

Threat assessment for Sweden's banks

Published May 2025



Svenska
Bankföreningen
Finance Sweden



Threat assessment for Sweden's banks

Published May 2025

The banks' security organisations conduct an annual industry-wide threat identification and assessment based on the banks' operations. A threat consists of an ability, a will and an opportunity.

The banks' specialists when it comes to physical security, identification, cybersecurity, information security, fraud, card security, money laundering, outsourcing, sanctions, cash and security protection contribute to the report.

The threat assessment is divided into a number of areas, concluding with an assessment of the risk and threat level. Measures that banks cannot implement themselves are listed as requiring action by politicians and authorities.

Summary	4
Abuse, personal threats and violence against bank staff	6
The threat from insiders and enablers	9
The security policy situation, continuity and civil preparedness	11
Information security and cybersecurity threats	13
Fraud and financial crime	16
Money laundering	26
Use of businesses for criminal purposes	30
Terrorist financing	33
International sanctions	34
Bank robberies, cash in transit robberies and ATM attacks	36
The challenges in relation to cash	37

Summary

The security policy situation and crime trends in Sweden in recent years are now affecting the banks and their customers, primarily in the areas of cybersecurity, fraud and money laundering. In the autumn of 2024, the number of denial-of-service attacks increased, as well as becoming more sophisticated and more difficult to combat. Measures taken by banks to combat telephone fraud have had an impact, and the proceeds of crime from that approach decreased significantly in 2024 compared to 2023. In the field of money laundering, collaboration has been strengthened in 2025 with the establishment of a financial intelligence centre, in which the banks are involved. Collaboration by banks has been strengthened in all areas of security, both between the banks themselves and with the authorities.

In the field of **abuse, personal threats and violence against bank staff**, banks are reporting increased tension and more aggressive customer behaviour in recent years. Many employees are unwilling to represent the bank in legal contexts. The exposure of individual employees may increase the threat to the individual, rather than to the bank. Ensuring a safe working environment for bank staff is not only the responsibility of the banks, but part of a broader societal commitment.

An **insider/enabler** can use their insight into the bank to carry out illegal transactions or manipulate financial flows on behalf of criminals or a foreign state. This is also a way for threat actors to influence decisions, information flows and business strategies in the bank. Foreign states can use insider networks to gather intelligence, destabilise the economy or influence political decisions.

In the field of **continuity and civil preparedness**, current hybrid threats and incidents in the immediate area show that security policy developments require long-term contingency work in Sweden, and this also includes financial services. With an armed attack on Sweden as a defining condition for continuity work in the banks, more far-reaching requirements are imposed than in the case of peacetime crises. In this event, it is necessary to address issues such as the evacuation of data and functions, extensive backup arrangements and the protection of critical facilities such as office buildings and data centres, wartime organisation, etc.

During the period, the field of **information security and cybersecurity** is characterised by more sophisticated denial-of-service attacks of increased strength and scope. The primary purpose of the attacks is the impact on information manipulation and interference on society and citizens, where the attackers are trying to show that critical financial services are at risk. Companies in the financial sector continue to be affected by ransomware (extortion software that encrypts the data of its victims), although in this respect they are no different from other sectors. During the period, threats to critical infrastructure have been made tangible in the form of suspected sabotage of electricity and communication cables in the Baltic Sea.

Social manipulation has made **fraud offences** more targeted and more personalised. The number of fraud attempts increased in 2024, but the number of fraud cases reported to the police decreased. Earnings from crime also decreased in 2024 compared to 2023. The banks' programme of action to reduce telephone fraud resulted in a 40% reduction in the proceeds of crime in 2024 compared to 2023, as well as a clear drop in the average amount per telephone fraud offence.

Money laundering threats remain widespread, with origins in areas such as fraud, drug trafficking, welfare crimes and tax crimes. Other risk areas for money laundering include companies dealing with currency exchange, cash management, cryptocurrencies, the property market, luxury consumption and the gambling sector.

Companies are used frequently and on a large scale for criminal purposes, with straw men being used to conceal the real operators. Companies can be used for different types of crime in parallel, and the returns from such crime are often high. It is common for loose-knit criminal networks to run a large number of companies and conduct criminal transactions between them.

Terrorist financing involves many different approaches, such as crowd funding and the use of cryptocurrencies. One risk factor is that banks often lack access to information from the police about how such financing takes place and who is involved.

With growing geopolitical tensions, **international sanctions** have become an increasingly important means of exerting pressure on foreign and security policy. At the same time, the scope of the sanctions has increased rapidly, making it increasingly difficult for business operators to understand and apply them. Greater information is required here, along with cooperation and dialogue between the various actors in the field of sanctions. One particular challenge is the increasingly sophisticated circumvention of sanctions.

In 2024, there were no **bank and cash in transit robberies** and no attacks on Bankomat AB's ATMs. The threat of bank and cash in transit robberies and ATM attacks remains, but the number of robberies and attacks is expected to remain low in 2025.

There are policy incentives aimed at increasing the use of cash in Sweden. For the banks, the **challenges associated with cash** are that it creates risks for those working with cash, as well as the fact that the traceability of cash is low or non-existent. Since cash is used to such a little extent in normal conditions, the notion that cash can play a major role in the event of a crisis or war event is also not realistic.



Abuse, personal threats and violence against bank staff

Several employees and managers in the banks testify to a more aggressive tone and tougher customer behaviour in recent years. Banks are seeing signs that employees feel less secure, and surveys carried out by the banks and the Financial Sector Union of Sweden show that employees are being subjected to threats and violence.

This picture varies, however: some banks consider that threats and abuse are at roughly the same level as before, while other banks have noticed a sharp increase over the past year. It is difficult to explain this change. It may be the result of an increased propensity to report or an observed increase. For banks with a large number of branches, around half the instances of abuse and threats are linked to physical branches, while the other half are directed at telephone banking.

More and more customer appointments booked

More and more banks are requiring customers to make appointments for visits to their branch. This decision is often business-driven, in order to improve the quality of customer meetings, but the change is also reducing the threat to employees. Abuse by customers via social media occurs, for example, when customers have been ejected from a branch or when the customer relationship has been terminated for various reasons.

The shift towards more digital customer meetings is affecting working methods, and the change means that new types of threat situations may arise. It's true that there are fewer threats associated with pre-booked appointments, but the threats would not

disappear even if all appointments were pre-booked. For example, an unauthorised person might force their way onto the bank's premises when a customer is entering or leaving.

Tools to deal with threatening customers

The banks are terminating more customer relationships now than in the past. Reasons for this include a lack of customer due diligence, the fact that the bank is detecting more irregularities and that more customers are making threats against bank staff. A higher number of customer relationship terminations is affecting the threat landscape. When the bank terminates a customer relationship or does not allow a person to become a customer of the bank, an internal process is required to assess and anticipate any possible threats to both the branch and the employees of the bank. However, the threat landscape previously anticipated by the banks in relation to the termination of customer relationships has not materialised to the extent that was feared. Banks have been proactive in their security efforts, but there is still a need to monitor developments.

Employees can find themselves in difficult situations with customers who are under financial pressure. Banks therefore provide conflict management training to all staff working in branches and telephone banking, and the banks also work with support functions.

Other tools for dealing with poorly behaved customers include the bank calling or sending warning letters to the customer, explaining that it does not accept abusive behaviour towards bank staff.

Banks are trying to develop methods to better understand and target their efforts: is it a case of an illegal threat or “just” an unfortunate choice of words from an emotional customer? The unsafe situations that arise in physical meetings with customers tend to be repeated in online and telephone meetings. The step from a normal tone of voice to becoming unpleasant is perceived to be short. At the same time, the limit of what an employee can accept varies from individual to individual.

A threat can be actual or perceived. The difficulty in assessing and communicating an actual threat is due to the fact that it is difficult to read threats based on actual events. The key point is that situations that cannot be defined as a threat in the eyes of the law may be experienced and perceived as a threatening situation that contributes to an unsafe working environment.

Banks have the ability to assess a threat, but it is difficult to assess the severity of a threat. Is it genuine or not, will it be realised or is it more a case of an unpleasant incident? The level of anxiety is nevertheless perceived to have increased.

Different parts of the bank experience different kinds of threats

If you live in a small town and meet customers physically outside of work on a day-to-day basis, the situation is different compared to employees who live in large cities or telephone banking employees who do not meet customers physically.

To a large extent, the crucial factor is whether an employee has contact with customers. If the bank has a network of branches, customers often choose to visit a physical branch. If the bank has only one visible physical head office, it is more exposed compared to a telephone bank that may have offices in different locations around the country. Decision-makers in money laundering and fraud investigations, who are often located in central functions, are also affected by the threat landscape, and duality in decision-making has the effect of helping to mitigate threats.

Depending on how the threat landscape evolves, changes may need to be made to physical safety measures.

Controls and measures create customer frustration

Banks receive many enquiries from public authorities, for example in relation to transactions associated with criminal investigations. There are indications of increased concern among staff working with customer due diligence, the reporting of money laundering and fraud. The exposure of individual employees, rather than the bank, can lead to increased threats towards the individual.


Increased efforts to combat crime, in the form of more checks and follow-up measures, can create frustration among customers. Some of the measures taken by banks cause frustration among customers, especially inter-bank measures such as blocking BankID. Recurring sources of frustration include the updating of customer due diligence and instances where the customer wants to make an unusual transaction or add a product/service.

Measures by banks to protect their staff

In response to these threats, banks are working to protect the identities of their employees in various ways. E-mails are sent to a greater extent from central functional mailboxes, such as kundkontakt@banken.se. Furthermore, external customer communications by fraud investigators are restricted. Banks are also considering introducing systems of aliases that can be used by staff for sensitive actions, such as terminating customer relationships.

Even if the identity of the sender is hidden, employees feel threatened when pressure is put on the bank.

Employees will sometimes be unwilling to represent the bank in legal contexts, due to the fear of threats. Employees may find it tough to report threats or crimes they have been subjected to in their work to the police, as this can generate new threats. When making such a report, the employee is the plaintiff, and when a prosecution is brought, the report becomes a public document. The bank cannot make such a report – the victim has to make it themselves. There is a trade-off between reporting the customer to the police and the risk of publishing an employee's name in a police report. One thing the bank can do is to ensure that support is available in the event of any trial.



The exposure of individual employees may increase the threat to the individual, rather than to the bank.



Ensuring a safe working environment for bank staff is not only the responsibility of banks, but part of a broader societal commitment.

Banks are continually implementing protective measures to ensure that individual employees are not unnecessarily exposed publicly in connection with certain types of decisions or other actions. However, this work is hampered by the public authorities occasionally disclosing bank employees' personal data, combined with the availability of detailed personal data through public search services. If the disclosure of personal data entails a risk of the person or their relatives being subjected to threats, it should be permitted for aliases to be used instead. The person's name should also not be disclosed by the authorities.

Ensuring a safe working environment for bank staff is not only the bank's responsibility, but also part of a larger commitment for various actors in society to combat fraud and money laundering.

The increase in the terrorist threat level from 3 to 4 by the Swedish Security Service in August 2023 has resulted in banks reviewing their existing security and business continuity efforts, even though the banks themselves are unlikely to be a direct target.

Several banks have been the subject of demonstrations by groups that want to protest against the banks' business activities, such as environmental organisations. This is not a problem for the banks, but rather a natural aspect of an open society. On the other hand, protests and actions can occur where entrances and exits are blocked, which risks complicating any evacuation and puts staff and customers in danger.

Need for action by politicians and authorities

- The requirements imposed on banks by the authorities have contributed to an increased threat level in relation to bank employees. Banks are being forced to expose individual employees in the event of a police report and other contacts with the authorities, which increases the risk of threats. If the threat relates to an entire branch, the bank can report this to the police. It ought to be possible for the bank to report a threat to the police in such a way that employees do not need to be exposed. Banks are requesting a centralised function that can represent a bank in cases of fraud, for example, or to explain in court how, for example, a payment service works. The person making the report would thus be neutralised, as it is the organisation's stance and not that of the individual employee. In such cases, the bank can also choose who will represent it. As a result, the employee does not need to feel they are being identified, in addition to the threat to which they were previously subjected.

