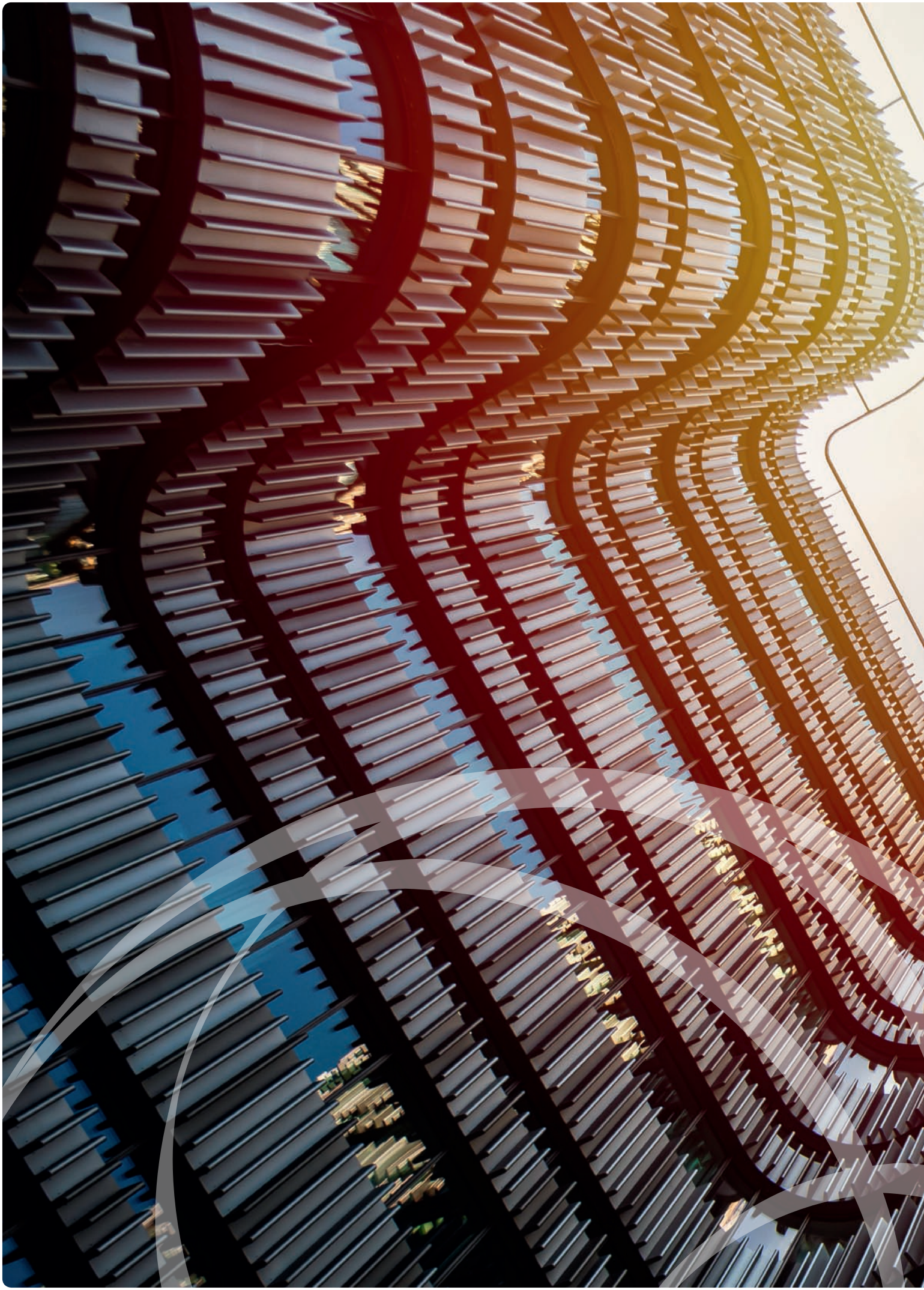
Threat assessment for Sweden's banks

Published May 2026

Svenska Bankföreningen
Finance Sweden



Threat assessment for Sweden's banks

Published May 2026

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 several sections. Each section concludes with a summary assessment, a threat level assessment and a trend indicator. The threat level indicates the current situation, while the trend indicator shows the direction. The model is explained at the end of the report. The section on the threats facing security-sensitive activities is based on open-source information and the security authorities' situation assessments.

Measures that banks cannot implement themselves, but that are considered to have an effect on reducing the threats, are listed as need for action by politicians and authorities.

Summary

Elevated

In the field of **abuse, threats and violence against bank staff**, banks are reporting a continued aggressive tone and aggressive customer behaviour. The exposure of individual employees may increase the threat to the individual, rather than to the bank. A significant proportion of the threats are linked to banks' anti-money laundering efforts, for example in connection with frozen accounts or restrictions to services. Ensuring a safe working environment for bank staff is not only the responsibility of banks, but part of a societal commitment.

Elevated

An i**nsider/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 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.

Elevated

The deteriorating security policy situation means that the threat to the financial sector remains elevated in the area of c**ontinuity and civil preparedness**. Suspected acts of sabotage against critical infrastructure, vulnerabilities in digital dependencies, as well as reliance on foreign IT providers are placing increased demands on banks' continuity and contingency efforts. At the same time, planning for heightened preparedness requires the development of the banks' wartime organisational structure, staffing and coordination, where unclear mandates and regulations currently act as limiting factors.

Elevated

The field of **information and cybersecurity** is characterised by a broader and more complex threat landscape, where cyber extortion is increasingly based on information and identity theft as well as the exploitation of supplier dependencies. At the same time, denial-of-service attacks have had less actual impact due to banks' increased resilience, although the threat remains. Overall, increased third-party risks and the emergence of AI-based attack methods mean that greater demands are being placed on banks' ability to detect, manage and withstand both direct and indirect cyberattacks, the consequences of which could have a systemic impact in a worst-case scenario.

High

Social engineering has made **fraud offences** more targeted and more personalised. The banks' programme of action to reduce vishing fraud have resulted in an approximately 60% reduction from the proceeds of crime in 2025 compared to 2023, as well as a clear drop in the average amount per vishing fraud offence.

High

The **threat of money laundering** remains widespread due to the fact that the illicit economy generates large sums of money every year. Criminals prefer to launder money through the formal economy in the first instance. Any proceeds of crime that cannot be used are basically of no value. There are several risk areas, with the most prominent including cash handling, cryptocurrencies and the trade in luxury goods and vehicles.

High

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 not uncommon for welfare crime and tax crime to generate criminal proceeds. It is common for criminal networks to run a large number of companies and conduct criminal transactions between them.

Elevated

Terrorist financing involves many different approaches, such as the use of crowd funding, hawala and cryptocurrencies. Terrorist financing generally takes place under false pretences and can therefore be difficult to detect. One risk factor is that banks often lack access to up-to-date information about where such financing is suspected and which individuals or organisations may be involved.

Elevated

With growing geopolitical tensions, **international sanctions** have become an increasingly important means of exerting pressure on foreign and security policy. 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. Particular challenges include increasingly sophisticated methods for circumventing sanctions, as well as the growing diversity of sanctions that banks have to take into account.

Low

In 2025, 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 2026.

Low

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.

Elevated

As regards the **threats facing security-sensitive activities**, the assessment is that, within the cyber domain, there is both the intent and the ability to carry out sophisticated and sustained attacks. Capabilities in respect of personnel and physical security are considered to be more limited, involving the use of insiders or basic physical attacks carried out by local actors with limited perseverance.

1 Abuse, threats and violence against bank staff

Many employees and managers in the banking sector testify to a continued high tone and tough customer behaviour. Banks are seeing signs that employees are feeling insecure. The banks consider that the threat level remains roughly the same as last year.

For banks with extensive branch operations, around half of the incidents are linked to physical branches, with the remainder being directed at telephone banking and digital channels.

Changed working methods and new risks

Having a greater focus on scheduled customer meetings is now an established practice within banks. The decision is often business-driven and aims to improve the quality of customer meetings, but it is also related to shorter opening hours. This development has helped to reduce the threat level at the branches, although threats have not been eliminated.

There are still instances of unauthorised individuals forcing their way into bank premises when customers are entering or leaving. Threatening situations can also arise during scheduled meetings, which shows that the threat does not disappear simply by changing procedures.

The shift to digital customer meetings has also given rise to new types of risk scenarios. Employees perceive that customers are more likely to make offensive remarks in phone and web meetings. Harassment on social media also occurs.

Threats related to customer relationship terminations and regulatory compliance

Banks are currently terminating more customer relationships than in the past, primarily due to an increase in the detection of irregularities and threatening behaviour. The higher number of customer relationship terminations is affecting the threat landscape, although the most serious scenarios previously feared have not materialised to any significant extent.

Studies carried out by banks show that a significant proportion of the threats are linked to banks' anti-money laundering efforts, for example in connection with frozen accounts or restrictions to services. For this reason, when a customer relationship is terminated or a person is denied customer status, internal processes are required to assess and manage a potential threat to both staff and operations.

Tools and support for employees

Employees can find themselves in difficult situations, especially when dealing with customers facing financial difficulties. To address this, banks provide conflict management training for staff in branches and call centres, as well as access to various support functions. Other measures to address inappropriate customer behaviour include the bank contacting the customer by phone or sending a warning letter, making it clear that abuse and threats aimed at staff is not accepted.

Perceived and actual threats

Threats can be either actual or perceived. Assessing the seriousness of a situation is a key challenge, since incidents that do not meet the legal criteria for a threat may still be perceived as highly threatening and thereby contribute to an unsafe working environment.

Banks generally have a good capacity to identify threats, but the severity of the threat and the risk of escalation are often difficult to assess. Banks are therefore working to develop methods to better understand and address the threat landscape, for example by drawing a distinction between genuine threats and offensive but empty statements.

Conflicts within the criminal world contribute to a heightened sense of insecurity in society, which in turn exacerbates the perceived threat even in parts of the bank that do not involve direct customer contact. Even though threats are seldom carried out and violence is rare, the working environment is negatively affected.

Differences between various parts of the bank

The threat landscape varies depending on work duties and geographical context. Employees in small towns, who are more likely to encounter customers outside of work, may face a different kind of vulnerability than employees in larger cities or call centre staff who do not meet customers in person.

As mentioned previously, staff who have direct contact with customers are generally the most exposed, although there are also examples of key decision-makers in money laundering and fraud investigations being affected, particularly when customers whose accounts have been terminated direct their frustration upwards in the decision-making hierarchy. For customers whose accounts have been terminated, the customer ombudsman is the person at the bank to whom they are referred. This has led to an increased workload for customer complaint departments and a rise in police reports related to threatening incidents.

Frustration linked to the banks' actions

Requests from authorities, for example regarding transactions related to criminal investigations and subsequent inter-bank measures – such as blocking BankID and Swish – often give rise to significant frustration among customers. A blocked BankID is viewed as a major disruption to daily life, since many private and public e-services have adopted BankID as their authentication method. This measure could lead to threats being made against bank employees, since it is the banks that provide these services. Asking Know Your Customer questions, declining a transaction or refusing to provide a product are common sources of conflict with customers.

