes run in parallel with other activities, such as travel agencies and gold shops. Purely criminal businesses offering exchange and other payment services are a particular challenge for the supervisory and law enforcement authorities, partially because a large part of the transactions is conducted outside the regular business and is therefore less visible.

Compliance

Risk awareness of the service varies, which is partially due to some businesses having only been in existence for a short time, and that the service is offered to a high degree by small actors. Awareness and knowledge of the anti-money laundering regulations is deemed to be low for these actors. The overall regulatory maturity is generally deemed to be low. Experience from supervision has also shown poor compliance within the area such as general risk assessment, customer risk classification, customer due diligence, monitoring and reporting to the Swedish Police Authority.

Because the service is mainly provided by small companies, the criteria for managing risks linked to money laundering are a challenge; for example, when the company has to set up functions for combating money laundering. For many of the companies, transaction monitoring is manual, while exchange is usually implemented immediately. There is therefore a risk in the business model of there being no chance of adopting adequate customer due diligence procedures for currency exchanges. This implies considerable vulnerability to money laundering.

Law enforcement authorities have seen examples of the service being exploited by customers able to inflict violence. The fact that many companies providing the service used to be locally-based probably increases the risk of them performing transactions (and failing to report suspicious transactions) for fear of threats or reprisals. There are also many smaller actors offering the service and who are likely dependent on repeat business.

Intelligence and investigation has identified obliged entities who ignore the risks for their own financial gain. There are also obliged entities running businesses that require registration without having applied for, or being granted, registration by the FSA. This increases the risk of non-compliance and increases the vulnerability to money laundering. If a business is run for the purpose of facilitating money laundering, compliance will be limited for obvious reasons.

Summarising assessment

Because cash is used less and less within the Swedish financial system and society in general, businesses within currency exchange may especially be exposed to threat actors using their services for money laundering. The fact that the sector is cash intensive, and that transactions can be executed quickly through currency exchange, means poor traceability, and increased chance of anonymity. Small businesses within the sector are also deemed to have fewer resources to protect themselves from being exploited for criminal schemes, and the application of relevant rules. They are therefore attractive to threat actors. The sector is deemed to be very vulnerable to money laundering.

In conclusion, vulnerability to money laundering is deemed to be high.

Risk scenario, including known approaches of terrorist financing

Currency exchange is deemed to be a way in which money can be used for terrorist financing. The objective is often to exchange to a currency that can be used to send money out of the country and to use couriers to take cash out of Sweden. The money is usually exchanged to an internationally more usable currency, such as US dollars or euros, before the money is taken out of Sweden by couriers.

One method of exchanging cash is to visit several exchange bureaux, either on the same day or over a longer period, and exchange small amounts to avoid deeper checks by the bureau.

Threat – terrorist financing

Scope, ability and anonymity

Currency exchange is easy to perform given the number of bureaux. When large amounts – or amounts in unusual currencies – have to be exchanged, it is more likely to be done at a minority of niche and trusted bureaux to avoid attracting attention. No special abilities or knowledge are needed to exchange currencies, but to avoid unwanted attention and checks, special abilities in the form of knowing which bureaux to use for the type of transaction is required.

Regarding anonymity in this sector, the same factors as for money laundering are decisive for terrorist financing.

Vulnerability – terrorist financing

The chances of detecting terrorist financing

The same actual circumstances as described in the section on money laundering also apply to terrorist financing.

The amounts a threat actor can try to exchange for the purpose of terrorist financing are often much lower than those for money laundering. This means that it is harder for the obliged entity to detect non-conforming transactions.

Exchanges made for the purpose of terrorist financing can differ from those made by tourists, but not always. The sole fact that odd amounts or unusual currencies is not an independent indicator that an exchange can be used for terrorist financing. This is a problem to deal with when it comes to choosing what to report.

Compliance

Concerning compliance when it comes to terrorist financing, no assessment has been made other than that for money laundering.

8 Process and method

The national risk assessment of money laundering and terrorist financing in Sweden is based on the sectors in the application of the AML act, and is an update of the sector based risk assessment published in 2021. The update takes into consideration new knowledge and changes occurring since the previous assessment with regard to such aspects as approaches, threat actor ability or the ability of the obliged entities to detect or prevent money laundering and terrorist financing.

The assessment has been produced with the participants in the Coordination Function according to the guidelines of the Financial Action Task Force (FATF) for the implementation of national risk assessment.¹⁵⁶ The work has been supported by the Swedish Police Authority and other participants in the Coordination Function.

8.1 Overall method and implementation

The report analyses threats and vulnerabilities for the respective sectors. Threats concern the capability of actors seeking to exploit a sector for money laundering and terrorist financing. Vulnerability covers the limitations and possible weaknesses within the respective sectors concerning their ability to resist threats and prevent money laundering or terrorist financing. The overall assessment of threats and vulnerability then gives a risk value for each sector.

The impact on society that can be caused by the risks is then analysed. The consequence analysis makes it possible to rate the risks in the various sectors in relation to each other, creating an overall picture of the national level. This overall picture can be used as a guide when deciding which sectors ought to be prioritised or which are efforts against money laundering and terrorist financing should be focused on.

8.2 Definitions of threat, vulnerability and consequence

According to the FATF, **risk** is a function of three factors: threat, vulnerability and consequence. The FATF states that it is up to the country itself to define a product or process based on a method decided by the affected parties in a country, and that the definitions of threat, vulnerability and consequence are suitable for use. To follow is a more detailed description of the FATF's definition of threat, vulnerability and consequence. The definitions have been used generically to create a conceptual framework for all the actors who took part in this national risk assessment.