The assessment is that the threat to bank staff is affected by both the development of society and the requirements of authorities.

The threat from insiders and enablers

So-called enablers of crime are an ever-present factor requiring vigilance and adequate measures. An enabler of crime in this context is an insider who, through their professional role, acts improperly. This might be for personal gain, for organised crime and criminal networks, or for a state actor. Organised crime and criminal networks are the defining threat.

High-risk behaviour and vulnerabilities

The incentives for an external antagonist to plant or recruit an insider at a bank are generally considered to be strong, as this provides greater opportunities for various types of fraud, money laundering schemes, the potential to influence decisions and access to inside information. An insider can be an active enabler, actively share information or have more of an advisory or coaching role. The employee may also be unaware that they are being used as an insider.

The insider is often a person who has various forms of high-risk behaviour and vulnerabilities, such as drug abuse, gambling addiction and/or personal financial problems. He or she may also be in a vulnerable situation in other ways, through family relationships or friendships. This type of relationship can be expected to have a negative impact on the performance of their role, which is based on suitability. There may also be links to high-risk countries or criminality. Another incentive for disloyal behaviour on the part of an employee is underlying disenchantment with the employer, due to lack of appreciation, lack of promotion or poor salary progression.

Some methods require an enabler on the inside

Some methods cannot be carried out without an enabler on the inside. An employee who has knowledge of the bank's products, services, procedures and processes, credit regulations and transaction monitoring rules is of interest to external actors. As well as the bank's own credit preparation process, loan intermediaries, with additional parties in the loan chain, create various kinds of incentives for fraud and money laundering for an insider.

Pressure can take different forms

External antagonists may seek contact with staff in a bank in order to cultivate and exploit them in various ways. Social media such as LinkedIn and other open information sources are used to map employees in the bank and to search for enablers. The number of contacts offering to conduct paid interviews, for example via LinkedIn, is estimated to have increased in recent years.

Criminals and other hostile actors also advertise for people who are prepared to help from the inside. In this way, social manipulation merges with the physical threat landscape, as improper contacts can subsequently result in physical threats being made against employees. This might involve pressure, help with debts, the possibility of being paid for providing information or the insider feeling needed. It might also relate to employees' contacts in the pub, as well as various forms of substance abuse that could lead to blackmail situations. There are also instances of individuals with links to an external antagonist seeking employment in a bank with the aim of enabling crime.

Threat actors and enablers can influence decisions, information flows and business strategies in the bank.





Banks are demanding clearer rules

One question that arises is how the bank can protect employees against improper contacts from state actors or organised crime groups, for example. Security protection legislation, which often relates to a limited portion of the bank's operations, regulates how this should be managed, but the threat exists across a wide range of activities, from fraud to how to circumvent sanctions. Background checks, which are mainly used at the time of recruitment, do not offer the same opportunities as security clearance.

In this respect, it would be of interest for banks to have sufficient control options both in connection with the recruitment procedure and during the period of employment. There is a high level of interpersonal trust in Sweden. This is fundamentally positive, but can give rise to naïve attitudes. At present, banks need to rely to a large extent on the information provided by job applicants themselves. Sweden also focuses heavily on discrimination, occupational health and safety and data protection legislation, which can be contradictory.

Banks are requesting clearer laws and regulations in the field of ongoing controls, in respect of practice and levels of evidence. When anomalies are found during the course of employment, how should these be handled and what should the approach be in cases where irregularities are identified? Banks should also be given the opportunity to share information, so that they can work together to ensure that an insider, once discovered, cannot find employment at a new bank and continue their enabling activities there. The increased mobility in the labour market raises the question of whether there should be some form of right of communication between banks in order to address the challenge of insiders.

Information needs of law enforcement authorities

Banks are hampered when it comes to discovering insiders and taking adequate measures, because in many cases they do not receive sufficient and timely information from law enforcement authorities who suspect the presence of an insider in a bank. As insiders often use private communication channels to illegally disseminate information and communicate with criminals, it is law enforcement authorities that are best placed to detect these activities. It is important for authorities to be able to share information with banks so that they can take action.

Although the Swedish Security Service identified intelligence threats in February 2024 from Russia, China and Iran in particular, the difficulty is that insiders could be absolutely anyone. Approaches aimed at addressing this threat landscape range from technical controls to ensuring that measures are implemented so that all employees feel safe to report anomalous behaviour, secure in the knowledge that they will not be perceived as informants.

Threat actors such as nation states (Russia, China, Iran, etc.) and criminal groups have different aims. Although the police consider that the threat to banks comes mainly from criminal groups and not nation states, the recently identified links between state actors and criminal networks in Sweden are having a significant impact on the insider problem.

The banks' own control options

Preventing, deterring and detecting internal crime is an important part of a bank's security work. This can include monitoring digital flows in the bank's own systems and thereby identifying inappropriate digital behaviour and patterns of behaviour. Banks have extensive internal control options, including entry and exit logs, monitoring customer searches, authorisations, documentation requirements, etc. The most successful method is to cross-fertilise different control environments. Anomalies in individual systems and processes may not be significant, but when multiple data points can be aggregated, a different picture can emerge.

In order to reduce the vulnerability of the business or individuals to the risk of being exploited by criminal actors, several departments need to be involved in the internal investigation process. This also applies to cases of misconduct and breaches of the rules.

The assessment is that insiders/enablers are a threat that exists internally in banks and that will persist in 2025.

The security policy situation, continuity and civil preparedness

Sweden is in a difficult security policy situation, which is also influencing the threats to the financial sector. The risk of antagonistic hybrid threats aimed at influencing banks and financial infrastructure is considered to have increased.

During the latter part of 2024, Swedish banks were targeted by sophisticated denial-of-service attacks aimed at affecting the availability of internet services. Denial-of-service attacks in themselves are nothing new for banks. They have been happening every now and then for at least the last ten years. However, the most recent attacks show an increase in strength and scale. There may be many different motives behind attacks of this type, but most often the aim is to destabilise and damage confidence in financial services and the financial companies that provide them. The Swedish Bankers' Association also notes the threat in the local region to the critical infrastructure on which banks depend.

Sabotage against critical infrastructure

In threat assessments conducted in recent years, banks have noted threats to critical infrastructure resulting from the security situation in the region. During the reporting period, the threats have been made more tangible in the form of suspected sabotage of electricity and communication cables in the Baltic Sea. It is therefore considered that the threat is even more relevant to Swedish banks.

In addition, there have been media reports of a foreign power mapping critical infrastructure using drones, for example. It also appears that the actor behind this is not afraid of being discovered.

Swedish banks need to maintain their focus on reviewing their dependence on critical infrastructure. They need to plan in order to increase their resources and capacity, for example in respect of electronic communication and power supply. This is true regardless of whether or not the recent suspected sabotage proves to be an antagonistic act. It is also in line with work on total defence and civil preparedness, which is now being intensified in both the financial sector and nationally.

At the same time, it can be difficult for individual banks to get an overview of threats and vulnerabilities in critical financial infrastructure, as the global financial sector is highly integrated and interconnected at an operational and technical level. There is widespread dependence on foreign IT service providers in the financial sector, and digital sovereignty issues are now higher up on the agenda. Banks need to continuously monitor and evaluate the risks associated with relying on foreign providers for business-critical services.

The risk of antagonistic hybrid threats aimed at influencing banks and financial infrastructure is considered to have increased.



The banks' civil preparedness work and continuity

Civil preparedness work in relation to civil defence has now been added to the continuity and security work. The expertise and human resources that banks possess in this area will be built up and expanded over time. By implementing and integrating risk management frameworks into their civil preparedness work, banks are endeavouring to ensure the continuity of critical financial services. The aim is to be prepared for widespread digital and physical disruptions, including potential armed attacks against Sweden. At the same time, with an armed attack on Sweden as a defining condition for continuity work, more far-reaching requirements are imposed than in the case of peacetime crises. In this event, it is necessary to address issues such as the evacuation of data and functions, extensive backup arrangements and the protection of critical facilities such as office buildings and data centres, wartime organisation, etc.

Several civil preparedness initiatives are now being added to banks' security and continuity functions. Furthermore, many initiatives in the fields of contingency and operational resilience are being launched simultaneously and without prior notice, by several different authorities and the Government. These initiatives are often uncoordinated and overlapping. This results in banks lacking information about the conditions they need to take into account in their planning, as well as clear guidance on how to prioritise security and contingency efforts. All in all, this means that the build-up of capabilities in both the short and the long term is being put at risk. There is a danger that the tangible results expected from this work will not be achieved in time.

Swedish banks need to continue to focus on reviewing their dependence on critical infrastructure.

Need for action by politicians and authorities

- A clear, shared objective for the financial sector's civil preparedness work needs to be developed by authorities and companies operating in the sector. This objective must be firmly established and possible for all authorities and companies in the sector to understand.
- Clear cross-sectoral priorities need to be determined and communicated by the sector's authorities. Priority will be given to those focus areas that are initially deemed particularly important for increasing the overall capability and impact within the sector. Until now, contingency issues in the sector have only been addressed from the perspective of individual actors. The Swedish Bankers' Association sees a need to raise the perspective to a strategic level, where capacity development and required investments in contingency measures are analysed at sector level.
- In their civil preparedness planning, banks need far more detailed threat descriptions, scenarios and assumptions regarding the development of events in the event of an armed attack on Sweden. These include, for example, descriptions of access to electricity supplies, telecommunications and data communications, particularly important geographical areas in Sweden that the banks need to take into account, and assumptions in respect of the timing of the armed attack.

The assessment is that banks are affected by Sweden's security situation and the enhanced threat landscape. As future developments are difficult to assess in both the short and the long term, banks need to continuously monitor and assess how the situation is impacting the threat to their own operations. The Government's expectation is that banks will contribute to the ability of total defence to defend Sweden and our population against an armed attack.

Information security and cybersecurity threats

Ransomware

During the period, a large number of businesses have continued to be affected by ransomware attacks, i.e. extortion software that encrypts its victims' data until a ransom is paid. The number of attempted attacks remains at a high level compared to previous years, although fewer businesses are being affected. There is also a trend towards attacks focusing more on breaches via exposed standard software used in businesses, such as file transfer software or VPNs (virtual private networks). At the same time, attacks involving access via employees' computers are decreasing to some extent, as better protection is now available.

Companies in the financial sector also continue to be affected, although in this respect they are no different from other sectors. Incidents include the attack on US mortgage lender LoanDepot, which suffered a ransomware attack affecting almost 17 million customers in January 2024. The attack resulted in sensitive personal information being stolen. The attack also forced LoanDepot to take its systems offline, causing disruption for about a week. The threat actor BlackCat/Alphv has claimed responsibility for the attack. In June 2024, Evolve Bank & Trust was hit by a ransomware attack carried out by the threat actor LockBit. This attack involved the personal data of around 7.6 million individuals being stolen. The incident also affected several fintech companies working in collaboration with the bank, increasing the scale of the attack.

Data is not only encrypted during attacks, but is also stolen, and the actors responsible threaten to post the information publicly on the internet unless the ransom is paid. It is believed that thefts of information related to ransomware attacks are increasing compared to the previous year. In some cases, the threat actor fails to encrypt the information during the attack, but does succeed in stealing the information. Threats relating to information theft have also been made without actors actually stealing any information. The content of stolen information may also be exaggerated to gain attention.

Threat actors also attack third-party suppliers with ransomware attacks. This serves to create a leverage effect, as the customers of suppliers are also affected. Attacks also hit businesses supplying banks during the period. However, there is no evidence to suggest that these suppliers were attacked because they have banks as customers.

Banks should continuously monitor and assess the ransomware threat and improve their protection measures. In the event of an attack, the bank must have developed measures in order to detect and respond to it, and to restore operations. Large-scale ransomware attacks on the financial sector could have a very significant impact. Studies and analysis carried out by the International Monetary Fund (IMF), the European Systemic Risk Board (ESRB) and the Swedish Central Bank show that a sufficiently large cyber attack on the financial sector could threaten financial stability.