Measures by banks to protect staff

To reduce the exposure of individual employees, banks are implementing various protective measures. Employees do not always need to provide both their first and last names during contacts with customers. Other examples include making greater use of central functional mailboxes and limiting external customer contact for staff in certain roles. The issue of aliases is discussed, and it is important that the possibility of using aliases exists, but it is rarely considered justified based on the actual threat landscape.

Employees will sometimes hesitate to represent the bank in legal contexts due to the fear of threats. Reporting an incident to the police often means that the employee is the plaintiff and is thereby publicly exposed. Banks are therefore trying to balance the need for legal action against the risk of further exposure, and to offer support in the event of any legal proceedings.

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

Threats are primarily directed at the parts of the bank that have contact with customers.

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

Need for action by politicians and authorities

- Banks are calling for changes to reduce the exposure of individual employees in cases involving police reports and contacts with authorities. It should be possible for the bank to file a police report and act as the plaintiff. Having a centralised function that can represent the bank in legal proceedings – for example, in fraud cases or to explain in court how a payment service works – can reduce the risk of personal threats and increase employee safety. 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 pointed out, in addition to the threat to which they were previously subjected.

Particularly serious situations – threats of suicide

Banks have noted a sharp increase in threats of suicide by customers over the past year. These situations are very difficult to handle and are perceived as extremely stressful for the individual bank employee. There are specific procedures and support materials in place to guide employees on how to respond, such as encouraging the customer to contact helplines or loved ones. If the bank perceives an imminent danger, it may waive banking secrecy and contact the police.

The assessment is that the threats to bank employees are influenced by the banks' actions under the Anti Money Laundering regulation and other regulatory requirements. Customer-facing roles primarily bear the brunt of regulatory requirements and societal changes.

2 The threat from insiders and enablers

So-called enablers of crime are ever-present, requiring vigilance and adequate measures. An enabler of crime in this context is an employee at the bank who, through their professional role, acts improperly. This may be for personal gain, on behalf of a criminal network or for a state actor. Organised crime and criminal networks represent the primary threat, which means that banks need to adjust their resource allocation and working methods accordingly.

High-risk behaviour and vulnerabilities

The incentives for an external hostile party (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 at the bank 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 hostile parties may seek contact with staff in a bank 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 hostile party 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 from organised crime groups, for example. The Protective Security Act, which often relates to a limited portion of the bank's operations, provides tools and greater opportunities for preventive measures and follow-up, but the threat exists across the entire breadth of the operation, 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.

It is important for banks to have sufficient control options both in connection with the recruitment procedure and during the period of employment. At present, banks need to rely primarily 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 demanding clearer laws, regulations and practices regarding the potential to conduct ongoing checks. When anomalies are found during 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 with each other, to prevent an insider, once discovered, from finding employment at a new bank and continuing their enabling activities there.

The increased mobility in the labour market also raises the question of whether there should be some form of right of communication between banks to address the challenge of insiders.

Information needs of law enforcement authorities

The difficulty is that an insider could be absolutely anyone. 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 when law enforcement authorities 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 the 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.

The Swedish Security Service has identified Russia, China and Iran as the primary sources of intelligence threats. The banks' measures aimed at addressing this type of threat landscape range from technical controls to ensuring that measures are implemented so that employees can feel safe reporting 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 identified links between state actors and criminal networks in Sweden are having a significant impact on the insider problem.

The banks' own control options

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 are aggregated, a different picture can emerge.

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 and enablers are a threat that exists internally in banks and that will persist in 2026.

3 The security policy situation, continuity and civil contingency

Sweden is continuing to face a challenging security policy situation. Russia's war of aggression against Ukraine is affecting the threats to the financial sector in Sweden.

Sabotage against critical infrastructure

The threat remains to the critical infrastructure on which banks depend. During 2025–2026, these threats have been further intensified due to a series of incidents involving suspected acts of sabotage against telecommunications masts, fibre-optic cables and other digital infrastructure. In addition to physical damage, there have also been reports of GPS interference, particularly in the Baltic Sea region. It is therefore considered that the threat remains relevant to Swedish banks. This threat landscape is familiar from the September 2025 report by the Swedish Armed Forces and the then Swedish Civil Contingencies Agency, entitled "Premises for total defence 2025–2030, Scenario 1 – Hybrid threats".

Swedish banks today make up a large part of the Baltic states' financial infrastructure, which also affects the threat scenario. For some of the banks, the three Baltic states and Finland are important domestic markets. The threat landscape facing the Baltic states and Finland is described in the aforementioned report "Scenario 6 – Reinforcement of the alliance's northern flank", which involves Swedish units reinforcing NATO's northern flank in Finland with the aim of defending the alliance's territory. The same applies to "Scenario 7 – Reinforcement of the alliance in the Baltic Region", which describes an armed conflict in the region in which Swedish units reinforce NATO in and around the Baltic states.

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 applies regardless of whether the suspected acts of sabotage are hostile acts or not. It can also 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.

Reliance on foreign IT providers

The financial sector is heavily reliant on foreign IT service providers. However, digital sovereignty issues are now higher up on the agenda, both nationally and at the EU level. Swedish banks rely heavily on IT providers and payment infrastructure from the United States, which has long contributed to a stable and predictable foundation. However, banks need to consider how a shift in US foreign policy could affect access to these services, either directly or indirectly. Although no immediate threats can be identified, it is reasonable to include this dimension in the banks'

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

strategic risk management, particularly given that US political priorities currently tend to shift relatively quickly. Banks need to continuously monitor and evaluate the risks associated with relying on foreign providers for business-critical services.

The banks' contingency and continuity work

Contingency work in relation to civil defence has now been added to the banks' work on continuity, crisis management and security. If an armed aggression on Sweden is used as the basis for business continuity planning, the demands placed on operations are significantly higher than in the case of peacetime crises. In this instance, the business must be able to address issues such as the relocation of data and critical functions, comprehensive backup solutions, as well as the protection of key physical facilities such as offices and data centres. In such a scenario, it would also be necessary to establish and staff a wartime organisation.

In recent years, Finance Sweden has called for clearer coordination and planning among the sector's regulatory authorities, as well as clear planning conditions and guidance on how to prioritise contingency efforts. In 2025, the Swedish Financial Supervisory Authority published a planning framework designed to supplement and clarify the planning principles applicable to civil defence as a whole, adapting them to the specific conditions of the financial sector. A new framework for public-private cooperation regarding contingency issues in the financial sector has also been developed. The new collaboration, known by its Swedish abbreviation FTPOS (Financial Services Public-Private Partnership, formerly FSPOS), is intended to facilitate a more appropriate and speedy development of the financial sector's preparedness.

Wartime organisation, expertise and human resources

The expertise and human resources that banks possess in this area are built up and expanded over time. At the same time, it can be challenging for banks to plan for the right skills and staffing levels in the event of heightened preparedness or, in the worst-case scenario, war. On the one hand, there is a limited supply of personnel possessing both financial expertise and knowledge about total defence; on the other hand, many critical functions within banks may be highly specialised, which could create vulnerabilities in the event of staff absences or mobilisation. Banks need to ensure that their staffing levels can handle peak workloads, infrastructure disruptions and geographical dispersion, as well as parallel crisis or war scenarios. Even in peacetime, however, it is a challenge for banks to secure access to certain key skills in terms of security, IT and emergency preparedness, due to fierce competition for qualified personnel and limited availability of specialist expertise.

There is considerable uncertainty regarding what legal mandate a contingency authority has to identify a specific function and thereby enable banks to conduct availability checks on staff at the Swedish Defence Conscription and Assessment Agency. The Swedish Financial Supervisory Authority, which is the sectoral authority responsible for the financial services contingency sector, has stated in a legal opinion that it considers such identification to be an administrative decision for which it lacks the legal mandate. As a result, banks are currently unable to secure the required staff for their wartime organisation for critical financial services outside the payments sector, which is delaying the companies' ability to establish a wartime organisation. By contrast, the current procedures for monitoring staff availability and mobilising personnel work well for the financial companies that are covered by the Riksbank's regulations on payments during peacetime crises and periods of heightened alert.

Fragmented contingency frameworks and requirements in the Nordic region

Banks operating across the Nordic and Baltic region face challenges as individual countries develop distinct frameworks and requirements for civil defence. Differences in legislation, expectations, governance and planning mean that banks have to adapt their plans in parallel across multiple jurisdictions, which increases complexity and costs. This can lead to conflicting objectives, when a solution that meets the requirements in one country is insufficient or even impossible in another. This hinders the development of a cohesive and effective emergency response structure for the entire group.

Contingency work in relation to civil defence has now been added to the banks' work on continuity, crisis management and security.

Need for action by politicians and authorities

- It is important for planning and coordination between the Swedish Financial Supervisory Authority, the Swedish Central Bank and the Swedish National Debt Office to be put in place in 2026.
- 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. Finance Sweden welcomes the Government's submission of a bill to the Swedish Parliament in the spring of 2026 regarding the crisis management function. Since the Riksbank, the Swedish Financial Supervisory Authority and the Swedish National Debt Office are to collaborate within this function, it is important for the governance of the function to be clear and not overlap with the work carried out within the Financial Services contingency sector.
- Adopt the proposals from the Royal Swedish Academy of Engineering Sciences' (IVA) Resilient Digital Infrastructure project from 2025, which has identified concrete measures to strengthen Sweden's digital resilience. Finance Sweden has participated in and sponsored this project. Relevant examples from the project that would also strengthen the banks' resilience include:
  - The Swedish Post and Telecom Authority is authorised to coordinate and gather monitoring data from fibre owners and other relevant stakeholders. Data from fibre monitoring will be integrated into national situational awareness assessments, enabling a faster and more precise response to incidents and helping to prevent them.
  - The expansion of the power grid will continue in order to minimise the risk of power outages.
  - The Swedish Armed Forces, in collaboration with the telecommunications operators, are developing a solution for international roaming in the event of the loss of digital contact with other countries.

  To ensure the success of cross-sector proposals of this type, it is important for the authorities responsible for each sector to jointly coordinate efforts to enhance the capacity of Sweden's infrastructure. Financial institutions are dependent on other sectors, such as electronic communications and electricity supply, to ensure that the financial system continues to function even during crises and, in the worst-case scenario, wartime. There is a need for a structured dialogue with related sectors regarding interdependencies and how financial activities that are critical to society should be prioritised in the event of a shortage of resources. Common prioritisation principles and a shared assessment of the situation are essential for avoiding conflicting objectives and ensuring that critical financial functions can be maintained.
- Implement measures that enable banks to conduct availability checks on relevant personnel working in societally critical financial services.
- Increase the coordination of Nordic and Baltic regulations and requirements for civil defence applicable to private operators. By agreeing on common Nordic principles, basic requirements and planning assumptions, it is possible to create better conditions for effective contingency planning for companies operating throughout or in parts of the region, without compromising on national responsibilities or security policy needs. Specific national requirements should be clearly justified, proportionate and coordinated. Such an approach would strengthen resilience, reduce the administrative burden on private operators, as well as contribute to a more robust and cohesive civil defence system in the Nordic and Baltic regions.
- The Government should adopt a comprehensive national approach to Sweden's dependence on foreign IT services, as the issue concerns the fundamental continuity of operations that are critical to society. These dependencies extend far beyond the banking sector and affect the functioning of society as a whole, justifying clear signals from the authorities regarding the strategic importance of this issue. Such an approach should be based on the perspectives of continuity and resilience, rather than on individual suppliers or countries.