Threat is defined as a person, group or business able to harm, for example, the state, society or the economy. Threats can be made by criminal actors, but also by their helpers, assets and businesses. Threats often act as a key principle for developing an understanding of the risk of money laundering and terrorist financing. To be able to perform a risk assessment, it is therefore important to understand the entire chain. For money laundering, it is necessary to understand the predicated offence and the criminal proceeds, and how the latter are laundered. For terrorist financing, an understanding is needed of the source of funds and how they are used to finance terrorism.

The term **vulnerability** is intended to identify weak points in various systems that can be used by the organisation or individuals that represent a threat. Such weak points can be weaknesses in the financial structure, loopholes in the law or unclear delegation of responsibility between authorities. It can also concern the properties of a given sector, financial product or type of service that makes it interesting for threat actors who want to launder money or finance terrorism.

The term **consequence** is generally intended to describe the effect or damage that money laundering and terrorist financing can cause. This includes the impact of the crime or terrorism on the financial system and institutions, along with the economy and society as a whole. In other words, consequences are the impacts that money laundering and terrorist financing can cause in the short and long terms, and how they can impact the population, special groups, the business climate, national and international stakeholders, the reputation of the finance sector and attraction of a country.

¹⁵⁶ FATF Guidance, *Money Laundering National Risk Assessment Guidance*, 2024.

According to the FATF, a risk assessment must include an estimate of threats, vulnerabilities and consequences. Because it is generally hard to determine or estimate the consequences, it is widely accepted that such an analysis cannot go too deep, but must provide an overall picture of the consequences of the threats and vulnerabilities for society. In this national risk assessment, the Coordination Function opted to include a consequence assessment. The method is presented on the following pages.

8.3 Process

The report was produced in four main stages, see figure 8.1.

Figure 8.1



Stage 1. Defining changes

In 2024, the Coordination Function members received the responses to a number of different questionnaires for each sector on which changes had occurred since the previous risk assessment. The questions sought to identify new approaches and indicators of threats and vulnerabilities. The responses received consisted of information from the supervisory functions, intelligence from the law enforcement authorities and knowledge from other authorities in the Coordination Function. Dialogue was also conducted with the trade associations via the supervisory authorities, and data collected from parts of the charity sector.

Information from various sources such as intelligence, supervision, investigations and suspicious activity reports (SAR) to the Finance Intelligence Unit (FIU) was then merged and used for the risk assessments. Changes occurring between comparison years 2020 and 2024 were then analysed for certain key figures, including SARs made to the FIU.

Threat and vulnerability assessments are based on the same basic criteria as in the previous sector-based risk analysis, but in a scaled-down version, see table 8.1. The risk criteria and their parameters reflect the headers used in the description of the sectors in the sector catalogue.

Table 8.1 Parameters for threat and vulnerability assessment

Parameters for threat assessment	Parameters for vulnerability assessment
Scope Threat actor capabilities Anonymity	The chances of detection Compliance

Stage 2. Assessing sector risk based on threats and vulnerabilities

Based on the information gathered and the new knowledge, threats and vulnerabilities were evaluated for the respective sectors. The risks of terrorist financing were only assessed in qualitative terms, while the threats and vulnerabilities of money laundering were assessed quantitatively on a four-tiered scale. The threat and vulnerability assessments regarding money laundering were then merged into a risk level according to the same principal as in the last risk assessment, see figure 8.2.

Figure 8.2 Matrix for threats, vulnerabilities and risks



The heavier emphasis on vulnerabilities in the risk matrix are in line with the EU's supranational risk assessment, and based on the assumption that vulnerabilities can be identified and exploited to lead to future threats.

The assessment scale for threats and vulnerabilities is presented in table 8.2.

Table 8.2 Assessment scale for threats and vulnerabilities

Risk criteria	Low	Moderate	Significant	High
Threat	No indication of criminals intending to use this method for money laundering.	Criminals have the ability to exploit this sector for money laundering.	Criminals exploit this sector for money laundering.	Criminals exploit this sector repeatedly for money laundering.
Vulnerability	Negligible risk of money laundering gives effective barriers and control system.	A certain risk of money laundering in the sector which has effective but not completely impenetrable control systems.	Significant risk of the sector being exploited for money laundering as the control systems have limited effect.	High risk of the sector being exploited. No control systems or not fit for purpose.

Stage 3. Assessing consequences

An appraisal of the consequences of money laundering was made for each sector. The assessment was based on criteria for the sector's trading/dignity, along with the estimated overall impact of the sector.

Table 8.3 Assessment template for the consequences of money laundering

Risk criteria		Moderate	Consequence
How much money is handled in the sector?	How susceptible is the sector for large scale money laundering?	How is society impacted in general?	
< SEK 5 bill.	There are no prerequisites for large scale money laundering in the sector.	Only individual obliged entities are impacted.	Low
SEK 5-250 bill.	There are some prerequisites for large scale money laundering in the sector.	Money laundering can have negative effects on the whole sector, such as loss of confidence.	Moderate
SEK 250-1000 bill.	The sector can play a key role in large scale schemes.	Negative impacts on society may occur outside the sector, such as inflated property prices.	Significant
> SEK 1000 bill.	The sector fulfils a necessary function in large scale money laundering.	Money laundering can give negative consequences at national level, such as threatening financial stability or Sweden's reputation internationally.	High

Stage 4. Identifying risk mitigation measures

Finally, the need for measures to reduce the risks found within the framework of the analysis are identified. The proposal includes measures to increase the transparency of transactions and account holders, means of making supervision more effective and changes to the law that can help combat facilitators and companies being used as fronts for crime.

SAMORDNINGSFUNKTIONEN MOT PENNINGTVÄTT OCH FINANSIERING AV TERRORISM