Infostealers

An infostealer is a type of malware designed to steal sensitive information from infected IT systems. This information may include login details, financial information and other personally identifiable information. Infostealers are often used by threat actors to carry out additional criminal activities such as fraud and extortion.

Attacks using infostealers are considered to have increased significantly in recent years. In the financial sector, the 2024 attack on the Spanish bank Santander stands out. The threat actor ShinyHunters succeeded in accessing sensitive information about both employees and customers in Spain, Chile and Uruguay. The attack affected a large number of customers and employees, although no transaction data or online banking credentials were stolen. Individual bank customers are also at risk from infostealers. This has been observed in a number of countries. Sweden has been affected to a lesser extent, but there are grounds to monitor this threat as part of the security efforts.



Destructive malware

During its war of aggression against Ukraine, Russia has repeatedly used destructive malware (wiper malware) in an attempt to destroy systems and data in critical infrastructure. Ukraine has been successful in defending itself against this. In threat assessments carried out in recent years, banks have described the threat to Swedish banks as an indirect risk exposure, due to the fact that attacks risk spreading to actors and geographical areas other than the intended target. This type of uncontrolled spread of destructive malware does not appear to have occurred in the last year.

Nevertheless, the threat posed by wiper malware should not be downplayed. The risk of direct attacks or the indirect spread of wiper malware is considered to be low, although the consequences would be extensive. In a situation involving the rapid deterioration of the current security situation, the threat could become a reality, and there is every reason for banks to continue monitoring this area.

Denial-of-service attacks

During the latter part of 2024, Swedish banks were targeted by sophisticated denial-of-service attacks by a specific threat actor, aimed at affecting the availability of online services. Denial-of-services attacks in themselves are nothing new for banks – they have occurred from time to time for at least the last ten years. However, the most recent attacks show an increase in strength and scale, as can be seen from the following examples.

- **Duration:** The duration of the attacks has increased tenfold compared to previous situations.
- **Strength:** The attacks have been around 15 times stronger than before.
- **Damage:** The exact cost is difficult to calculate, but the price tag for the attacks is estimated to be in the tens of millions of Swedish kronor. These attacks are particularly damaging to trust in the sector.
- **Geography:** The attacks have also taken place from Nordic IP addresses, making it difficult to prevent them. However, the majority of the IP addresses originate from countries outside the Nordic region.
- The threat actor has not publicly stated the purpose of the attacks.

The threat actor for the current attacks also has the ability to rapidly change and adapt attack techniques, making the attacks difficult to stop.

The primary purpose of the attacks is to undermine confidence in critical financial activities. If disinformation about serious cyber incidents in financial companies spreads and gives rise to herd behaviour among banking customers, such as mass withdrawals from bank accounts, the consequences regarding financial stability could be severe.

IT supply chain risks


Banks use IT providers, cloud services and publicly available software in their operations. One consequence of this is that malware can spread through established supply chains. Another consequence is that vulnerabilities are discovered by threat actors, who immediately use them to attack systems before they can be addressed. This type of vulnerability is usually referred to as zero-day. During the year, such vulnerabilities have once more been highlighted globally. Some of the highlighted cases have occurred in IT security solutions such as Fortinet and Ivanti.

These vulnerabilities pose a significant risk to banks as well, as they enable attacks where there are no defence mechanisms. The number of vulnerabilities also appears to be increasing, and they are also being exploited more rapidly than before, leaving banks with less time to react. Banks also need to continue actively monitoring and addressing non-zero-day vulnerabilities. Overall, this is increasing the pressure on banks' IT functions, which in turn entails a need to bring in resources to manage the risks.

Perhaps the largest incident during the period in these areas was the CrowdStrike incident that occurred in July 2024. An incorrect update of CrowdStrike's Falcon Sensor security software caused extensive problems with Microsoft Windows computers. The update caused around 8.5 million systems to crash and fail to reboot correctly. The incident affected many sectors and services globally, demonstrating the concentration risks that are built up when multiple customers use the same IT solution. The incident impacted banks in Sweden, albeit marginally.

Artificial intelligence and deep fakes

With the emergence of AI services on the internet, the risk of information leakage is increasing for banks, where employees use the services incorrectly and input sensitive information into the services.



Banks should continuously monitor and assess the ransomware threat and improve their protective measures.

Fake videos, images or audio that are so advanced that they appear genuine tend to be known as 'deep fakes'. The development of artificial intelligence is both accelerating the development of deep fakes and making them more difficult to detect. The use of deep fakes for fraudulent purposes is a growing threat in society. In banking operations, for example, deep fakes could be used to impersonate people in senior positions, for example in relation to bank staff working in the field of payments. The aim of this might be to make fraudulent payments.

During the year, there have also been examples of senior bank executives being impersonated using deep fakes in order to deceive bank customers. Phishing e-mails are also getting ever better and more realistic in terms of their language, suggesting a link to AI.

Phishing and banking Trojans

Malware or links to malware via e-mails to bank employees are a common threat. Another approach is spear phishing, i.e. phishing that targets selected individuals at banks. Spear phishing has been targeted, for example, at bank employees who might have higher IT access rights. LinkedIn has been used to identify the IT staff at banks, who have then received fake job offers with links to malware. The purpose of this type of spear phishing is probably that the threat actors view it as a quick way of gaining a foothold in the infrastructure at banks.

At the same time, phishing that does not target specific individuals, but is more opportunistic and random in nature, is still common. There is also phishing in relation to staff at IT providers as a way of potentially attacking banks. As a further development of phishing, it is now increasingly common to use quishing, where QR codes are used to trick people into visiting malicious websites or downloading malware.

The assessment is that malware via phishing continues to be a high risk for banks. A small increase in spear phishing can be observed during the year. Exercises and training for staff to be able to detect phishing e-mails, as well as technical solutions at banks to block phishing e-mails, remain important countermeasures.

The occurrence of banking Trojans is continuing, affecting customers of banks and financial companies right across Europe, including in Sweden, albeit to

a lesser extent. Attacks with banking Trojans appear to go in waves in different countries, returning to Sweden when the threat actors want to test new attacks against Swedish bank customers. Banking Trojans that infect mobile phones and mobile banking solutions are often designed to steal customers' login credentials. Banking Trojans developed for Android phones are still considerably more common than for iOS phones. Bank customers have had their mobile phones infected by downloading apps that contained malware.

Need for action by politicians and authorities

- As soon as possible, implement the proposals in the study "A new function for crisis management in the event of serious operational disruptions in the financial sector's digital infrastructure", in which the Riksbank is tasked with establishing the function.
- Ensure that the Riksbank is tasked with defining clear roles and responsibilities for the crisis management function and how the function should interact with the National Cyber Security Center (NCSC), CERT-SE, and the National Defence Radio Establishment (FRA), for crisis management and support measures in the event of cyber attacks against societally important financial operations.
- Ensure that the Riksbank, with the support of the NCSC, CERT-SE and FRA, is tasked with establishing specific support measures for operators of societally important financial operations in the event of major cyber attacks.
- Introduce the new crime of data interference in the Criminal Code. Denial-of-service attacks are currently covered by the crime of hacking, even though no breach of a particular computer system has occurred. This is actually a case of a temporary disruption of access to the computer system, but not its content.

The assessment is that the threat level in the field of information and cybersecurity remains high, and that it is influenced by criminal groups and state-sponsored threat actors. An increase in the number of denial-of-service attacks has been observed over the period, and they have become more sophisticated and more difficult to combat. In the cyber field, the threat landscape can also be influenced by hostile actors who are persistent and driven, and who see opportunities linked to the development of security policy.

Fraud and financial crime

The reduced number of bank and cash in transit robberies, digitalisation and society's increased demands for e-commerce to use the bank's security solutions have changed financial crime.

In 2024, a total of 227,434 fraud offences were reported in Sweden, according to the police. This is a decrease of 8,231 offences, or 3%, compared to 2023.

Fraud attempts increasing, but proceeds of crime decreasing

The number of telephone scams reported to the police increased in 2024, although the criminal proceeds arising from them decreased by 40% compared to 2023. According to the police, the main reason for the reduction is the banks' programme of action to combat fraud, which was launched in May 2024.

The police estimate that criminal proceeds from fraud amounted to around SEK 4.2 billion in 2020, SEK 4.6 billion in 2021, SEK 5.8 billion in 2022, SEK 7.5 billion in 2023 and SEK 6.3 billion in 2024.

The increase in criminal proceeds from fraud in recent years, up until the break in the trend in 2024, can largely be explained by the marked increase in fraud involving social manipulation. In 2019, for example, the number of vishing scams reported to the police stood at 5,285, while by 2024 this number had increased to 31,155.

Although the banks' measures are restricting opportunities and have had an impact on limiting the proceeds of crime, fraud offences have evolved to become highly flexible and adaptable. Organised crime with a high level of violent capital is currently influencing banks in the areas of physical security, cyber, fraud and money laundering, where the different elements are intertwined.

New products and third-party suppliers

One of the challenges in work to counter fraud is that the development of services and digitalisation are progressing very quickly, which means that the threat landscape is changing rapidly. The speed of these developments, in turn, requires real-time protection regarding information sharing, and there is a need to share technical information. Banks are continually taking down fake websites, which demands skills and resources. Banks need to understand what threats and vulnerabilities the new products entail, and to develop countervailing measures.

New services and products are not always developed by the bank itself, rather this can take place in collaborations with other actors or be performed by third parties. It is necessary to strike a constant balance between versatility and customer friendliness on the one hand, and steadiness and increased security on the other. The development process is strongly business-driven, and customers expect the bank to offer new products and services in line with technological developments. Some actors in the payment chain do not have the control in respect of the end customer that the authorities require banks to have. This may relate to risk assessment of customers, customer due diligence and fraud monitoring measures, as well as a process that ensures that the various elements are interconnected.

With PSD2 and service deliveries based on third parties' access to accounts and data, also referred to as open banking, several parties have been added in the payment chain, entailing new risks and challenges. Monitoring may become more and more difficult for banks, due to the increasing number of actors. For consumers, it can be difficult to understand what they are giving their consent to and which actor has access to customer data.

To address this shortcoming, the upcoming EU Payment Service Regulation includes a proposal to introduce a list of individual consumers' consents to third-party providers.



More actors gain access to the banks' information

There is currently an EU legislative proposal to move from open banking to open finance. The political objective is to improve and tailor financial products and services for customers, as well as to create increased competition within the financial sector. This proposal could open up the banking infrastructure to more actors within various financial services, in addition to payments and account information. Open finance allows more financial actors to access and have the potential to share a large amount of financial data. This means that more of the bank's customer data will be available to be used by third parties, not just for payments, but also for mortgages, loans, savings, pensions and insurance.

Highlighted risks include cybersecurity risks, fraud and financial crime. Customers' knowledge and awareness of how products and services work, as well as how data is stored, used and distributed, are therefore all important issues. It is equally important that the same requirements are imposed on all open finance actors as on banks.