The assessment is that banks are affected by Sweden's security situation and the impaired 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 in their own operations. Regardless of the outcome of Russia's war in Ukraine, hybrid threats will not disappear, and banks have to continue focusing on capacity building and resilience. Finance Sweden considers that the improvements that have been implemented have created better conditions for effective contingency planning in the sector.

4 Information security and cybersecurity threats

A shift in the cyber extortion threat – information theft, false threats and supplier risks

During the period, various types of cyber extortion attacks have continued to affect a large number of organisations. In the past, ransomware attacks have been the most common method, where data on the victims' IT systems is encrypted. The trend shows that data is not only being encrypted during attacks, but is also being stolen, with the actors responsible threatening to post the information publicly on the internet unless a ransom is paid. There are also cases of extortion involving false information that is more or less credible. The threat actors pretend to have stolen data and threaten their victims. The result is that resources still have to be devoted to investigating the incidents.

For many of the most active threat actors, information theft is the method of choice. Stealing information is faster and can be done more discreetly. It is also possible to attack more victims in a short period of time, with a higher chance of success. The failure to encrypt data means there is no immediate operational disruption or societal impact, and the incident is therefore unlikely to receive as much attention from law enforcement authorities. There is also a trend whereby small and medium-sized enterprises are being affected to a greater extent than large companies. Small and medium-sized enterprises appear to be more likely to pay ransoms.

Hundreds of companies fall victim to cyberattacks every month. Compared to many other sectors, financial companies in the Western world often have a relatively high level of cybersecurity. Since the majority of criminal threat actors are opportunistic, i.e. they seek out the paths of least resistance, these businesses are not the first choice. The obvious vulnerabilities exist in other companies in other sectors. At the same time, the affected companies are part of the digital ecosystem that is also vital to financial institutions.

The total number of victims worldwide increased in 2025, a trend that has been observed on websites that publish information about cyber extortion attacks. Some of these victims are suppliers to banks, and some of them have been entrusted with handling the banks' data. This serves to create a leverage effect, as the customers of suppliers are also affected. Supplier vulnerability therefore poses a key risk to financial institutions, as these suppliers often handle sensitive information, such as customer data and transaction details, on behalf of banks. A cyberattack on a supplier could therefore indirectly threaten both the security of banks and the privacy of customers. However, there is no evidence to suggest that these suppliers were attacked because they have banks as customers.

A new category of cybercriminal threat actors has become increasingly visible in Europe in recent years, consisting of Western-based criminal networks that are not part of the traditional Russian-speaking cybercriminal ecosystem. This type of threat has previously been observed primarily in the United States, where several high-profile breaches with significant business impact have been targeted at large companies, including those in the gambling and casino sectors. Over the past year, similar threats have also been directed at companies in Europe. Several incidents in the United Kingdom clearly illustrate the phenomenon of Western-based criminal actors carrying out cyberattacks that have significant operational and financial impact.

In parallel with this, large-scale exploitation of vulnerabilities in cloud-based business platforms, such as Salesforce environments, has been observed. These vulnerabilities have enabled attacks on a large number of organisations in a short period of time. For Swedish banks, this development means that the range of threats is further expanding. The threat posed by cybercriminal actors based in the West should be considered a growing risk area.

Banks should continuously monitor and assess the threat of cyber extortion and review their security 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. A large-scale cyber extortion attack targeting the financial sector could have an enormous impact. Studies and analyses carried out by the International Monetary Fund (IMF), the European Systemic Risk Board (ESRB) and the Riksbank show that a cyber attack on the financial sector,

where the interconnection between and the concentration of affected stakeholders are sufficiently extensive, could threaten financial stability.

Threats in digital supply chains

Banks rely heavily on IT providers, cloud services and off-the-shelf software in their operations. The threats to these digital supply chains have increased over time, partly due to greater reliance on external suppliers and partly due to a rising number of cyberattacks being targeted at those suppliers. For financial companies, it is now a reality that suppliers and business partners are falling victim to data breaches and cyberattacks. The use of Software-as-a-Service, for example, is contributing to the banks' attack surface expanding beyond their own direct control.

Here are a few examples:

- In 2025, several US banks, including systemically important institutions, have suffered data loss or the exposure of customer data as a result of cyberattacks and security breaches at third-party suppliers. In several cases, these incidents have originated at specialised suppliers that handle large volumes of customer data for multiple banks simultaneously, highlighting the structural risk exposure resulting from dependence on third parties.
- In November 2025, the US financial and real estate technology provider SitusAMC suffered a data breach. The company handles large amounts of sensitive information on behalf of banks, including documentation related to loans and mortgages. According to reports, several major US banks were alerted that customer-related data may have been stolen from the supplier's systems.
- In 2025, Marquis Software Solutions, a provider of CRM, marketing and compliance systems for banks, was subjected to a data breach. The attack resulted in the exposure of customer data from at least 74 US banks and credit institutions, including details such as names, social security numbers, account information and other sensitive data. According to reporting of the incident, more than 400,000 bank customers were impacted, even though the banks' own IT environments were not affected.

Zero day vulnerabilities are vulnerabilities that are discovered by threat actors, who then immediately use them to attack systems before they can be remedied. Vulnerabilities of this type continue to constitute a significant threat to banks and show no signs of abating. These vulnerabilities pose a significant challenge to banks, as they enable attacks where there are no defence mechanisms. It is not only vulnerabilities that are exploited, but also errors in technical configuration and social manipulation of bank employees.

Events and incidents that do not involve a threat actor also have to be taken into account in banks' cybersecurity efforts. In 2025, major IT providers such as Cloudflare, Amazon Web Services, Google Cloud and Microsoft Azure experienced incidents that resulted in prolonged disruptions and service outages. These incidents affected many sectors and services globally, demonstrating the concentration risks that are built up when multiple customers use the same IT solution.

The threat landscape means that third-party risks can no longer be treated as a secondary risk or as primarily a contractual issue. Regulatory frameworks such as DORA require banks to systematically identify, classify and monitor risks associated with their ICT providers. These developments are driving a more continuous and risk-based approach to managing supplier relationships, with requirements for robust agreements, incident reporting and resilience testing, as well as effective exit and substitution plans. All in all, this means that attacks on suppliers must be given greater weight in banks' own operational risk and threat assessments, rather than being viewed as external incidents.

Destructive cyberattacks against societally critical infrastructure

During its war of aggression against Ukraine, Russia has repeatedly used destructive malware (known as wiper malware) in an attempt to destroy systems and data in critical infrastructure. To date, Ukraine has been successful in defending itself against these attacks. Attacks involving wiper malware risk spreading to actors and regions beyond the intended scope. This type of uncontrolled spread has not been observed among Swedish banks over the past year.

Banks need to constantly monitor and assess the threat of cyber extortion and to review their security measures.

At the same time, the attack directed against the Polish energy system in late December 2025 demonstrates that the threat to societally critical infrastructure in Europe is very real, and that destructive malware continues to be used as a tool in state-run cyber operations. The attack, which is believed to have been carried out with the intention of causing damage, targeted energy production and distribution-related systems and used wiper malware in an attempt to disrupt the distribution of electricity. Although the attack did not result in any actual disruption, it demonstrates that threat actors have both the desire and the ability to carry out operations of this type even outside Ukraine.

For the financial sector, attacks of this type pose an indirect but significant risk, as banks' operations are heavily dependent on a stable power supply and reliable communication networks. A successful attack using wiper malware against energy or communications infrastructure could lead to widespread disruption in payment systems and access to digital services. In the long run, this would undermine confidence in the financial system, even without the banks themselves being directly targeted.

Against this background, the threat posed by wiper malware should not be underestimated. The risk of direct attacks on banks or indirect spread via other sectors is still considered to be low, but the consequences of a successful attack would be far-reaching. This threat could become a reality in the event of a rapid deterioration of the security situation in Europe. As a result, banks have good reason to continue monitoring developments and to include scenarios involving destructive malware in their risk and contingency assessments. In the worst-case scenario, a large-scale wiper malware attack targeting the financial sector in Sweden could have a system-threatening impact.

Identities under attack

An infostealer is a type of malware designed to steal sensitive information from IT systems. Infostealers are no longer a threat in and of themselves, but rather one of the tools that threat actors use to gain access to identities and login credentials. Infostealers are often used by threat actors to carry out subsequent criminal activities such as fraud and extortion.

In today's IT environments, which often include cloud services, systems and technologies are constantly changing. Users' accounts and login credentials tend to remain over time, however. That is why identities are now a primary target for threat actors seeking to attack entities such as banks. In simple terms, it is often easier to log in using stolen credentials than to gain access by attacking the systems directly.

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 elevated 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. Phishing also occurs in relation to staff at IT providers, as a way of potentially attacking banks.

An important basis for addressing the threat landscape is the banking sector's established security hygiene, systematic working methods and well-developed collaboration.

Vishing targeting bank employees also occurs, with threat actors using phone calls or voice messages to trick bank employees into disclosing sensitive information, such as login credentials. The purpose of vishing attacks targeting bank employees can be difficult to analyse at first.

It is judged that attacks targeting users' accounts and logins have increased and are continuing to rise. This is no longer just a matter of stolen passwords: attackers are increasingly hijacking ongoing logins and sessions. This applies to both cloud-based systems and systems operated in-house. Protecting users' identities has therefore become one of the most important security issues for banks. Exercises and training for staff to be able to detect phishing e-mails and vishing calls, as well as technical solutions at banks to block phishing e-mails, remain important countermeasures.

Denial-of-service attacks – a diminishing but not yet eliminated threat

Denial-of-service attacks, which affect the availability of online financial services, have been one of the most common means of undermining confidence in financial services and financial firms. The actual impact of denial-of-service attacks has decreased during 2025, partly as a result of banks strengthening their capabilities, security and resilience. Banks have also noted a decline in the number of attacks since the summer of 2025.

Another contributing factor is considered to be the previously very active Gorilla botnet, which was used for large-scale denial-of-service attacks against banks, for example. This botnet appears to have been taken down or significantly restricted, after its central infrastructure and associated communication channels were identified and shut down.

Denial-of-service attacks remain a threat that banks must monitor, however, as threat actors still have the ability to adapt and carry out such attacks. The primary purpose of the attacks is to undermine confidence in societally critical financial activities.

Risk exposure to denial-of-service attacks is also growing in line with the increasing level of digitalisation. The attacks could also target suppliers, and so risk affecting financial institutions. Banks need to impose requirements on their suppliers regarding securing their systems against attacks.