New rules for payments

Another legislative proposal is the European Commission's proposal to amend the regulatory framework for payment services. This will result in a Payment Service Regulation, which will be directly applicable in Sweden. Negotiations are currently under way regarding the legislative proposal, which contains measures to counter fraud as well as proposals for

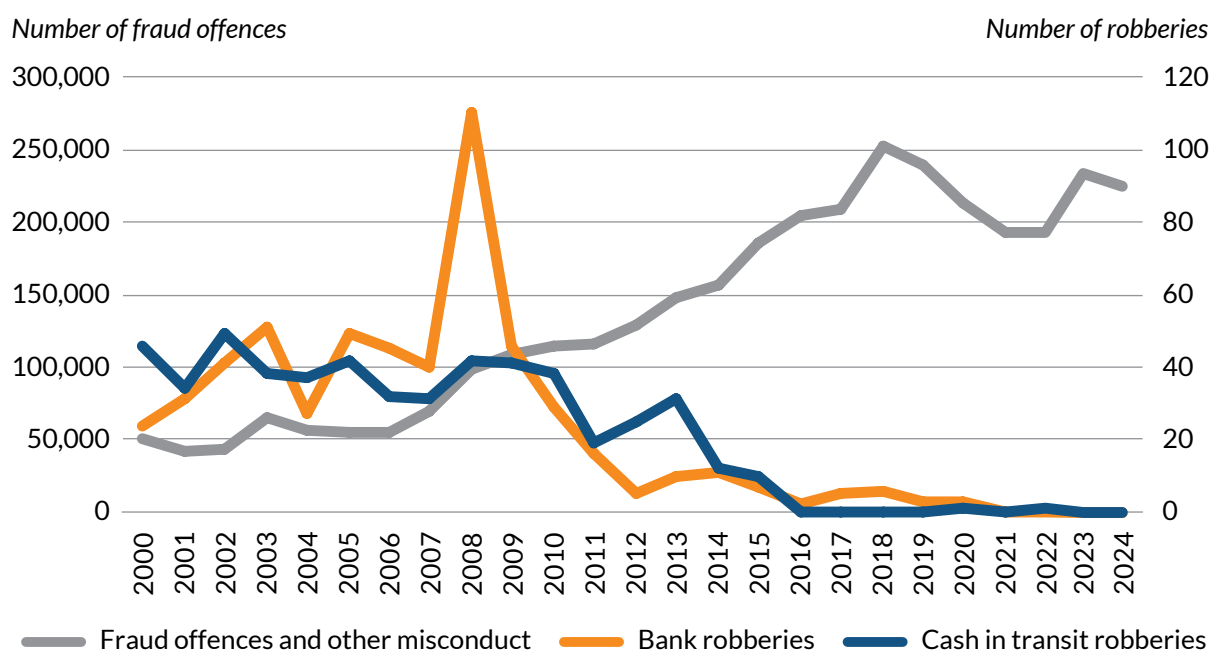
increased consumer protection. For example, it is proposed that banks will have greater liability for reimbursing customers in certain fraud situations.

A shift in the division of responsibilities towards the bank, and the accompanying requirement to reimburse customers in cases of fraud, could result in an increase in friendly fraud. Friendly fraud is where a customer who claims to be a victim of fraud is actually in collusion with the fraudster.

With guaranteed compensation to the customer in the event of fraud, an additional problem arises – the customer may pay less attention to security. This also removes the incentive for other stakeholders (telecoms and social media/online platforms) to cooperate with banks, as the full financial burden of fraud will always be borne by the banks. To effectively deal with the problem, the focus should instead be on preventive measures across the entire ecosystem, including non-banking actors.

The shift in the division of responsibilities may also lead to greater inertia in the banks' services. Regardless of payment instruments, limits, etc., banks will restrict and customise their services. In such cases, banks will probably work on more individualised customer due diligence updates, as well as maintaining ongoing contact with their customers and requesting documentation. It will also become increasingly important to assess what the customer wants to do and actually does in such circumstances. For example, customers may increasingly need to tell the bank what they want to do before they do it.

Number of fraud offences and bank and cash in transit robberies (2000–2024).



Source: Swedish Bankers' Association and Swedish National Council for Crime Prevention.

A customer may only be allowed to transfer to certain pre-notified accounts, and only up to a low amount limit. It is likely that even better technical conditions will be required, as well as more studies of customers, flows and understanding customers' links with each other. In such cases, banks will also increasingly need to look at fraud reports from two perspectives: the first with the customer as a victim of fraud, the second with the customer as an enabler of fraud.

Under the new Payment Service Regulation, which is currently being negotiated within the EU, an extensive package of measures to combat fraud is under discussion. The measures include improved information sharing between different actors, the potential for banks to halt transactions that are suspected of being fraudulent, the introduction of spending caps, as well as a cooling-off period for customers in cases where the spending cap has been raised. While the existence of political ambitions to combat fraud is very positive, it is also very important for these measures in the Payment Service Regulation to be designed in a way that both strengthens consumer protection and provides banks with the right tools to effectively combat fraud.

New rules for real-time payments

The EU is also proposing the speeding up of payments. In 2024, new rules came into force regarding payments in euros. They require payment service providers to offer their customers real-time payments through the same channels in which they are offered regular account transfers in euros. The term 'channels' refers primarily to online banking, mobile banking and telephone banking. Real-time payments pose a number of challenges when it comes to fraud and financial crime.

These challenges will grow if instant payments become an available option for more types of payments. To balance these challenges and limit the risk of an increase in instances of fraud, banks need to adjust existing systems and find new working methods for identifying and stopping fraud, at the same time as raising their customers' awareness of the risks associated with real-time payments.

The threat landscape is changing

Banks have historically had the capacity to fend off fraud offences, but the digitalisation of society and PSD2 have altered the situation. The business model, infrastructure and risk distribution of card payments have previously served as a kind of protection for consumers. However, as demands increase for e-commerce to use the bank's security solutions to a greater extent, demands on customers are also increasing, both to be able to use the digital tools and to be able to withstand social manipulation.

As a consequence of the increased authentication demands within e-commerce, criminality has been driven towards methods involving a larger degree of social manipulation, such as telephone fraud. Either the customer is tricked into surrendering information or they are misled, at the fraudster's request, into carrying out a transaction themselves (a so-called authorised transaction under PSD2). The threat landscape has consequently changed and it is necessary for the preventive measures to be adapted.



Fraudulent offences have evolved to become highly flexible and adaptable.

The main fraud threats

The main fraud threats in 2024 have been vishing, smishing, investment, romance and credit fraud, as well as Business E-mail Compromise (BEC) fraud. The methods used are explained below.

Vishing fraud (telephone fraud): The fraudster calls a consumer who, during the phone call, is tricked into either surrendering codes from a security device or identifying themselves or signing orders with their e-identification. Customers are often tricked into carrying out the transactions themselves, for example under the pretext that money needs to be transferred to a “secure account”.

Smishing fraud (fake text messages): The fraudster sends a text message to a customer with information intended to persuade him or her to do something. The fraudster’s intention is to create a stressful situation in which the customer has to act quickly: call a phone number, install a piece of software or follow a link and disclose information. Common schemes include text messages to the customer informing them of “suspicious activity on a card or account”, or text messages from “Mum who has switched phones and needs help”.

Romance scams: The consumer is contacted and courted by a fraudster. The fraudster seeks to contact people in situations in which they are vulnerable, and love is a strong driving force.

Investment fraud: The fraudster contacts a consumer and offers a fictitious investment opportunity, always with elements of high return at low risk. These contacts often continue for an extended period, and it is common for consumers to be deceived multiple times.

Credit fraud: The fraudster applies for a loan on false grounds. This can be based on false documentation, incorrect information or the fact that the customer has no intention of repaying the loan. The identity used may be that of a person who has emigrated, be assigned to another person or be fabricated.

BEC fraud: Business E-mail Compromise, such as CEO fraud, involves someone within a company being tricked into making transactions to fraudsters.

Consumers and businesses are also vulnerable to attempted fraud in many other ways, however, and there are several entry channels. Everything from phishing for login credentials (e.g. e-identification and security devices), malware distribution, ID theft, advertising scams, subscription traps, fake offers on Facebook and Instagram, goods that are not received and fake websites.

Social manipulation continues

All banks notify their customers about how the bank’s services and products work, but information alone is not enough to reverse the criminal trend in social manipulation. There is no single change that can resolve the challenges posed by social manipulation, rather it is a case of working with a number of preventive and collaborative measures, in addition to the banks’ own measures.

The common denominator in fraud schemes is the desire to influence and persuade the bank customer to do something: click on a link, make a payment or call a number. Crime has become more targeted and more personalised, and approaches are increasingly being tailored to the circumstances. The same *modus operandi* are essentially being developed to become more accurate. For example, fraudsters are increasingly inserting the real name of a parent’s child in the “child text message” scheme. It is currently profitable for organised crime to invest in this type of fraudulent crime concept, since only a low proportion of fraud offences are solved, despite traceability being high.

The scams affect all target groups. Current events in the outside world are often used as bait. Another trend is the increase in the number of customers who become victims of multiple scams. The most common recovery scam is where a victim of crime is misled into believing that they can get money back from a previous investment fraud.

A growing challenge is where vulnerable customers are induced to send the money through other customers and/or institutions in one or more stages before it reaches the intended final recipient. This creates difficulties when it comes to allocating responsibility, investigating and reporting.

Hybrid modus operandi dominating

The hybrid approach between vishing and smishing is currently the dominant method, i.e. a text message from a fake operator that contains a phone number to a fake customer service function. The customer then calls the fraudster and is tricked during that call, or the customer is “connected” to “their bank”.

The trend involving frauds where the customer has personally approved transactions online or via mobile banking poses a more complex problem for the bank, both when it comes to monitoring and understanding what has happened. Banks need to obtain accurate information about what the bank and other actors are doing and not doing. Other actors cannot connect to the bank’s security department, for example, and all the things the fraudster wants to “help with” are things the banks can do themselves if needed, as banks already have all the information about the customer.

Both consumers and businesses are increasingly being subjected to fraud, the aim of which is to gain rapid access to, and to empty, the customer’s bank accounts. To be able to carry out this type of fraud, the customer is manipulated in various ways in order to use their e-identification or security device.



During 2024, measures by banks against telephone fraud reduced crime profits by 40% compared to 2023.

Business operators are exposed

As it becomes increasingly difficult for fraudsters to withdraw large sums of money from the bank accounts of private individuals, more sophisticated fraudsters are targeting businesses. Business operators and users with access to multiple commitments, such as accountants, have become more vulnerable in recent years. For example, new technologies are being used to lull the victim into a false sense of security, making the scammers' approach more difficult to see through. In this event, the proceeds of crime can amount to several hundred thousand Swedish kronor or more. In the worst cases, fraud can wipe out businesses and lead to bankruptcy, as business operators do not enjoy the same basic protection against financial loss due to crime as consumers.

Duality, i.e. the need for two people to approve a transaction, gives rise to inherent inertia, but also security. But even if you employ duality when it comes to signing or have a duality limit of a certain amount, some companies, associations and foundations do not have internal procedures that are followed. Security awareness among customers needs to be strengthened. In order to increase the amount levels, the bank can educate and create awareness to ensure that customers understand. For example, the bank's customer due diligence may need to demonstrate that customers have a duality process in place and are working in line with it, in order for the bank to approve other amount levels.

Remote access tools

Customers are also tricked into installing remote access tools on their phone or computer, giving the fraudster complete control over their screen and keyboard. Customers are rarely familiar with how this technology works and how products function. The fraudster can then set up transactions in the customer's bank, which the customer is then tricked into signing.

The challenge posed by remote access tools is that it is legitimate software. In order to counter remote access, banks are attempting to identify and analyse behavioural patterns regarding how customers use computers and apps.

It would be effective if banks could detect when remote access tools is being used on a computer, a service or a session. The bank could then refuse all payments or choose to close the service or session, for example. If banks had such tools, it would make things much more difficult for fraudsters, and many fraud offences would be stopped.

Artificial intelligence

Fraudsters are already employing an automated and robotised approach, and banks need to monitor developments as regards the use of AI by fraudsters. Banks also have the opportunity to use such technology in their crime prevention efforts. Automated conversations are used in some fraud schemes via social media and chat apps. Banks expect better quality when it comes to language and design, as well as increased scalability when it comes to future phishing, smishing and vishing schemes.

The risk is that modus operandi used against business operators, including BEC scams such as CEO fraud, will be enhanced with elements of AI, through voice cloning, recorded messages or other means. Banks consider that it may become increasingly difficult for a bank to assess whether or not a customer who is a victim of fraud has been

communicating with a real person. Technological developments will entail even greater challenges for both banks and customers when it comes to distinguishing between what is fraudulent and what is genuine.

Monitoring customers requires data

Customers today complete many banking tasks themselves, and so it is becoming increasingly important for banks to be able to interpret their customers' behaviour and identify discrepancies. Banks work systematically with preventive methods, such as limits and restrictions within products. Monitoring customers' transactions is therefore an important tool for banks. The more data points to which banks have access, the more accurate their assessments will be.

If legislation were to allow more data sharing, for example of straw men registers and IP addresses, this would contribute to better risk assessment and monitoring. When banks no longer control the technical interface in apps or payment platforms, for example, they have less data to analyse, making it harder to monitor transactions and track flows. The fraud and money laundering controls at banks are also hampered if transactions are routed to collection accounts, rather than directly to the actual recipients. The emergence of real-time payments is further increasing the need for accurate risk models and dynamic restrictions in order to act quickly.

Advantages and disadvantages of increased data sharing

Increased data sharing in the financial sector is both a prerequisite for better risk management and a source of new threats. Regulations such as the Financial Data Access Regulation (FiDA) aim to create a more interconnected financial ecosystem, in which banks and other actors have access to more information than before.

This can enable more efficient credit assessments, more tailored financial services and increased competition. At the same time, it means that the attack surface for cybercriminals is growing, as a more open data flow grants more parties access to sensitive information. If security at one actor is inadequate, this can have consequences for the entire financial ecosystem. Cybercriminals can exploit the vulnerabilities in order to steal or manipulate data. The manipulation of data, in the form of small, invisible changes, can affect credit ratings and risk analyses and lead to incorrect decisions with major financial consequences.

The regulatory framework has to balance the need for increased transparency with the requirements of responsible data management. With more actors sharing sensitive information, liability issues are becoming increasingly complex, and clear rules are required to ensure that all data is protected. Customers also need to understand who is processing their data and what risks exist.

Fraudsters map their victims

A trend that has intensified in recent years is the fact that fraudsters are becoming increasingly skilled at mapping their intended victims in various target groups. Open internet search services allow fraudsters to see a person's social security number, address, income and other information. Using this information, the fraudster builds up a credible story with the aim of manipulating the intended victim. Fraudsters often hide behind masked phone numbers, where the fraudster chooses which phone number is to be shown on the display. It may then look like it is the bank that is calling.

Fraudsters also access data through data breaches. In this case, they will have access to more informative and accurate information, enabling them to better target their attacks. In addition to using open sources to expose a particular group to vishing and smishing, there are examples of individuals carrying out work for telecom operators' customer base and then using that data for fraudulent purposes or selling it on. Other examples are when the "health centre" calls the customer when the customer has been there as a patient earlier that day.

Home visits continuing

The number of home visits by fraudsters, for example claiming to be bank officials, police officers and home care workers, continues to be a problem. This can also take the form of physical outreach, such as a fake transport services. The transparency of Swedish society, where personal data is open, makes targeting easier for fraudsters.

The fraudster's pretext is often to "help" with an alleged problem, while the purpose of the home visit is to steal valuables or to access the customer's bank card and e-identification. One trend being witnessed is that home visitors appear to be physically forcing their way in to a greater extent now than in the past.

There is a real risk that the number of home visits will increase, and thereby that personal risks will increase, in line with the bank blocking the potential for other approaches. This needs to be taken into account as part of work to combat fraud. In late 2024 and early 2025, the number of home visits is increasing significantly.

Credit fraud

Credit fraud has long been a common phenomenon. Understanding the various credit fraud schemes – at all stages of the credit cycle, from application to repayment – is challenging. The amount of false documentation remains at a high level. Credit fraud can be carried out in several different ways in each stage, and several parts of the chain can be involved. It can be difficult to get an overview of the scope of the fraud. If banks receive incorrect information from the authorities, which they then use as a basis for their credit decisions, preventive efforts are affected.

In the case of business loans, this often involves taking out a wide variety of loans in parallel over a period of time, during which a company can be used as an instrument of crime. This can include regular business loans, more rapid business credit, and making large purchases on credit of expensive goods such as machinery, equipment or vehicles. The company receiving the credit is generally represented by a straw man.

Since creditors always need to carry out some form of verification of the existence, creditworthiness and ability to pay of the person or company, it is consequently a matter of manipulating the system so that their creditworthiness appears to be better than it actually is.

One common scheme involves an individual taking out as many large loans as possible from different lenders over a short period of time, with no intention of repaying them, and often with the intention of lying low or leaving the country. The fraudster takes advantage of the fact that the different creditors are not able to share information up until the moment when information starts to appear in the credit reports. The aim is to maximise the proceeds of crime in as short a time as possible.

Another common scheme is where a person takes out long-term credit, such as a mortgage, on false grounds. Individuals who do not have a credit rating create a false picture of their financial position. As long as the person complies with the agreed loan terms, the chances of the fraud being detected are often low. Interest in credit fraud increases when interest rates are low.

Payments, instalments and the redemption of credit represent another risk area, as it can be a money laundering scheme. All credit payments should be checked against the customer due diligence data. If the origin of the funds is questionable, the bank is in a difficult situation with regard to how the customer relationship should be managed. There is also a danger of cases becoming complex very quickly.

Requirement for resources to prevent credit fraud

Countering credit fraud requires a great deal of resources and extensive analytical work. In addition, customer management, staff training, amended processes and monitoring are all required. Examples of credit fraud in the area of consumer credit include straight rollers and bust-outs, i.e. people who take out several loans in a short space of time with no intention of paying. Analyses of straight rollers have resulted in changes to onboarding processes in order to detect warning signs at an early stage. Estate agents are increasingly acting as enablers, particularly in private housing transactions, but also in the corporate sector.

If information about revoked residence permits could be updated and shared with banks on an ongoing basis, they could block more credit applications from people who disappear from the country.

The Swedish Tax Agency's changes to the confidentiality rules in 2024 regarding income from employment and income from business activities have made it more difficult to ascertain where income originates from. This was previously specified, but it is now no longer possible to distinguish between income from employment and income from a sole proprietorship.

As credit fraud is based on one or more false pieces of data, a number of banks have started to use external services to check customers' income data. However, false information about income is also registered with Swedish authorities, making it more difficult for the banks to rely on the information regarding identities and family relationships. As it is easy to change the data that is reported to authorities, the control mechanisms are being partially compromised. Given this trend, all actors and stakeholders need to increase their training efforts and thereby raise the level of knowledge about credit fraud.

Investment fraud

Investment fraud is a growing problem. The number of unrecorded victims and the hidden proceeds from this crime are probably large. Fraudsters exploit people's desire for high returns against low risk on the money they invest.

The fraudsters (principals) are often located abroad, and initial contact nowadays takes place primarily through social media advertisements, e-mails or recommendations from friends and superficial acquaintances. Fraudulent schemes are largely carried out via digital platforms, using the names and images of famous people in advertisements to create false confidence.

Fraudsters take advantage of customers' lack of knowledge about complex investment vehicles, such as cryptocurrencies. In order to increase credibility, fraudsters create fake websites where victims can log in and watch "their invested money" grow. The data shown on the screen is completely fictitious. The victims' money has never been invested in any assets, rather it has gone straight into the fraudsters' pockets.

The fraudsters have often been in contact with the victim over an extended period of time. It may take time before behavioural patterns and transactions start to deviate significantly from the customer's normal behaviour, causing the bank to start asking questions. In addition, it is not uncommon for the fraudster to provide the customer with a script of answers to future questions from the bank. This makes it challenging for banks to detect and halt an ongoing case of fraud. This is because the bank receives answers to its control questions, as well as supporting documents.

In some cases, victims are encouraged to take out loans to finance additional investments. In other cases, loan applications are initiated in their identities without them being fully aware of what is happening. Remote access tools are commonly used in investment fraud, in order to take control of the victim's computer.



One trend that has intensified is the fact that fraudsters are becoming increasingly good at mapping their intended victims.

By signing orders, sometimes without understanding what they are authorising, victims risk losing a lot of money. Just as with other forms of social manipulation, fraudsters play on giving the impression that victims need to act quickly.

Customers transfer money in order to make an investment that is promised to be significantly better than both the banks' return on their accounts and the realistic return on investments. When the investment appears to have grown and the victim tries to withdraw their money, the fraudsters make this difficult by claiming that fees and taxes need to be paid. This causes the value of the investment to suddenly drop dramatically, often causing the victim to start to realise that they have been scammed.

In many cases, victims are subsequently contacted by additional scammers posing as government agencies or law firms offering to help recover the money. This help obviously comes at a cost, resulting in the victims being exploited once again.

As the contact with the fraudster often takes place over an extended period, the victim initially tends to trust the fraudster more than their own bank. A negative tone in the public debate regarding financial companies influences the relationship between bank and customer. Banks devote considerable resources to talking with their vulnerable customers, but it is very difficult to get them to change their minds. The customers themselves often deny how

much money they have sent off and how long the situation has been going on. For the bank, it is also challenging to understand whether the customer is a victim of fraud or whether they have just made a bad investment.

Straw men enable fraud

In this context, straw men are enablers of financial crime, and the number of straw men in Sweden remains a problem. Criminals who are discovered in one bank quickly switch to another bank and continue their criminal activities there. The banks work in a structured way to analyse and counteract the opportunities for straw men to commit repeated crimes.

Straw men and straw men accounts are a prerequisite for fraudsters' activities. There are a large number of money laundering straw men operating in Sweden. According to the police, over 80,000 people were registered as being reasonably suspected of fraud offences during the period 2018-2021. But there are probably also a large number of unreported cases. A functioning flow of information between banks and the police is therefore crucial to increase the effectiveness of law

enforcement. Without such information sharing, it will be difficult for banks to counteract the room for manoeuvre enjoyed by straw men and prevent fraud and money laundering.

Young people are often exploited and used as straw men, which can be a gateway to more serious crime. One scheme might involve a young person being lured with the promise of earning SEK 10,000 quickly in return for receiving and forwarding SEK 250,000. This can subsequently lead to threatening situations when the young person wants to back out.

Another way of recruiting straw men is to first subject the person to an investment fraud. The person is manipulated into making an “investment” in the belief that it will yield high returns. The person is initially cheated out of small amounts, although these often quickly escalate to larger amounts. When the customer exhausts their own funds, they are encouraged to borrow money to invest further. The customer risks ending up in a desperate situation, where they will do anything to get their money back. In the end, the customer risks allowing themselves to be used as a straw man to “save the investment”, by receiving and forwarding money. The money may come from other affected customers, which could ultimately entail money laundering. Cryptocurrencies are often used to move money in vishing and investment scams.

The Swedish Bankers’ Association’s programme against fraud – Increased customer protection

Telephone fraud increased significantly in 2023, and the Board of the Swedish Bankers’ Association therefore decided in December of that year to issue a recommendation to banks regarding measures to increase customer protection against fraud. The recommendation focused on vishing and smishing (fraudulent calls and text messages) and was conducted in cooperation with the police. It was presented in May 2024.

The measures, which are to be implemented as soon as possible, although no later than 2025, include:

- Limits (ceiling amounts)
- Time delay.
- Potential for duality (two people must approve the transaction).
- Review of products provided.
- Checks in connection with new products.
- Improved transaction monitoring.
- Information and training.

The major banks had most of these measures in place by the end of 2024. The initiative has received positive feedback from customers.

Straw men are a prerequisite for fraudsters’ activities, and there are a large number of straw men in Sweden.



The impact of these measures on fraud trends is being monitored together with the police. Police statistics are showing a 40% fall in criminal proceeds from vishing between 2023 and 2024, as well as a clear decline in the average amount per vishing offence. The strengthened issuing process for Mobile BankID has resulted in the virtual elimination of unauthorised transactions when issuing Mobile BankID.

Lack of statistics regarding fraud

Banks are working to better understand what measures will have what impact for Sweden. It is easy for an individual bank to understand its own measures, but it is more difficult to understand the effect of a measure in all police reports in Sweden.