Generative AI as a new dimension in the banking sector's threat landscape

In line with the rapid growth and wider availability of AI-based services, there is an increasing risk of data breaches for banks, particularly when employees use external AI services in ways that are not consistent with internal regulations. If sensitive information, customer data, internal analyses, business logic or operational details are fed into public or inadequately controlled AI services, there is a risk that data will escape the bank's control. In practice, this means that the data becomes accessible to third parties, through storage, model retraining or due to inadequate technical and organisational security measures at the service provider. Data transfers to external AI platforms pose a new and, in many cases, underestimated information security risk in the financial sector.

At the same time, the market for AI services has become highly fragmented. A wide range of generative AI tools, assistants and specialised applications have been established in a short period of time. This has often happened without the services undergoing the same maturity, security and compliance processes as traditional IT services.

In addition to the risk of information leaks, generative AI also introduces new risks related to how users interpret and use AI-generated output. AI services can generate responses that appear credible, but that are incomplete, misleading or outright incorrect, known as hallucinations. If AI output is used without sufficient human oversight and an understanding of the context, it can lead to incorrect assessments, analyses and recommendations. This can affect credit ratings, risk analyses, regulatory compliance and strategic decision-making.

The development of generative AI has lowered the threshold for developing and customising malware, which means that more threat actors than ever before are capable of carrying out technically sophisticated cyberattacks against banks. AI is used to rapidly develop and tailor malware to specific targets. As a result, the time from attack to damage being sustained is becoming shorter. Of particular concern is the emergence of AI supported dynamic malware, which can change its behaviour during the course of an ongoing attack, making detection and incident management more difficult.

Overall, this means that cyber threats against banks are becoming more agile, harder to detect and more scalable, with potentially greater consequences, even in the event of individual security breaches. For banks, this is increasing the need to detect breaches at an early stage, as well as placing greater emphasis on resilience rather than purely preventive measures.

Generative AI is also lowering the threshold for the production and spread of disinformation on a large scale, as it is enabling the rapid creation of convincingly worded texts and images. The narratives can be tailored to specific target groups and events. Disinformation campaigns can be used to influence public opinion, create uncertainty or fuel concerns about alleged incidents in the financial sector. This, in turn, can contribute to confidence in banks and financial services being damaged and undermined, with potential repercussions for financial stability.

However, banks are well-positioned to manage these new risks as well, by continuing to build on their established systematic security measures. This work needs to encompass not only the development and implementation of AI solutions, but also the ability to prevent, detect and respond to cyberattacks in which AI is used as a tool by threat actors. Integrating information security, compliance and risk management at an early stage creates the conditions for using AI in a controlled manner that adds value, at the same time as strengthening operational resilience.

Development of quantum computers – a long-term cryptographic shift

The development of quantum computers poses a long-term threat to the encryption currently used to protect communications, identities and data in banking systems. The reason for this is that sufficiently powerful quantum computers can solve certain mathematical problems much more quickly than classical computers, undermining security.

Although viable quantum computers are not expected to be available in the near future, there is a risk that information that is encrypted today could be stored and decrypted by threat actors in the future, making this issue relevant from a long-term confidentiality and continuity perspective. For banks, the transition to quantum-secure cryptographic solutions could entail significant transition costs, as cryptography is deeply integrated in systems, applications and customer communications, as well as dependencies on suppliers and shared infrastructure.

This work therefore requires careful planning, an assessment of how and where banks use cryptographic systems, as well as coordination with suppliers. At the same time, the banks' established frameworks within security and change management provide a solid foundation for managing this technological shift in a gradual and controlled manner.

Need for action by politicians and authorities

- The Riksbank should be tasked with defining clear roles and responsibilities for the crisis management function. The Riksbank should also define how the function, together with the National Cyber Security Center (NCSC), CERT-SE and the National Defence Radio Establishment (FRA), should perform crisis-management and provide support in the event of cyber attacks against societally important financial operations.
- 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 is elevated, and that it is influenced by criminal groups and state-sponsored threat actors. Cyber extortion is evolving from data encryption toward data theft, which is both easier and faster to carry out. The risks in digital supply chains are changing as a result of the increased use of suppliers and a rise in the number of cyberattacks targeting these suppliers. In the cyber field, the threat landscape can also be influenced by threat actors who are persistent and driven, and who see opportunities linked to the development of security policy. However, a decrease in the number of denial-of-service attacks has been observed during this period. An important basis for addressing the threat landscape is the banking sector's established security hygiene, systematic working methods and well-developed collaboration, both within the sector and with relevant authorities. This structure and maturity constitute a solid foundation for effective, long-term security efforts, even in a changing threat environment.

5 Fraud and financial crime

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

In 2025, a total of 229,161 fraud offences were reported in Sweden, according to the police. This is an increase of 1,727 offences, or 1%, compared to 2024.

Increase in fraud attempts, but lower criminal proceeds

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, SEK 6.3 billion in 2024 and SEK 5.7 billion in 2025.

The increase in criminal proceeds from fraud, up until the break in the trend in 2024, can largely be explained by the marked increase in fraud involving social manipulation. For example, the number of vishing offences reported to the police, i.e. telephone fraud, stood at 5,285 in 2019, whereas by 2025 this figure had risen to 32,844.

Although the number of reported vishing fraud offences has remained largely unchanged over the past two years, the proceeds from these crimes have decreased by approximately 60 per cent in 2025 compared to 2023. The average loss (proceeds of crime) from a vishing scam in 2025 was the lowest since 2017 (when tracking of this method began).

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. However, fraudulent offences have evolved to become highly flexible and adaptable. One consequence of this is that the methods used are developing and expanding as the group of crime victims widens, for example to include younger people.

New products and third-party suppliers

One of the challenges in the 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 this change, in turn, requires real-time protection in respect of information sharing. There is also 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 to both fraud and money laundering the new products entail, and to develop counter measures.

New services and products are not always developed by the bank itself, rather this can take place through 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, which creates risks.

More actors gain access to the banks' information

Since 2023, there has been a legislative proposal from the EU regarding transitioning from open banking to open finance through the Financial Data Access (FiDA) regulation, which will be directly applicable in Sweden. 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 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 relate to cybersecurity, fraud and financial crime, for example. 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 to apply the same standards to all stakeholders in the ecosystem.

New rules for payment services

Another legislative proposal that will enter into force in 2026 is the European Commission's proposal to amend the regulatory framework for payment services. This will result in a Payment Service Regulation (PSR), which will be directly applicable in Sweden. The legislative proposal 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.

The new Payment Services Regulation includes a comprehensive package of measures to combat fraud. 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. The Payment Services Regulation clearly reflects the political commitment to combat fraud, which is very encouraging. At the same time, it is crucial for the new rules to both strengthen consumer protection and provide 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 several 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.

Increased reporting obligations for clearing houses

In early 2025, the Government presented a bill regarding measures to combat the misuse of the payment system, with reporting requirements for clearing houses being a central component. Acting in collaboration with banks and clearing houses, Finance Sweden has therefore developed a concept that enables the monitoring of transactions at clearing level. Clearing houses have an overview of the payment system that no single bank can have. This is an important step towards strengthening the ability to combat fraud and money laundering more effectively, as well as reducing vulnerabilities in the payment system.

The threat landscape is changing

Banks have historically had the capacity to fend off fraud offences, but the digitalisation of society has 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.

Because of the changes, criminality has been driven towards methods involving more 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. The threat landscape has consequently changed and it is necessary for the preventive measures to be adapted.

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 by several operators in society, 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-sms" scheme (the fraudster impersonates the parent's child in a text message). 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, such as the Covid-19 vaccine, electricity subsidy payments, tax refunds, etc. Another trend is the increase in the number of customers who fall victim to fraud on multiple occasions. 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 fraud offences 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 provide accurate information to customers about what the bank and other actors do and do not do. 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 to use their e-identification or security device.

Business operators are exposed

As it becomes increasingly difficult for fraudsters to withdraw large sums of money from the bank accounts of consumers, 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. 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 creates inertia and security

Duality, i.e. the need for two people to approve a transaction, gives rise to inherent inertia, but also security. Duality is available as an option for customers but is not mandatory. Even though all corporate customers are offered duality, not all of them take advantage of this option. Even if companies are offered duality when it comes to signing or have a duality limit of a certain amount, not all companies, associations and foundations ensure that their internal procedures are being complied with. It is also important that the second person who is to approve a transaction verifies the details and does not simply sign off on it out of habit.

Security awareness among customers needs to be strengthened. 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. If the option of duality is not utilised, lowering the limits may be considered. It is extremely important for corporate customers to be informed about the duality options in banks' systems, to prevent fraud-related losses.

Fraudulent offences have evolved to become highly flexible and adaptable.

Remote access tools give the fraudster control

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.

If banks were able to detect when remote access tools are being used on a computer, a service or a session, they could, for example, refuse payments or choose to shut down the service or session. The challenge posed by remote access tools is that it is legitimate software. To counter remote access tools, banks are attempting to identify and analyse behavioural patterns regarding how customers use computers and apps.

Banking trojans

Banking trojans are continuing to affect customers of banks and financial institutions across Europe. Banking trojans that infect mobile phones and mobile banking solutions are often designed to steal customers' login credentials. Bank customers have had their mobile phones infected by downloading apps that contained malware. Banking trojans developed for Android phones are still considerably more common than for iOS phones. In 2025, there was a significant increase in Android trojans, although this threat is not common in Sweden.

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 can also use such technology in their crime prevention efforts. Automated conversations are used in some fraud schemes via social media and chat apps. Banks are anticipating better quality when it comes to language and design, as well as increased scalability when it comes to future telephone fraud (phishing, smishing and vishing schemes). Banks still don't see many AI videos, but there are signs that AI is being used in various ways. For example, these tools can find out more about the first names of the victims' siblings and parents in a more automated way.

There is a risk that scams targeting business owners, such as BEC scams (for example CEO fraud, in which someone within a company is tricked into carrying out transactions for fraudsters), will be amplified by AI elements, including voice cloning and pre-recorded messages. It may become increasingly difficult for banks to assess whether a customer who is a victim of fraud has been communicating with a real person or not. 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 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 vulnerabilities. Regulations such as Financial Data Access (FiDA) aim to create a more interconnected financial ecosystem, in which banks and other actors have access to more information than before. To realise these benefits, however, data sharing needs to extend beyond the financial sector. Sharing certain types of information, for example with telecommunications providers and other public sector entities, can have a clear preventive effect, particularly in the fight against fraud.

Wider data sharing can also improve credit assessments, enable more accurate risk models and strengthen competition by giving more market participants access to relevant information. At the same time, a more open flow of data means that the attack surface for cybercriminals is expanding. As more parties process sensitive information, there is also an increased risk that a single vulnerable actor could become a point of entry for attacks that have consequences throughout the entire financial ecosystem. Even small-scale manipulation of data that is difficult to detect can affect credit ratings and risk analyses and thereby lead to incorrect decisions with major financial consequences.

In addition, conflicting objectives arise between different regulatory frameworks and societal interests. GDPR requires data minimisation, short retention periods and limited aggregation capabilities, which is often directly contrary to the need for long-term analysis, traceability or the potential to investigate serious crimes. At the same time, there is a growing expectation that banks should do

more to prevent fraud, money laundering and other financial crimes – which requires relevant data to be stored, linked together and shared when necessary.

These challenges are compounded by the fact that various government agencies – such as the Swedish Authority for Privacy Protection, the Swedish Financial Supervisory Authority, the Swedish Tax Agency and the Swedish Police Authority – sometimes interpret what is permitted and appropriate in different ways. In collaboration with law enforcement authorities, banks are expected to be able to produce comprehensive and structured information quickly, although privacy and regulatory considerations limit the potential to have such information aggregated and indexed in advance.

Overall, clearer and more appropriate preconditions are needed for banks to be able to exchange information about fraud, fraudsters and risk patterns. Without a modernised data-sharing framework, there is a risk of a widening gap between what society expects from banks and what banks can deliver.

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. For example, it might look as though the bank 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 telephone fraud, 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. Banks consider that AI tools are already capable of identifying potential high-volume fraud.

Electronic identity theft in a physical environment

As digital security has strengthened, fraud involving physical elements has increased. In 2025, there was an increase in the number of BankID thefts occurring in person at the same location as the victim. Fraudsters are creative and use a variety of methods to deceive their victims. The approach involves scammers, who rarely work alone, managing to get hold of the victim's phone. They borrow phones from taxi drivers, approach young people in bars and restaurants, and respond to sales advertisements on various marketplaces; they also go door-to-door.

By the time the scammer has the phone in their hands, they have somehow also managed to find out the victim's BankID security code. The security code is required to activate BankID on the scammer's phone. The method used by scammers is known as the "app-to-app flow", in which a device with an active BankID is used to create a new BankID on another device. For the issuing to work, both devices must be paired via Bluetooth and placed next to each other. Location services must also be enabled on both devices.

In other words, there are several steps and requirements that must be completed to successfully create a BankID this way. In some cases, this is likely to be a matter of "friendly fraud," but not always. Affected customers will not always have realised that a scam has taken place and are therefore unable to describe what happened. The fraudsters may then wait a long time before using BankID to circumvent monitoring, which makes the fraud process more protracted. It is important for banks to ensure that the story provided by the victim matches the parameters that the issuing bank can see in connection with the BankID transaction and the issuing.

Proceeds from telephone fraud in 2025 were at their lowest since 2017.

In late 2024 and throughout 2025, the number of home visits has been increasing significantly.

The number of home visits is increasing significantly

In late 2024 and throughout 2025, the number of home visits has been increasing significantly. Home visits by fraudsters claiming to represent various companies and government agencies are a growing problem. This can also take the form of physical outreach, such as a fake transport services.

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. There is a real risk that the number of home visits will increase, and thereby that personal risks will increase, when banks block the potential for other approaches. This needs to be taken into account as part of work to combat fraud. The transparency of Swedish society, where personal data is open, makes targeting easier for fraudsters.

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.

An example: 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.

One common scheme is where an individual takes 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 cannot 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 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, for example making interest payments, 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's Know Your Customer data. If the origin of the funds is questionable, the bank is in a difficult situation regarding how the customer relationship should be managed. There is also a danger of cases becoming complex very quickly.

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 the fraudster manipulating the system so that their creditworthiness appears to be better than it actually is.

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, rapid business credit and 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.

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 consumer credit include people who take out several loans in a short space of time with no intention of paying. Analyses of this method have resulted in changes to onboarding processes to detect warning signs at an early stage. Estate agents are increasingly acting as enablers for fraud, 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, it 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, several 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.

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. These contacts often continue for an extended period, and it is common for consumers to be deceived multiple times. So-called deepfake articles and fake ads featuring celebrities on social media are often the starting point.

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 peripheral acquaintances. Fake advertisements are largely found on digital platforms, using the names and images of famous people to create confidence.

Fraudsters take advantage of customers' lack of knowledge about complex investments, such as cryptocurrencies. 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, and sometimes also 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 often used in investment fraud. By signing orders, sometimes without understanding what they are authorising, victims risk losing a lot of money.

Customers transfer money to make an investment that is promised to give a significantly better return than both the banks' savings 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 fraudsters 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 has been subjected to investment fraud or whether they have just made a bad investment.

Pump and dump

A pump-and-dump scheme is a form of investment fraud that relies on the existence of a stock that has a real value, but where there is extensive market manipulation. In the autumn of 2025, it became apparent that this approach had become more organised and AI-focused, and that it was taking place outside Sweden in small US companies listed on Nasdaq.

The method involves fraudsters buying a large stake in a stock that is often obscure and has low liquidity (a stock whose price is easy to manipulate). The fraudsters then spread misleading and false information to generate interest in the stock and drive up its price. The information is spread via social media, e-mail campaigns, chat groups, investment forums and fake ads. Customers perceive that there is an active investment community surrounding the stock. In practice, it is often a case of one or two fraudsters working in conjunction with several AI-based chatbots that are reinforcing the impression of legitimacy.

Once the stock price has risen high enough, the fraudsters sell their holdings, causing the price to plummet. The small investors who bought in at the peak – or during the upward journey – are then left holding stocks that have rapidly lost their value and are often difficult to sell.

Romance scams

Romance scams are based on long-term social manipulation, in which the fraudster initiates a long-distance relationship with the victim with the aim of defrauding them of money. Contact often begins on dating platforms and social media, before moving to chat services. The fraudster seeks to contact people in situations in which they are vulnerable, and love is a strong driving force.

It often takes banks a long time to identify victims, for several reasons. First, the contact begins in channels that are beyond the bank's control. Banks can shut down phishing sites, but they can't shut down Meta. Second, the amounts and types of transactions vary, which makes it difficult to identify discrepancies. Third, customers don't always realise that they're being scammed. They feel that they are in an ongoing relationship that feels good. Fourth, customers rarely want to talk about the "relationship" – this is inherent in this type of crime. They may have been told to keep the "relationship" to themselves and to lie to the bank. Fifth, the longer the fraud has been going on, the harder it is for the bank to reach the customer, who has invested a great deal of emotion and money in the "romantic relationship" and may feel ashamed of having been deceived.

The banks' efforts to combat romance scams are divided into preventive measures, dealing with ongoing scams, as well as measures taken after detection.

- **Before a romance scam**, the focus is on reducing the risk of customers becoming victims. Information needs to be up-to-date and relevant in order to raise awareness about how romance scams are conducted and what the warning signs are. In parallel with this, banks are developing systems and processes to identify unusual behaviour, such as unusual payment patterns.
- **During an ongoing romance scam**, the banks' goal is to detect and break the sequence of events as early as possible. When suspicions arise, the customer is contacted to inform them about the risks and to help them understand that they may have been manipulated. Customers of this type generally exhibit an inherent tendency to avoid contact, which makes it difficult for the bank to reach them. The discussions are difficult, because the customer resists the bank's attempts to contact them and often trusts the scammer more.
- **After a romance scam**, banks try to limit the consequences and reduce the risk of re-exposure. The recurrence of this type of fraud is, however, very high.

The rise in social manipulation as the starting point for a variety of fraud schemes raises the question of whether there should be some form of communication rights between banks to share information about vulnerable customers, even though this would constitute a significant invasion of privacy.

Straw men enable fraud

Straw men and straw men accounts are a prerequisite for fraudsters' activities. There are many money laundering straw men operating in Sweden. 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.

According to the police, a total of 95,000 people has been registered as being suspected of committing fraud offences during the period 2022–2025. 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.

Finance Sweden's first programme of action – increased customer protection against fraud

Vishing fraud increased significantly in 2023, and the Board of Finance Sweden therefore decided in December of that year to issue a recommendation to banks regarding measures to increase customer protection against fraud.

The recommendation, which had been developed in collaboration with the police, focused on vishing fraud and was presented to the Government in May 2024. The recommendation was also expected to have an impact on other types of fraud.

The measures, which were to be implemented no later than in 2025, include:

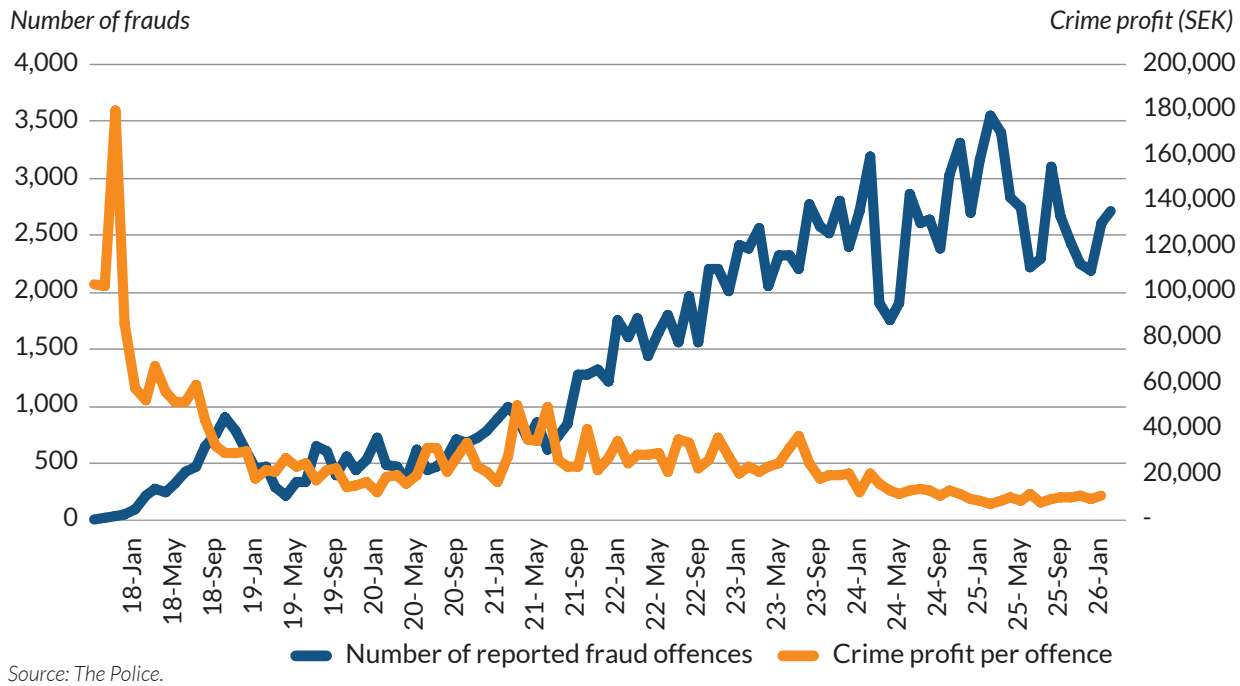
- Limits (ceiling amounts).
- Time delay on products and payments.
- Potential for duality (two people must approve the transaction).
- Review of products provided.
- Increased checks in connection with new products.
- Block misuse of banks' phone numbers and SMS (spoofing).
- Improved transaction monitoring.
- Evaluate ID methods.

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.

- Bank common initiatives for issuing BankID.
- Bank common initiatives for blocking BankID and Swish.
- Information and training.