The statistics provided by the police, the Swedish Financial Supervisory Authority and the European Central Bank are primarily intended for their own use, and it is difficult to draw any conclusions from this data. Police statistics do not illustrate the actions of the banks or the police, whether transactions are

authorised or unauthorised, or whether consumers or businesses are affected. The police data is complex, and it is difficult to obtain information about the proceeds of crime from methods other than telephone fraud. The police therefore need to develop the opportunities to report crime, in order to strengthen analytical capacity and decision support, and steps have been taken in this direction.

The assessment is that joint crime prevention efforts by the banks have been very successful. The risks of fraud and financial crime remain high, however, and at the same time the threats are becoming increasingly complex and collaborative through combined approaches in the same criminal scheme.

Need for action by politicians and authorities

- The legislator should restrict the publication of personal data online. It is currently all too easy to identify single elderly people with good finances, for example. At the same time, the change needs to meet the legitimate needs of banks to be able to perform various types of checks.
- Telecommunications operators working in Sweden should be required to make it more difficult/impossible to mask phone numbers by means of an anti-spoofing infrastructure for phones and text messages.
- The Government should implement the proposals set out in the ID card inquiry (SOU 2019:14), to reduce the number of issuers of physical ID cards and improve opportunities for banks to verify ID documents. The physical ID document links the physical identity with the digital identity in two directions: first when the bank issues the BankID and then as an additional verification option when the e-identification is used, based on the bank's risk monitoring.
- Banks should be able to share information with each other more easily. A flow of information between banks and the police is also required, such as information about straw men. For banks, the aim of effective information sharing is to strengthen customer due diligence, customer risk assessment and transaction monitoring.
- The Swedish Police Authority should develop the opportunities for victims of crime to report all the most common forms of fraud to the police online. The limited opportunities available at present to report crimes to the police – it can take a long time to get through via 114 14, for example – pose a risk of there being many unrecorded crimes.
- The most important measures to counter investment fraud are:
 - 1) Tech companies must assume more responsibility for what is published on their platforms. Platforms such as Facebook, WhatsApp and Instagram are major enablers of fake advertisements published on their sites that trick customers, for example through investment scams. The platforms should therefore raise the minimum requirements for being able to advertise in order to eliminate, or at least reduce, the number of fraudulent advertisements on various platforms.
 - 2) Banks must be better able to track the use of remote access tools. Remote access is very common in investment fraud. Under the pretext of helping the customer, the fraudster takes control of the victim's device through tools such as Anydesk and TeamViewer, and can then perform fraudulent transactions. Suppliers of this type of tool should therefore be required to offer an API that enables banks to detect whether remote access is being used for a customer.



Society does not want money that stems from crime. Any proceeds of crime that cannot be used are basically of no value.

Money laundering

In practice, money laundering encompasses a range of different money laundering activities. This might be transactions involving the proceeds of crime moving between different bank accounts or turnover through purchases, as well as other actions such as using false documents that represent a value. Money laundering can be preceded by relatively simple crimes involving individual actors, or by complex criminal schemes, often involving a whole chain of actors acting in concert. A person who is guilty of money laundering within the meaning of the law is convicted of a money laundering offence or commercial money laundering offence.

For the banks, money laundering normally manifests itself as transactions involving the proceeds of crime moving between different bank accounts. Good customer due diligence procedures and appropriate monitoring of customer behaviour are therefore the most important tools for a bank to detect and prevent money laundering. Monitoring is carried out on an ongoing basis to detect anomalous activities and transactions.

Of all money laundering detected in Sweden, the majority is believed to take place through the regular financial system. It is also conducted through cryptocurrencies, the gambling market, Hawala banking (an alternative payment system primarily for international money transfers outside the banking sector, which from 1 July 2025 is required to be licensed by the Swedish Financial Supervisory Authority) and trade in goods and services.

In 2024, a total of 52 831 reports of suspicious transactions and 8 509 reports of suspicious activity were submitted to the Financial Intelligence Unit (FIPO), which was a rise of 4% respectively 54% compared to 2023. Banks account for the overwhelming majority of reports. In total, the financial sector was responsible for over 90% of the reports in 2024, according to FIPO's statistics.

The main money laundering threats

Society does not want money that stems from crime. Any proceeds of crime that cannot be used are basically of no value. Money laundering occurs when criminals try to hide the origin of their criminally earned money.

Criminals often demonstrate great ingenuity when it comes to finding new ways to launder money. This may involve investing the proceeds of crime where turnover potential is high and controls are inadequate. There are also areas where money laundering controls cannot yet be satisfactorily exercised, such as cryptocurrencies.

The international payment system is also used to carry out criminal exchanges beyond the control of a particular country's authorities. Transfers may take place to or from countries that do not cooperate with Swedish authorities, or where cooperation does not work effectively. During 2024, Swedish authorities stepped up their efforts to expand international judicial cooperation in criminal matters, which may include tracing and securing misappropriated assets. The impact of the agreements that have been entered into regarding legal assistance and extradition of suspects remains to be seen.

The primary threats to efforts by banks to combat money laundering and terrorist financing are posed by organised crime, which uses the services and products provided by banks for criminal purposes through the use of straw men, front men and legal entities, but without exposing themselves personally. Another aspect of anonymity is the limited information that can be obtained about counterparties in payments resulting from the rapid development of alternative payment solutions. Because money laundering can be carried out in so many different ways, monitoring developments and taking effective countermeasures quickly represent a challenge.

Official controls in relation to money laundering

The national anti-money laundering regime has shortcomings, with the result that in some cases the state may support or facilitate criminal activities and money laundering. Many rules are designed according to conditions that are no longer relevant, while existing phenomena are not covered by current regulations.

In some cases, authorities and business regulations are not sufficiently adapted to the threats posed by organised crime. This is reflected, for example, in poor or non-existent controls on businesses and individuals, which enables welfare and tax crime.

Money laundering schemes that are difficult to detect

As a bank can only see the portion of a transaction chain that has taken place within its own operation, sophisticated money laundering chains involving transactions in several banks are often difficult to detect. Banks have only limited opportunities to share information with other banks.

To counteract the rise in fraud offences, Swedish banks have implemented both technical improvements and restrictions in relation to their customers. This has led to changes in money laundering practices.

The number of potential ways to carry out transactions has increased in recent years, a trend that is expected to continue in 2025. In some cases, this has resulted in a reduced understanding of the origins of money and a reduced ability for banks to monitor and limit a customer's services based on the type of transaction. As a consequence of this, banks are facing challenges when it comes to effectively monitoring and responding to transaction types that have been assessed as constituting a high risk.

Financial intelligence centre

In December 2024, the Government tasked the Police, the Swedish Economic Crime Authority and the Swedish Tax Agency with setting up a financial intelligence centre (Finuc) during 2025, in consultation with the business community (banks etc.). Finuc will entail increased and lasting cooperation between the authorities and the business community in areas such as money laundering. The overall aim is for the parties to contribute jointly to the disruption of the illicit economy through effective information sharing and tangible actions.

Finuc has been operational since 1 April 2025, but the centre's activities will gradually be built up over an extended period of time. The expectation in the longer term is that Finuc will be able to act quickly and effectively both for crime prevention purposes and in relation to advanced money laundering schemes. This is an essential initiative, but it remains to be seen whether the legal framework will allow sufficiently effective information sharing and other forms of collaboration.

Welfare crime and tax crime

Whenever new state or municipal grants or subsidies are established, they attract the interest of criminals. This was clearly demonstrated in connection with the payment of financial support related to the Covid pandemic, electricity support and environmental promotion measures.

Criminals also analyse tax legislation and tax procedures in the EU and Sweden, in order to identify gaps and shortcomings and tailor criminal schemes. Such criminal schemes are used, for example, by international criminal organisations that set up a criminal corporate structure in Sweden.

The exploitation of the welfare society and the tax system by criminals poses a particular challenge for banks, as the payments come from highly trusted senders, i.e. public authorities. It is difficult for a bank to check whether there has been an underlying crime, in which authorities have been misled into making payments on incorrect grounds. Moreover, the recipients tend to be ordinary people or companies where there is no reason to suspect that they would not be entitled to receive the money.

The checks must therefore be carried out in the first instance by the determining or paying authority. As of 2024, a new authority, the Swedish Payment Authority, was established with the task of checking payments from welfare systems. Once the Authority is up and running and carrying out its mission in full, we can expect to see a reduction in incorrect payments within the framework of welfare crime. This in turn will reduce the banks' risk of transferring the proceeds of crime and thereby money laundering.

Property market and housing associations

The property market is attractive when it comes to money laundering, as real estate can be used in many different ways and requires large investments. This means that large sums of money obtained from crime can be laundered with a single purchase. The property can then be utilised for personal use, rented out or sold on. Additional money can be laundered through investments in the form of renovations and extensions, for example, which can also help to generate added value. Companies in the construction industry appear relatively often in investigations by banks into suspected money laundering.

Generally speaking, there is an interest in property transactions being carried out quickly, which in many cases is in conflict with an interest in conducting checks. Estate agents may fail to conduct money laundering-related checks, or may conduct such checks without sufficient rigour. In an increasingly pressured and competitive property sector, it is important not to deviate from the requirement to conduct appropriate checks.

Housing associations are vulnerable to money laundering. Money laundering schemes occur where values can be transferred between different individuals through undervaluation or overvaluation of the item when

buying or selling. Mortgages that are granted under false pretences can be used to finance these schemes.

Crypto-assets, payments and currency exchange

Crypto-assets, including cryptocurrencies, are a relatively new sector that is extremely vulnerable to money laundering. The market is global and volatile. Several of the world's largest actors are registered in countries with inadequate anti-money laundering regimes or with privacy rules that prevent transparency. Cryptocurrencies are often used as a means of payment by criminals in illegal trading on, for example, the Darknet and in ransomware attacks. In cases where cryptocurrencies can be purchased using bank cards, a link is created between the traditional financial system and the crypto market.

Cryptocurrencies have also become an increasingly common means of payment, both in the retail sector and between individuals, which is also increasing the risk of money laundering. However, with an increased focus on cryptocurrencies, businesses are becoming more aware of the risks of accepting them as a means of payment.

Particular high-risk groups are those providing services related to cryptocurrencies, such as payment intermediaries and currency exchangers. They are currently not subject to the same extensive rules that apply to banks, and some are still completely unregulated. In many cases, they have inadequate processes and controls for preventing money laundering, while at the same time using the banks' infrastructure and thereby transferring their own risks to the bank. In transactions involving crypto-assets, the funds go to a large extent to intermediaries of services whose recipient accounts are located in the former Eastern Bloc.

One increasingly significant risk is that countries and other actors are using cryptocurrencies to circumvent international sanctions. Cryptocurrencies have


proven to be useful in replacing globally viable currencies such as the US dollar. Furthermore, trading in cryptocurrencies can be an alternative for those actors who are excluded from international payment systems by sanctions.

International cooperation with corresponding regulations, definitions and standards could be crucial when it comes to controlling the cryptomarket and thereby reducing the risks of money laundering in future.

However, while sales of crypto-assets are vulnerable to money laundering, they offer greater opportunities for analysis than cash. A great deal of data regarding crypto-asset transactions is publicly available on the internet. Analysis of this data represents both an opportunity and a growing challenge for stakeholders on the market and law enforcement agencies.

In December 2024, the EU's new Markets in Crypto-Assets Regulation (the MiCA regulation) entered into force. MiCA aims, for example, to facilitate legal certainty for businesses and to attract more investment to EU countries. The EU is now the largest jurisdiction in the world to have introduced a comprehensive regulatory framework for the crypto market. What impact MiCA will have in practice remains to be seen.

Payment services and currency exchange, whether conducted on a professional basis or otherwise on a larger scale, are also vulnerable to money laundering. There are examples of such businesses that are run by criminals. As they make use of the payment infrastructure of banks, they affect the vulnerability of banks. In recent years, regulations have been introduced to increase the demands placed on currency exchangers, among others, which should help to reduce the risk of money laundering.



Sophisticated money laundering chains involving transactions in several banks are often difficult to detect.