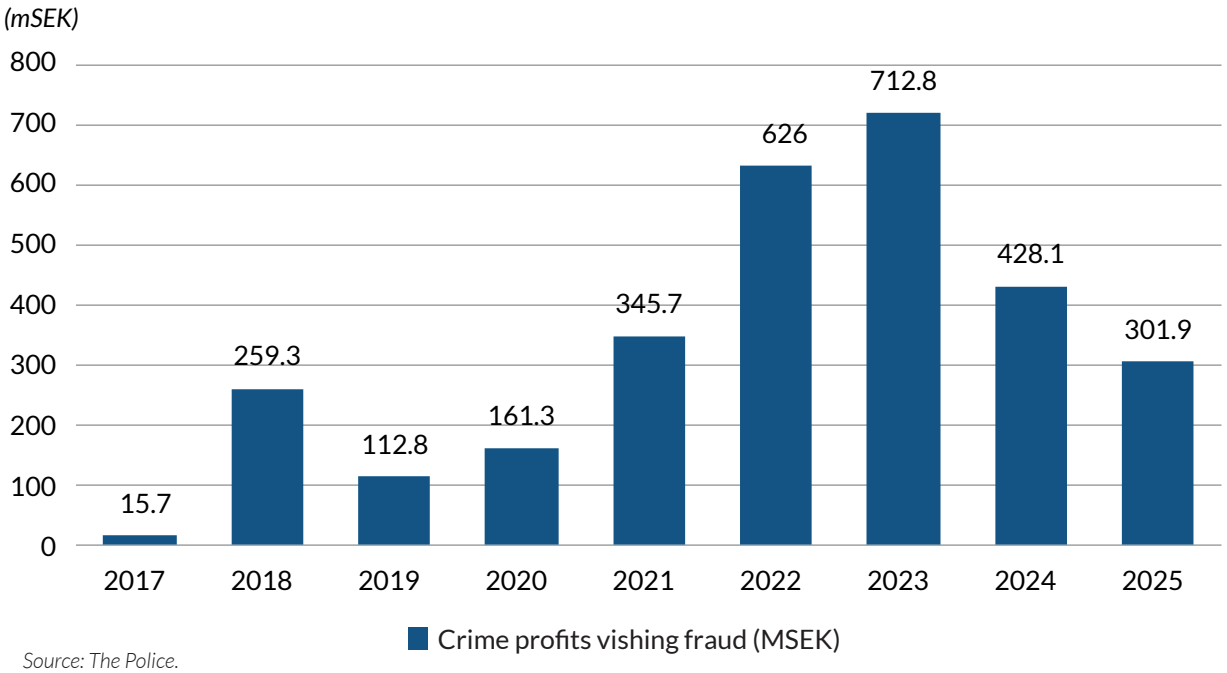
The measures were implemented in 2024 and 2025, considering individual banks' customers, product offerings and infrastructure. The banks have chosen different ways to comply with the recommendation. For example, a strict restriction for a certain product can reduce the need for other measures. A less strict product restriction can be combined with past customer behaviour (amount, frequency, only historical payees, etc.) which can provide good protection. AI-based transaction monitoring tools can also provide additional protection.

Number of reported vishing offences and proceeds of crime in SEK per vishing offence (2017–2025).



Source: The Police.

Proceeds from vishing fraud in millions of Swedish kronor (2017–2025).



Source: The Police.

The impact of these measures on fraud trends has been continually monitored together with the police. The aim is to understand how crime and the proceeds of crime are affected and change, particularly when it comes to shifts in criminal methods.

Police statistics show that proceeds from vishing fraud decreased by approximately 60 per cent in 2025 compared to 2023. The average loss (proceeds of crime) from a vishing offence in 2025 was the lowest since 2017 (when tracking of this type of scam began).

The strengthened issuing process for Mobile BankID has resulted in the virtual elimination of unauthorised transactions when issuing Mobile BankID. Ceiling amounts have been effective in reducing proceeds of crime.

According to the police, the main reason for the reduction in the proceeds of crime is the banks' programme of action to combat fraud, which was launched in May 2024. In addition to the reduction in losses achieved through the banks' measures, the police have carried out activities that have impacted prosecutions both in Sweden and abroad, and telecommunications operators have also implemented measures. The amounts involved remain significant, however, and efforts to further limit losses need to continue, particularly regarding preventing large losses.

Finance Sweden's second programme of action – increased customer protection against investment and romance scams

While proceeds from vishing fraud declined, investment and romance scams increased in 2024. In May 2025, the Board of Finance Sweden decided to issue a further recommendation to banks regarding measures focused on investment and romance scams.

The measures, which must be implemented no later than in 2026, include:

- Spreading awareness to highlight the risks of falling victim to fraud, such as investment or romance scams.
- Preventing and limiting the use of screen-sharing tools in various types of fraud.
- Informing and assisting customers who may be suspected of being or have been the victims of fraud. Customers are often manipulated and need to be informed about what is happening, to prevent them from carrying out transactions that are part of an investment or romance scam.

These measures complement the 2024 programme, with improved processes for informing and assisting customers who may be suspected of being or have been victims of investment or romance scams. The impact of these measures on fraud trends will be monitored together with the police.

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 and text messages. Telecommunications operators should also scan for known fraud patterns and block obviously fraudulent text messages, as well as collaborate with banks and other relevant stakeholders to combat fraudulent text messages and block traffic to websites containing malware.
- The Swedish Tax Agency and the Swedish Transport Agency should provide banks with better tools for verifying their identity documents, both in person and remotely, similar to the tools provided by the Police Authority.
- The Police Authority should establish a system for exchanging information with banks regarding Sverige-id (the Government's digital ID, scheduled for December 2026). The exchange should focus on usage. The purpose of this is to prevent unauthorised use of Sverige-id, for example in cases of remote control and exploited identities, and to monitor fraud patterns.
- 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 the most common forms of fraud to the police online. It can take a long time to get through via 114 14, with the risk of many crimes going unrecorded.
- The most important step in combating investment fraud is for social media platforms to take greater responsibility for the content published on their platforms. Platforms such as Facebook, WhatsApp and Instagram are major enablers of fake advertisements, which are published on their sites which trick customers. The platforms should therefore reduce the number of fraudulent ads by means of the following measures:
  - Requirements for the verification of advertisers and profiles.
  - Systems for monitoring suspicious behaviour (similar to those implemented by banks).
  - Verification of customer identity and assessment of risk profile.
  - Procedures and processes for reporting fake ads.
  - Centralised blocking of potentially fake profiles/advertisers.
  - Financial liability when fraud offences occur through the platforms' channels.
  - Closer cooperation between social media platforms, payment service providers and law enforcement authorities.

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.

Banks are working preventively to eliminate money laundering.

6 Money laundering

Regulation in the area of money laundering has both a criminal and an administrative aspect. For banks, the administrative regulations are the most important to their operations.

The **criminal regulation** of money laundering effectively criminalises a range of money laundering activities aimed at concealing the fact that funds are derived from crime. 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. The crime that precedes money laundering and leads to financial gain is usually referred to as a predicate offence. A person who is guilty of money laundering in the meaning of the law is convicted of a money laundering offence or commercial money laundering.

The **administrative money laundering regulations** are based on international principles established by an intergovernmental UN body called the Financial Action Task Force (FATF). These principles have subsequently been incorporated into EU law. Since 2024, the majority of Swedish regulations have been based on the EU regulation on measures to prevent the financial system from being used for money laundering or terrorist financing, namely the Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, (AMLR). The Regulation is directly applicable as Swedish law, and will be applied as of 10 July 2027. The AMLR is supplemented by EU-wide interpretative rules, known as regulatory technical standards (RTS). A fundamental principle of the administrative money laundering regulations is what is known as the risk-based approach.

Businesses and entities that are covered by anti-money laundering regulations must comply with a number of requirements, including conducting risk assessments of their own operations, performing customer due diligence, monitoring activities and reporting to the Financial Intelligence Unit.

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 in order to detect anomalous activities and transactions.

In addition to implementing measures to comply with money laundering regulations, such as monitoring, the banks work strategically on crime prevention measures and collaborate with one another in order to completely eliminate money laundering from the banking system.

Reporting money laundering

Under money laundering regulations, businesses in a wide range of sectors are required to report suspected money laundering to Sweden's Financial Intelligence Unit (FIU).

According to FIU's statistics, a total of 66,341 suspicious transaction reports (STRs) and 9,757 suspicious activity reports (SARs) were filed in 2025, representing an increase of 26% and 15% respectively compared with 2024. The financial sector accounted for more than 90% of the reports.

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, evade detection or secure assets intended for forfeiture. 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 and the supervision of prescribed measures to combat money laundering are not yet satisfactorily exercised, such as with regard to 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. In recent years, the Government and authorities have stepped up their efforts to expand international judicial cooperation in criminal matters, which may include tracing and securing misappropriated assets.

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 combined use of straw men, front men and companies, 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.

Money laundering schemes that are difficult to detect

As a bank can only see the portion of a transaction chain that has been conducted within the bank itself, sophisticated money laundering chains involving transactions in several banks are often difficult to detect. At present, banks have only limited opportunities to exchange information with other banks, but the AMLR is bringing improved opportunities that should be utilised to the fullest extent possible.

To counteract the rise in fraud offences, which often constitute predicate offences of money laundering, Swedish banks have implemented both technical improvements and restrictions of services in relation to their customers. As a result, the total proceeds from telephone scams have decreased, although at the same time money laundering methods have changed.

The number of potential ways to carry out transactions has increased in recent years, a trend that is expected to continue in 2026. New payment service providers are emerging that lack the banks' established procedures and experience of preventing money laundering. 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.

Cooperation in the area of money laundering

One aspect that has grown in importance in recent years is information sharing between law enforcement authorities and business operators. In this context, "information sharing" refers to deviations from e.g. bank secrecy or disclosure prohibitions that are permitted under the regulations. In other words, this is not a case of the free exchange of information, rather it may occur only in exceptional cases and under specific circumstances.

The Anti-Money Laundering Regulation (AMLR) includes a number of significant changes. One of the most prominent changes concerns the potential for information sharing between private entities, which will be able to take place within the framework of a so-called private-to-private (P2P) partnership. This is a new development in Swedish law. At present, a government agency needs to be involved.

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), in consultation with the private sector (banks etc.). Finuc entails 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 work together to disrupt the illicit economy through effective information sharing and crime prevention actions.

Finuc has been operational since 1 April 2025, but the centre's activities will gradually be built up until the start of 2027. 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 ongoing, sophisticated money laundering schemes. The banks welcome the establishment of Finuc.

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 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 is 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. This calls for wide-ranging, proactive measures on the part of society.

The checks must 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 the welfare system. Through data analysis and audits, the Authority identifies and prevents incorrect payments, including those suspected of being linked to criminal activity. This in turn will reduce the banks' risk of transferring the proceeds of crime and thereby money laundering. Once the Payment Authority has fully established its procedures and obtained the legal tools to investigate all relevant areas of payment, it is expected that it will be able to curb incorrect payments to a greater extent.

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-scale proceeds of 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, including of foreign purchasers, for example.

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. It is worth noting that, in 2026, the Government has proposed establishing a registry at Lantmäteriet (the Swedish mapping, cadastral and land registration authority) where all tenant-owned apartments must be registered, a move that the banks welcome.

Collaboration among banks is becoming more important.

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. Cryptocurrencies are used as a means of payment, although perhaps above all as an investment vehicle, with the intention of converting them into traditional currency. Several of the world's largest crypto 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 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 are used as a means of payment in both the retail sector and between individuals, which is also increasing the risk of money laundering. However, as the risks associated with cryptocurrencies have come under greater scrutiny, awareness within the business community has grown, leading to many players now steering clear of such currencies.

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 risk that has increased is that countries and other actors are using cryptocurrencies to circumvent the extensive sanctions imposed on Russia by the EU and others. Cryptocurrencies have proven to be useful in replacing globally viable currencies, such as the US dollar. Trading in cryptocurrencies can also be an alternative for those actors who are excluded from international payment systems by sanctions.

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

At the same time, 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 (known as blockchain analysis) represents both an opportunity and a growing challenge for stakeholders on the market and law enforcement authorities.

In December 2024, the EU's Markets in Crypto-Assets Regulation (the MiCA regulation) entered into force. MiCA aims, for example, to facilitate legal certainty for businesses and 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. It remains to be seen what impact MiCA will have in practice and how effectively supervision will be carried out.

Payment services and currency exchange, whether conducted on a professional basis or on a larger scale, are also vulnerable to money laundering. Since such operations use the banks' payment infrastructure, the banks' risk exposure is affected. In recent years, regulations have been introduced to increase the demands placed on currency exchangers and payment intermediaries, which should help to reduce the risk of money laundering.

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 using cash obtained from crime or using other means that have a background. Many of the luxury goods are easy to move from country to country, and to resell while retaining or increasing their value. This enables luxury goods to be used to transfer value without 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 that amount of 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 by means of money being 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.

Since traditional casinos were phased out in Sweden in 2025, gambling companies now operate exclusively online. 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 on the Swedish and European market. 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 January 2026, the Government tasked the Swedish Financial Supervisory Authority with developing guidance for banks on how to address the conflicting objectives between anti-money laundering regulations and the right to a bank account, which is expected to provide clarity.
- 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.

High

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 through the regular financial system will remain high. Banks are constantly seeking to mitigate their risks, mainly through good customer due diligence practices and appropriate transaction monitoring. The control relating to the tax and welfare system needs to be further increased in order to restrict the conditions for the crime that precedes money laundering.

7 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. This can be attributed in part to increased efforts by government agencies and banks in relation to private individuals, as well as to an increasingly comprehensive regulatory framework regarding the prevention of money laundering.

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. Crime prevention efforts in relation to companies are driving a shift in criminal activity towards other types of organisations, such as non-profit associations.

There are many reasons why businesses are particularly attractive as instruments of crime. Criminals can hide behind a company's façade of legitimacy. It is also possible that criminals, through a company, may open the door to other types of lucrative crime, for example by exploiting the security and stability that a company can represent 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, depending on 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 economic crime 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 may be suspected within the criminal scheme.

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 invoice fraud, as well as various types of welfare crime. Furthermore, criminal schemes aimed at money laundering via companies or corporate structures 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 aban-

doned. 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 business partners 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 in parallel, 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 increasingly effective and as regulations are tightened, criminals need to evolve their criminal activities. This results in increasingly sophisticated criminal schemes. For example, there are sophisticated corporate structures involving representatives, bank accounts, accounting or clients in different locations – often in different countries – as well as skilfully forged documents that are used to support transactions. Legitimate and criminal activities may also be combined within the same companies or corporate structures. Such well-planned criminal schemes are harder for law enforcement authorities and banks to detect, which means they can continue for a longer period of time.

Furthermore, attempts are made to legitimise these criminal schemes through contacts with, for example, the Swedish Tax Agency or accounting firms, with the aim of making them appear more legitimate to external parties such as banks and business partners. The individuals who commit these crimes in Sweden do not always understand how the overall scheme works or how criminal proceeds are actually generated, which means they often have difficulty answering detailed questions from banks. Advanced criminal schemes can be sold or managed by international criminal networks.

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 enablers or in any event as supporters 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.

Shortcomings on the part of one actor create risks for other actors.

Fake invoices, account statements, 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 often 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, the 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. As soon as such access exists, this leads to increased risks for other parties – such as banks – which then have to try to identify the risks based on the company's behaviour and subsequently take action.

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. Finance Sweden welcomes the work that has been initiated within the framework of the Government's assignment for the Swedish Companies Registration Office, as well as the ongoing investigations aimed at providing the Office with the necessary tools and legal framework.
- 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 other regulation with a similar impact should be introduced, in order to prevent criminals from gaining quick and easy access to existing or new businesses.

The assessment is that banks face a challenge in detecting risks of criminal activity involving corporate accounts, despite their advanced technical solutions and information sharing among themselves and with authorities. Appropriate and in-depth checks when banks enter into business relations with companies, especially in high-risk sectors, can help prevent crime. However, it is essential for effective pre-emptive controls of businesses to be introduced within societal structures.

Terrorist financing is often linked to welfare crime.

8 Terrorist financing

Terrorist financing refers to the handling of money or other property with the intention of using it for various types of terrorist-related activities. For banks, this often involves private or corporate customers using the bank's services in an unauthorised manner by transferring money for these illegal purposes. This generally takes place under false pretences and can therefore be difficult to detect.

At an administrative level, terrorist financing is regulated under the same legal framework as money laundering, although these are generally distinct phenomena in terms of methods and motives.

An increasing overlap between organised crime and terrorist financing is being observed in external monitoring. Extensive and complex international tax crime (such as VAT fraud, 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 banks have difficulty detecting the risks, partly because the turnover appears legitimate and because the paying body in this case is the Swedish Tax Agency. The same applies to various forms of organised welfare fraud.

In recent years, the number of cases of suspected terrorist financing via cryptocurrencies has increased. Examples of other forms of terrorist financing can include credit fraud, misuse of humanitarian aid and cash smuggling.

Crowdfunding is also used to finance terrorism. In this case, a large group of individuals with a shared interest 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.

A key risk factor in relation to terrorist financing is that banks, in certain cases, 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.

The assessment is that through increased collaboration and information sharing regarding the methods used and the actors involved, the risk of banks participating in terrorist financing can be reduced. In addition, more comprehensive oversight of the crypto sector is needed.

9 International sanctions

International sanctions – or restrictive measures – are part of the EU's Common Foreign and Security Policy. With a more complex conflict landscape 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. The effects of sanctions are usually not immediate – they require a long-term approach and perseverance.

A number of different countries impose sanctions. Key international actors include the UN, the EU, the United States and the UK. Sweden does not 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.

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.

The field of sanctions has become more unpredictable and complex.

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 a particular type of product or service that is legitimate in itself, but that the sanctioned party may be using for undesirable purposes. In this context, reference is often made to dual-use products, i.e. products that can be used for both civilian and military purposes. These might include chemicals, electronics or software, for example. Trading in such products entails particular challenges in terms of detection and prevention.

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.

In recent years, the use of sanctions has been more erratic and unpredictable, particularly in relation to the United States' foreign policy stance, which shifts rapidly. One example is the United States' imposition of retaliatory motivated sanctions against representatives of the International Criminal Court (ICC) in The Hague, which is further contributing to the intractable complexity of the situation.

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

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 mainly intended to restrict Russia's military capabilities 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 2026), the EU has adopted a total of 20 sanction packages against Russia. In 2026, additional and broader sanctions against Russia are anticipated.

However, Russia is finding new ways to systematically circumvent the 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 in many respects aimed at trying to address this evasion and circumvention, and this is likely to remain a priority within the EU in 2026.

Collaboration in the field of sanctions

Large-scale, complex and systematic circumventions of sanctions 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.

At a national level, the Government tasked the police in 2024 with strengthening compliance with international sanctions through the establishment of a cooperation council. This council is now operational and comprises a number of authorities.

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.

10 Bank robberies, cash in transit robberies and ATM attacks

There have been no bank robberies in Sweden since 2020. Since measurements began 45 years ago, 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 depositary 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 2025 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 2025 either. These statistics include ATMs being blown up or cut open, but not card skimming (theft of card information).

Low

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 2026, as will the number of attacks on ATMs.

The last bank robbery in Sweden took place in 2020.

Photo: www.bankomat.se press images

11 The challenges posed by cash

Sweden is one of the countries with the lowest demand for cash 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 reporting the same trend as in recent years, i.e. a decline of about 10 per cent annually.

Discussions about whether the use of cash should increase in society are becoming more widespread. There is an ambition to ensure the survival of cash for various purposes. This can be seen in regulations (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).

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.

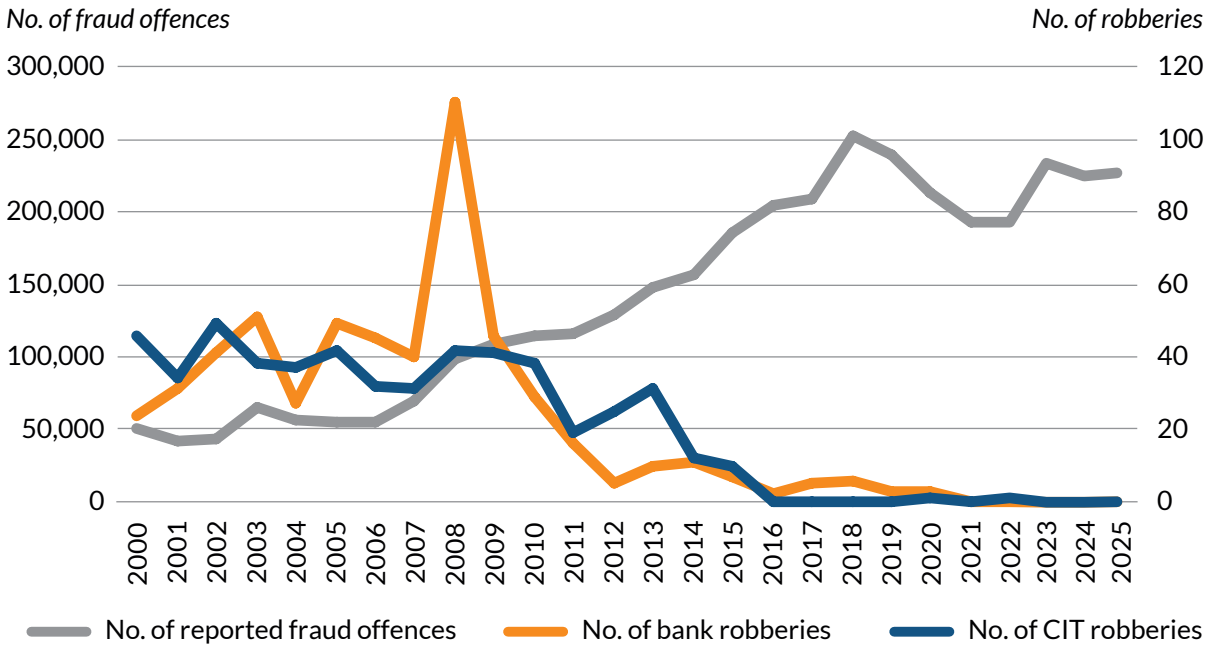
The focus of continuity and contingency solutions therefore needs to be on increasing resilience in the payment systems that are used, as well as in basic infrastructure such as the electricity supply and telecommunications.