Luxury goods and vehicles

The market for goods and services in the luxury segment, such as jewellery, watches, gold, designer clothing, travel and hotels, has grown over time. This market attracts criminals, both as an instrument for laundering money and as an investment for criminal assets. Payments are often made in cash or using other means with an unclear background. Many of the luxury goods are easy to move from country to country, and to resell while retaining their value. This enables them to be used to transfer value without sufficient traceability.

One common arrangement is to buy a luxury item in cash from a merchant and then return it. The merchant then does not have as much cash available, rather the money is refunded in the form of a deposit in a card account (in violation of the card regulations). This enables cash with a criminal background to enter the financial system.

As regards the trade in vehicles, mainly passenger cars, there are various money laundering schemes. In some cases, the purchase sum comes from the proceeds of crime that have been laundered through various channels, such as fake loan agreements and foreign bank accounts. There may also be criminal schemes involving importing or exporting vehicles that have been purchased with the proceeds of crime, as well as schemes to evade taxes or duties.

Gambling

The gambling sector entails a high risk of money laundering. Gambling company accounts can be used for money laundering purposes in such a way that money is stored and mixed together with other funds. This in turn means that when withdrawals or transfers are made from the gambling accounts, the origins of the money may appear legitimate. The gambling sector also handles cash to a relatively large extent, which is associated with particularly high money laundering risks.

Gambling fraud generates criminal proceeds that are paid out to the people involved. Such crime has elements of corruption and tends to be particularly difficult for authorities and other actors to detect.

Gambling companies can be both online-based and traditional casinos at physical addresses (Bill 2024/25:73 does, however, propose the phasing out of state-owned casinos). Online-based companies are often located in low-tax countries. Although the market is regulated by and subject to anti-money laundering regulations, there are numerous unlicensed companies. The fact that the gambling companies' professional associations promote good practice and the dissemination of knowledge among their members should help to reduce the risks in this area in the long term.

Need for action by politicians and authorities

- The risks of money laundering and terrorist financing need to be covered by the same regulations and supervision, regardless of where they arise. If banks are to be able to provide accounts for high-risk operations, the regulation and control of such operations needs to be significantly improved.
- In order for the measures to combat money laundering and terrorist financing to be effective, banks need to be better able to share information about suspicious customers, transactions and activities with each other. Organised crime takes advantage of the fact that banks are currently unable to share information between themselves. When criminals are discovered in one bank, they immediately switch to another bank and continue their criminal activities there.
- The new rules regarding cooperation and the sharing of information between banks and authorities investigating crimes are a step in the right direction, but they need to be further developed. By employing permanent forms of collaboration, it is possible to build up the necessary experience and trust between the various parties and achieve results. The establishment of Finuc is a welcome initiative for a more efficient sharing of information between affected parties. However, Finuc needs to be given the legal conditions to operate appropriately and effectively, with a wide range of participants and with a view to combating various types of financial crime.
- The police's Financial Affairs Department needs sufficient resources to rapidly handle and provide feedback on all suspicious transaction reports submitted by the actors covered by the money laundering regulation. If decisions to freeze assets are not taken promptly, there is a risk that criminal money will be transferred beyond the control of banks and authorities.

The assessment is that as long as crime that generates financial criminal proceeds remains at a high level in society, the risk level for money laundering will remain high. Banks are constantly seeking to mitigate their risks, mainly through good customer due diligence practices and appropriate transaction monitoring. The level of control in the public sector and the welfare system needs to be further increased in order to restrict the conditions for carrying out such crime that precedes money laundering.



Use of businesses for criminal purposes

There is growing awareness of the extensive use of businesses by criminal actors to commit crimes. Although the phenomenon has been widespread for a long time, there has been an increase in recent years.

In general, this relates to the criminal exploitation of small or medium-sized limited companies. However, criminal elements may also be present in large, reputable companies, where some of the activities may be targeted at areas such as tax evasion, thus gaining a competitive advantage. The use of sole proprietorships, partnerships, limited partnerships or foundations for criminal purposes is less common, but it does occur. In the case of foundations, it is likely that there is some under-reporting.

There are many reasons why businesses are particularly attractive as instruments of crime. They allow criminals to hide behind the company's façade of legitimacy. It is also possible that the company may open the door to other types of lucrative crime, by exploiting the security and stability that a company represents for society or individuals. Criminal actors can acquire large amounts of money in a relatively short space of time with the help of a company. The most lucrative financial crime schemes often affect the public sector.

Low risk of detection

The risk of being convicted of a crime has long been relatively low, for a number of different reasons. The most important reasons probably include a lack of opportunities and obligations as regards control and information sharing between authorities and other actors involved in the establishment and ongoing operation of a company. Furthermore, preliminary investigations regarding criminal activities within a business can frequently be aimed at investigating a specific type of reported crime, while there is a lack of resources for a broader approach encompassing all types of crime that are detected.

Types of crime

A business can be used to commit various types of crime. Common examples include the use of illegal workers (tax crime), VAT fraud (tax crime), fraud such as credit fraud, and various types of welfare crime. Furthermore, criminal schemes aimed at money laundering via companies may occur.

It is suspected that there may still be a large number of unreported cases. It can be assumed that many cases of money laundering and/or tax and welfare crime committed with the aid of companies are not reported or even detected.

Approaches

Many businesses are set up for the purpose of being used for crime, with weaknesses in various systems being exploited in parallel. The business is used intensively during the time before warning signs at authorities and banks generate questions and action. The company is then deemed to be exhausted and is wound up or abandoned. A last resort may be to exploit a bankruptcy for further criminal gain. When the company is abandoned, it is emptied of assets and only liabilities remain.

Those who carry out the criminal activities in a company rarely take into account interests other than their own. Former employees or operators with whom the company has done business often suffer long-term financial problems. Creditors have little prospect of recovering any money from their claims.

It is often the straw man, i.e. the person who has acted as the formal representative of the company, who is held criminally liable for the crime. In some cases, the straw man may be a young person or a person with weak ties to Swedish society.

Different types of crime are often carried out within one and the same company, either in parallel or consecutively. It is also common for the same criminal network to run many different businesses at the same time, and to conduct criminal transactions between them. These can include, for example, large-scale and systematic schemes to commit tax or welfare crimes.

Sophisticated criminal schemes

As law enforcement authorities become more effective and regulations are tightened, criminals need to develop their criminal activities. This results in increasingly sophisticated criminal schemes. Legitimate and criminal activities may be combined within the same company. This can be achieved, for example, through sophisticated corporate structures and international connections, cleverly forged documents and straw men with a low profile. Such well-prepared criminal schemes are more difficult for law enforcement authorities and banks to detect.

Advanced criminal schemes can be sold or managed by international criminal networks. The people who commit these crimes in Sweden do not always understand how the overall scheme works and how the proceeds of crime are actually generated.

Supporters and enablers

In order for a company to be operated for criminal purposes, it is necessary for a number of initial steps to be taken. For example, a new company needs to be started up or an existing business acquired.

External actors may need to be involved as supporters or enablers of the crime.

For example, this may be a question of acquiring a so-called historical company (a company with a documented history of apparently legitimate activities) from a business intermediary and thereby carrying out the necessary registrations with the Swedish Companies Registration Office.

In order to create a lasting legitimate façade, criminal schemes often require the day-to-day accounting to be taken care of. In this case, an accounting consultant is then hired to carry out bookkeeping and to submit tax returns to the Swedish Tax Agency.

Criminals often use businesses to commit various types of crime.



Fake invoices, transport documents or other falsified written documents may need to be obtained to support accounting records and as evidence for payments. It is common for external enablers to provide such documents in return for payment.

Other actors, such as legitimate business partners, creditors and banks holding accounts, need to be able to trust, for example, that registrations with the Swedish Companies Registration Office, information from the Swedish Tax Agency and prepared accounts correspond to the actual conditions. Counterparties need to know who they are doing business with or extending credit to, and under what conditions. Similarly, authorities need to know, for example, who is running a business, who is employed and to what extent work is being carried out.

Risks related to banking and business accounts

A business that does not have access to a business account cannot be used, either for legitimate or criminal purposes. For this reason, part of the criminal plan often involves gaining access to an account in a Swedish bank, and in many cases also a foreign currency account. Having an account in a Swedish bank means low transaction costs, as well as suggesting legitimacy in the business.

Banking transactions are often carried out by straw men, or other authorised persons who do not raise suspicions.

From the bank's point of view, the procedure generally appears normal and therefore does not raise any suspicions during an ongoing banking relationship. For example, making changes to the board of directors and operations are normal actions for legitimate operators as well, and do not raise any suspicion in the bank's Know Your Customer (KYC) analysis.

Only when the criminal activity deviates from the norm and, for example, is detected within the bank's transaction monitoring, does the bank launch an investigation and possibly a process to terminate the customer relationship. By that time, it is not uncommon for the company to have already served its criminal purpose and be considered exhausted.

In the case of longer-term crime, where a company or corporate structure is used continually for both legitimate and criminal purposes, the crime is even more difficult for the bank and other actors to detect. Within the framework of such activities, which in certain cases may be carried out by large, reputable companies, criminal transactions through business accounts or international payments may represent only a certain proportion of the total money flows.

Preventing individuals with criminal intentions from gaining access to a company is a challenge for society.

Need for action by politicians and authorities

- Banks must be able to rely on data and payments from Swedish authorities. The state therefore needs to assume responsibility for checking and verifying the information that is contained in state registers, in order to reduce the risk of the authorities being exploited by organised crime.
- The Swedish Companies Registration Office needs to tighten up its controls in order to achieve adequate efficiency and accuracy in the registered data. The Swedish Bankers' Association welcomes the work that has been initiated within the framework of the Government's new assignment for the Swedish Companies Registration Office.
- The activities of accounting consultants must be regulated. State authorisation should be made mandatory, in order to counter criminals' access to accounting services.
- Business intermediaries must be regulated. State authorisation or equivalent regulation should be made mandatory, in order to prevent criminals from gaining quick and easy access to existing or new businesses.
- Finuc needs to be given the legal prerequisites to be able to carry out preventive work in relation to crimes committed with the aid of companies. This means, for example, being able to include important actors such as the Swedish Companies Registration Office, the Swedish Enforcement Authority and the Swedish Payment Authority in the collaboration.

The assessment is that it is challenging for banks to refine their methods for detecting the risk of crime using corporate accounts, including through information sharing and advanced technological solutions. Appropriate and in-depth checks when entering into business relations with companies, especially in high-risk sectors, can help prevent crime.



There are often links between organised crime and terrorist financing.

Terrorist financing

A key risk factor in relation to terrorist financing is that banks do not have access to sufficient and up-to-date information about how such financing takes place and which individuals and companies are involved. If banks do not know what to react to or look for, it will be difficult to detect suspected terrorist financing.

In recent years, the number of cases of suspected terrorist financing via cryptocurrencies has increased. However, for banks that do not offer services related to cryptocurrencies, the risks only increase indirectly.

An increasing overlap between organised crime and terrorist financing is being observed in external monitoring. Extensive and complex international tax crime (such as VAT carousels, which have impacted the Swedish tax system extensively in recent years) requires considerable organisation and significant initial investments. It is not uncommon for these to amount to tens or hundreds of millions of Swedish kronor. The investments may derive from international criminal networks, which in turn may be suspected of having links to terrorism. The proceeds of crime go back in various ways to international criminal networks abroad, and are therefore difficult to trace.

The risks are difficult for banks to detect, partly because the turnover normally appears legitimate and because the paying body in this case is the Swedish Tax Agency.

Other forms of terrorist financing include organised welfare crime, credit fraud, misuse of humanitarian aid and cash smuggling.

Crowdfunding is also used to finance terrorism. In this case, a large group of individuals finance a business or project with small sums. Crowdfunding platforms enable private individuals to launch various types of fundraising at an international level via the internet. For the bank, it is very difficult to distinguish legitimate fundraising activities from those that take place with the underlying intention of financing terrorism.