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

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. Due to the declining use of cash, the number of bank and cash in transit robberies has fallen dramatically from the high levels witnessed 15–20 years ago. 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. At the peak of the robbery wave in 2008, two bank branches and one armoured vehicle were robbed each week, causing a great deal of distress to

Number of fraud offences reported to the police and the number of bank and cash in transit robberies (2000–2025).



Source: Finance Sweden and Swedish National Council for Crime Prevention.

the affected staff. 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. Even though 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 cash 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 raises the risks to staff and increases the risk of money laundering.

12 Threats to security-sensitive activities

Security-sensitive activities are activities that are of significance to Sweden's security. Not all of Sweden's banks engage in security-sensitive activities. In cases where a bank conducts security-sensitive activities, such activities only constitute a limited portion of the bank's overall business. Threats to security-sensitive activities may often resemble threats to other parts of the bank, both in terms of the underlying threat actors and the possible methods of attack. As a result, this section may appear to overlap other parts of the report.

Please note that, unlike the rest of the report, this section is describing the threats to a very limited and specific part of some of the banks' activities. The assessments provided below are based on current conditions, but are forward-looking, with a 1–2 year outlook. However, they may need to be reviewed on an ongoing basis. This section is based solely on the situation assessments by the Swedish security authorities and other open and commercially available sources and is a summary of a longer report that is available to banks engaged in security-sensitive activities.

Security-sensitive activities

The protection of security-sensitive activities is referred to as protective security, and is regulated by the Protective Security Act, the Protective Security Ordinance and regulations issued by various authorities, including the Swedish Security Service.

The decisive factor in determining whether an activity is considered significant to Sweden's security is whether a hostile act – such as espionage, sabotage, terrorist offences or other crimes – or the disclosure of certain information could result in harmful consequences at a national level. Harmful consequences at a national level might include, for example, disruptions to or the loss of supplies, services and functions that are essential from a national perspective.

Overview of security threats to the financial sector in Sweden

According to the Riksbank, the greatest threat to the financial system's participants and infrastructure comes from state-run and state-sponsored threat actors. In a 2021 report, the Riksbank notes that "state actors are currently seeking access to digital infrastructure that is critical to Swedish society in order to be able to disable it should they wish to". In other words, state-run or state-sponsored threat actors may in future increasingly have the intent and the ability to carry out cyberattacks and sabotage that could harm key societal functions in Sweden. Neither organised crime nor ideologically motivated groups are considered to be significant threat actors in relation to security-sensitive activities.

Foreign powers employ a wide range of methods to achieve their objectives, but when it comes to the financial sector, the cyber domain is considered to be the platform most frequently targeted in attacks.

Russia as a threat actor targeting security-sensitive activities in the financial sector

Russia is an actor that has advanced cyber capabilities, which are an integral part of the country's intelligence services. Cyber operations are used, for example, as a tool for intelligence gathering, strategic positioning and operations to exert influence. The motives may include gaining long-term access, covert information gathering, sabotage and the exploitation of third-party dependencies.

Unlike the more overt destructive cyberattacks that are occurring in Ukraine, cyberattacks outside Ukraine are considered primarily to involve covert information gathering. To date, there have been no widespread examples of destructive cyberattacks in the financial sector outside of Ukraine. Wiper malware, such as ZEROLOT, has been used against the energy sector in Ukraine, however, and if the security policy situation were to deteriorate, such capabilities could be used against critical infrastructure in Sweden.

In the coming years, Russia is expected to rely increasingly on the use of organised crime, ransomware groups and hacktivist fronts, in order to deny involvement in acts of sabotage.

China as a threat to security-sensitive activities in the financial sector

China is viewed as an actor that is focusing on long-term intelligence gathering, strategic positioning and preparations for gaining access, rather than destructive attacks. These activities are primarily targeted at government agencies, research and academia, as well as high-tech development. The financial sector, on the other hand, may be subject to indirect exposure through third-party breaches or incidents involving cloud or telecommunications providers.

Security-sensitive operations are operations that are of significance to Sweden's security.

Iran as a threat to security-sensitive operations in the financial sector

Iran's activities in Sweden that pose a security threat consist of both intelligence gathering and attempts to exert influence. Iran's primary targets in Sweden are considered to comprise Israeli and American operations, as well as certain individuals and organisations from the diaspora that are perceived to pose a threat to the Iranian regime. Iran is therefore not considered to have the intent or the ability to attack security-sensitive activities in the Swedish financial sector.

Security threats to Swedish banks' security-sensitive activities

The greatest threats to Swedish banks' security-sensitive activities are considered to come from state-run or state-sponsored actors, with Russia being considered the primary threat actor. Russia is the actor deemed most likely to have, or to develop, the intention of trying to destabilise Sweden as a nation, for example by attacking key points in the Swedish financial system.

It is well documented that Russia possesses highly advanced capabilities within both the cyber and intelligence domains. However, capabilities at this level are likely to be very few and are therefore reserved for the most important targets.

The Swedish banking market is diversified, but a large number of banks supply similar services, and there is a degree of interchangeability among them. In addition, the banks have well-established security measures and recovery capabilities. An attack on a specific bank would consequently probably have only a limited impact in this context.

It is therefore unlikely that security-sensitive activities at Swedish banks would be subjected to targeted cyber-attacks exploiting zero-day vulnerabilities, specialist operations by sophisticated sabotage units or infiltration by the Russian intelligence services through the strategic placement of operatives. In this context, the most likely scenario is considered to be an attack of a less sophisticated nature. Such attacks can be carried out using the attackers' own resources or via proxies, for example by enlisting the help of various criminal actors. The latter makes it difficult to determine who is behind an attack.

Overall assessment

- **Threats related to information security:** The assessment is that, in the cyber domain, there is probably both the intent and the ability to carry out fairly sophisticated destructive attacks, in the form of extensive and sustained DDoS attacks or attacks using malware that rapidly exploits newly discovered vulnerabilities. It is also considered that there is both the intent and the ability to exploit identified vulnerabilities to conduct covert information gathering.
- **Threats related to personnel security:** Even if the intent exists, the ability to carry out attacks using insiders is considered limited. The assessment is that the insider threat primarily consists of the opportunistic exploitation of individuals who generally lack detailed knowledge or higher-level physical or logical access rights. These individuals can be used as enablers of, or to carry out, attacks against information systems or physical facilities for the purposes of

espionage or sabotage. However, it cannot be ruled out that individuals involved in security-sensitive activities may also pose an insider threat.

- **Threats related to physical security:** Even if the intent exists, the ability to carry out sabotage or physical attacks in order to obtain sensitive information is considered to be significantly more limited than within the cyber domain. The resources that could reasonably be allocated to attacks against Swedish banks are mainly considered to rely on the use of local proxies. These are considered to lack effective planning and coordination capabilities and to lack long-term perseverance. Their practical abilities are considered to be limited to more basic forms of physical assault.

Need for action by politicians and authorities

- Swedish banks support the Swedish Post and Telecom Authority's (PTS) proposal, i.e. that the Swedish Security Service be tasked with investigating the possibility of establishing standards for assessing harmful consequences at a national level in the civilian sector.

  In a 2024 report to the Government, PTS n oted that the vast majority of operators face significant difficulties both in describing the potential harmful consequences for Sweden's security that might arise should their own operations be targeted by hostile acts, and in assessing the severity of those consequences. PTS noted several related issues, including the fact that the supervisory authorities sometimes send conflicting signals regarding their assessment of the operators' significance to Sweden's security.

  For this reason, PTS proposed that the Swedish Security Service be tasked with investigating the possibility of establishing standards for assessing harmful consequences at a national level in the civilian sector. Sweden's banks support the proposal from PTS.

- Swedish banks are calling for a structured collaboration regarding security protection in the financial sector. Such a collaboration should be led by government agencies.

  The financial sector is complex, and there is a high degree of interdependence among its various players. It is difficult for a single actor to have an overview of all the factors needed to make certain assessments. The Swedish Financial Supervisory Authority described this situation in a 2022 report, highlighting the need for a wide-ranging and comprehensive analysis aimed at identifying which companies and processes are most worth protecting from a national perspective.

  Although security protection regulations apply to each actor individually, Sweden's security is likely to benefit significantly by establishing a structured collaboration for security protection work within the sector. Such a collaboration should not only include banks, but also other actors in the financial sector that conduct security-sensitive operations, both companies and government agencies.

  Examples of specific sector-wide activities include analyses of:

  – which services, supplies, functions and capabilities in the sector (at sector level) are of importance to Sweden's security.
  – what harmful consequences for Sweden's security could arise from hostile interference with the aforementioned services, supplies, functions and capabilities, and how soon after an attack such harm would rise.
  – security threats to security-sensitive activities in the sector.

  Swedish banks are calling for a collaborative initiative from the Swedish Financial Supervisory Authority, the Riksbank and the Swedish National Debt Office on this matter. If operators fail to collaborate, stakeholders may draw different conclusions, resulting in the sector's overall security protection being weaker than necessary.

The assessment is that there is a threat to the banks' security-sensitive operations, and that this threat will persist during 2026.

Threat levels and trend indicators

Threat levels

Low
The threat is assessed as low – there are few or no reported incidents. The impact on operations is limited. Existing processes and controls are deemed appropriate to address the threat.

Elevated
The threat is assessed as elevated – there are clear indicators of increased activity or of incidents becoming more sophisticated and difficult to defend against. The threat landscape requires increased vigilance and, in certain cases, enhanced checks or temporary security measures. Regular monitoring of the situation and more frequent supervision are recommended. Resource requirements and priorities may need to be adjusted.

High
The threat is assessed as high – there is a risk of incidents that could have serious consequences for operations unless measures are taken. A number of factors indicate a situation that calls for immediate action and ongoing monitoring within the organisation and with partners.

Trend indicators

Increasing
The threat landscape is showing clear signs of intensifying over time. Activity by relevant stakeholders is increasing, or the risk of more serious consequences for operations is rising. The situation calls for increased vigilance and, in many cases, stricter controls or measures to enhance preparedness. If this trend continues, the threat level may soon need to be raised.

Unchanged
The threat landscape remains unchanged and is stable over time, with no signs of rapid change. Activity by threat actors is anticipated and follows previous patterns. The situation requires continued monitoring, but does not call for any immediate changes to preparedness or security measures. A stable trend does not mean that the threat level is low, however, simply that it is constant.

Decreasing
The threat level is decreasing compared to earlier periods, and the indications are becoming fewer or less serious. There are signs that the measures taken and external circumstances have had the desired effect. The situation should continue to be monitored, but the current situation is less critical than before. If the downward trend continues, the threat level may be lowered in the long term.

Design and graphic production: www.luxlucid.com Stockholm, May 2026

Svenska
Bankföreningen
Finance Sweden

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