International terrorism is the underlying cause of many of the world's sanctions. The application of sanctions, for example those issued by the Office of Foreign Assets Control (OFAC, the primary US sanctions authority), in practice greatly reduces the risk of banks inadvertently contributing to terrorist financing.

The assessment is that increased information sharing regarding the methods used as well as relevant actors involved in terrorist financing can reduce the risk of banks participating in transactions that constitute such financing.

International sanctions

International sanctions – or restrictive measures – are part of the EU’s Common Foreign and Security Policy. With a more complex conflict picture and growing geopolitical tensions in different parts of the world, sanctions have become an increasingly important means of exerting pressure on foreign policy.

The purpose of imposing sanctions is to influence the behaviour of the party that has been sanctioned, in line with a particular agenda on the part of the party imposing the sanctions. This might relate to human rights or peacekeeping purposes, for example. Sanctions can bring about changes at a political or state level.

Sanctions are an alternative to more intrusive measures, such as armed intervention. They can also be a precursor to more intrusive measures, i.e. if the sanctions have not had the desired effect.

A number of different countries impose sanctions. Key international actors include the UN, the EU, the United States and the UK. Sweden does not currently issue its own sanctions, but it does implement sanctions that have been determined by the UN or the EU. In practice, Swedish banks also need to take into account sanctions issued by third countries, such as the United States. This is necessary in order to avoid serious commercial risks and, in the long term, risks to Swedish society’s need for a functioning banking system.



Greater geopolitical tensions are leading to more extensive and complex sanctions.

The sanctions may be targeted at

- governments in non-EU countries
- entities (companies) that are financially supporting the policies being targeted by the sanctions
- groups or organisations, such as terrorist groups
- individuals who either support the policies being targeted by the sanctions, or are involved in terrorist activities, etc.

Sanctions apply not only to listed entities, but also to entities that have links to listed entities. In order to comply with international sanctions, banks therefore need to analyse who owns or controls a sanctioned entity. Sanctions may also be aimed at a particular type of product or service that is legitimate in itself, but that the sanctioned party may be using for undesirable purposes.

Developments in the field of sanctions and the sanctions imposed on Russia

In recent years, it has become increasingly difficult to monitor and apply sanctions in a consistent and effective manner. It is not only banks that need to comply with sanctions. The industrial sector, for example, needs to remain constantly vigilant in order to avoid any risk of violating sanctions.

Since Russia's illegal annexation of the Crimean Peninsula in 2014 and the invasion of Ukraine in 2022, the EU has issued unprecedented sanctions against Russian interests. The sanctions are intended to restrict Russia's military capabilities in various ways and to signal that the country's behaviour is unacceptable. The sanctions include travel bans, the freezing of significant Russian assets and an oil price cap on Russian oil exports. At the time of writing this report (May 2025), the EU has adopted a total of 16 sanction packages against Russia. The sanctions imposed on Russia are expected to be further expanded in 2025, including with the aim of limiting the so-called ghost fleet of oil tankers and the suspected sabotage of cables in the Baltic Sea.

Russia is, however, systematically circumventing these sanctions. With the aid of foreign interests, Russian actors have, for example, found ways to import advanced technology that can be used in the war industry or to receive the market price for oil. By changing the names of companies, falsifying documents, front men, etc., attempts are being made to conceal who actually owns or controls companies. The sanctions imposed on Russia are now largely aimed at trying to address this evasion and circumvention, and this is likely to remain a priority within the EU in 2025.

Collaboration in the field of sanctions

Large-scale and systematic sanctions violations are placing increased demands on both operators and authorities within the EU. Having an understanding of the problem is fundamental. Increasingly extensive sanctions and an ever more complex and high-risk situation are posing major challenges when it comes to collaboration in respect of sanctions.

In order for business operators to understand their risk exposure and be able to apply the sanctions appropriately, they need both support from authorities and the opportunity to engage with each other.

Moreover, international sanctions may increasingly interact with complex structures regarding trade and export restrictions, requiring information and analysis.

The assessment is that a growing conflict landscape and ever greater geopolitical tensions in different parts of the world are leading to increasingly extensive and complex sanctions. In order for the application of sanctions to be effective and for the purpose of sanctions to be achieved, as well as to combat violations of sanctions, it is necessary to have increased collaboration and dialogue between actors in respect of sanctions.

Bank robberies, cash in transit robberies and ATM attacks

There have been no bank robberies in Sweden since 2020. In the 45 years that these statistics have been recorded, there has never been such a long period with no attacks of this type. The long-term reduction in bank robberies is explained by the fact that the cash chain from the depository via cash in transit (CIT) companies to ATMs has been bolstered, banks have reduced manual cash handling over the counter and customers are increasingly using electronic payments.


There were no CIT robberies in 2024 either. The last ten years have seen a marked decrease in the number of CIT-related robberies compared with the previous decade. This decrease is explained by more effective protection systems, banknote staining and fewer transport operations, as well as improved collaboration and preventive measures between CIT companies and the police.

There were no attacks on Bankomat AB's ATMs in 2024 either. These statistics include ATMs being blown up or cut open, but not card skimming.

The assessment is that the threat regarding bank and cash in transit robberies persists, but that the number of robberies will remain at a low level in 2025, as will the number of attacks on ATMs.

The last bank robbery in Sweden took place in 2020.





More cash handling in society increases risks to staff as well as the risk of money laundering, as traceability is low.

The challenges in relation to cash

Sweden is one of the countries with the lowest demand for and actual use of cash payments. A well-developed card infrastructure and digital payment solutions, such as Swish, enjoy an extremely high utilisation rate. The use of cash in Sweden is expected to continue the trend seen in recent years, i.e. a decrease of around 10% annually.

Discussions about increasing the use of cash in society are becoming more widespread. Regulation (primarily the legislation on cash in the Payment Services Act), the Swedish Central Bank's responsibilities (e.g. regulatory powers in terms of preparedness for payments in RBFS 2023:3) and various inquiries (the Payment Inquiry and the Cash Inquiry, Fi2024/00068) have the ambition of ensuring the survival of cash for various purposes.

Cash as a contingency solution

Since cash is used to such a little extent in normal conditions, it is not a realistic solution that cash can play a crucial role in the event of a crisis or war event. Quite simply, it will not be possible to scale up cash supply and cash infrastructure to quickly replace large digital payment volumes. These conclusions have been drawn from studies in both Denmark and Norway, as well as experiences from Ukraine.

The focus of continuity and contingency solutions therefore needs to be on increasing resilience in the payment systems that are actually used, as well as in basic infrastructure such as the electricity supply and telecommunications.

Staff safety

Cash-intensive activities create risks for those working with cash. For banks, the security of staff is the most important aspect when it comes to cash. The last bank robbery in Sweden took place in 2020, and the number of cash in transit robberies has also decreased significantly over the past decade. The Cash Inquiry underestimates the security risks that cash entails. If the use of cash were to increase among some merchants, both the risk of robberies and the risk of internal fraud will increase.

Cash creates money laundering risks

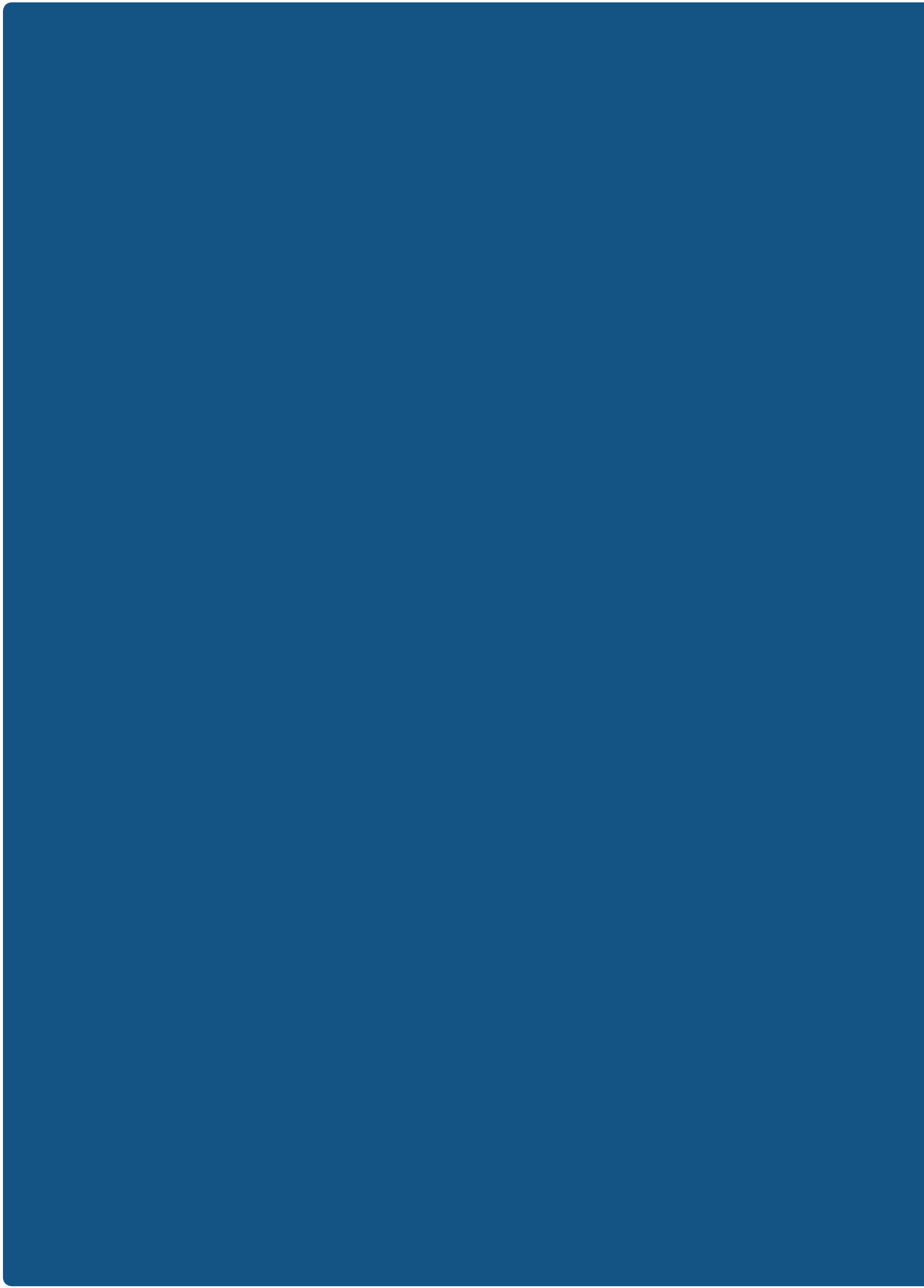
Cash-intensive operations are also associated with a high risk of money laundering. The traceability of cash is low or non-existent, which is a crucial disadvantage in most types of law enforcement. Cash is therefore still an attractive means of payment in the illegal economy. A large proportion of the trade in drugs and illegal services is paid for in cash. Despite the fact that the use of cash is generally decreasing across the EU, there is an increasing need for banknotes, demonstrating that cash is still an important tool as a value preserver.

Banks generally have good control over direct deposits and withdrawals made to a bank, but as soon as the investment phase is outside the bank, for example through cash purchases from traders, wholesalers, gambling companies and restaurants, the bank has more difficulty in understanding where the deposits are coming from.

When cash is exchanged in countries with high levels of cash use and poor controls, and then transferred to a Swedish bank account, it is very difficult for the bank to be able to perform the necessary checks. If money laundering is suspected, banks may need to take measures such as refusing to accept cash from certain foreign currency exchangers.

The difficulty is that it is virtually impossible to trace transaction flows backwards and demonstrate suspicious transactions and transaction flows. This means that various kinds of legal obligations to accept cash will increase the risk of money laundering, and the opportunity to identify criminal actors will decrease.

The assessment is that increased cash handling increases risks to staff and increases the risk of money laundering.





Svenska
Bankföreningen
Finance Sweden

Telephone: 08-453 44 00
Email: info@financesweden.se
www.financesweden.se