

Threat assessment for banks in Sweden

Published May 2024



Svenska
Bankföreningen
Swedish Bankers' Association



Threat assessment for banks in Sweden

Published May 2024

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

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

The security policy situation has been deteriorating for several years. Russia's ground invasion of Ukraine in February 2022 has redrawn the threat landscape. The invasion is affecting the banks in most areas of their security activities, and they have placed increased focus on civil defence and contingency issues.

The assessment of the threat landscape is divided into nine different areas, as follows.

Summary	5
Bank robberies, cash in transit robberies and ATM attacks	6
Abuse, personal threats and violence against bank staff	7
The threat from insiders/enablers	10
Security policy developments and preparedness	12
Information security and cybersecurity threats	13
Fraud and financial crime	16
Money laundering	24
Terrorist financing	28
International sanctions	29



Summary

There were no **bank and cash in transit robberies** in 2023, but there were five attacks on Bankomat AB's ATMs.

As regards **harassment, personal threats and violence against bank staff**, the banks have been reporting increased tension and tougher customer behaviour in recent years. Many employees are afraid to represent the bank in legal contexts. The exposure of individual employees can increase the threats towards the individual rather than the bank. A safe working environment for bank staff is not only the responsibility of the banks, but also part of a broader societal commitment.

An **insider/enabler**, acting on behalf of criminals or a foreign state, can exploit their insights into the bank to conduct illegal transactions or manipulate financial flows. In this way, threat actors can also influence a bank's decisions, information flows and business strategies. Foreign states can employ networks of insiders to gather intelligence, destabilise the economy or influence political decisions.

During the year, the field of **information and cyber security** has been characterised by threats from criminal and state-sponsored actors, particularly following Russia's attack on Ukraine. The number of financial companies affected by ransomware attacks has increased, albeit from a low starting point. Denial-of-service attacks against banks have continued, but with limited impact. The threat to critical infrastructure has been highlighted by the sabotage of gas pipelines and telecommunications cables in the immediate area. One growing threat is the rapid exploitation of technical vulnerabilities on the part of threat actors, as well as the use of AI for fraudulent purposes against both customers and bank staff.

According to the Police, almost half of **fraud offences** are linked to organised crime and gang crime. During the year, consumers and businesses have become even more vulnerable to fraud, with even greater consequences, and this is also affecting the banks. Social manipulation has meant that crime has become more targeted and personalised. Bank customers and businesses are subjected to a variety of fraud schemes, with vishing, smishing, investment, romance and credit fraud all having increased in 2023. The number of straw men who are enabling these schemes remains a problem.

Money laundering threats persist and have their origins in areas such as fraud, drug trafficking and tax crimes. Companies are increasingly being employed as tools for financial crime, with straw men being used to hide the real operators. Other risk areas in relation to money laundering are the exploitation of the welfare system, currency exchange, cash handling, cryptocurrencies, the real estate market, luxury consumption and the gambling sector.

In recent years, the number of cases of suspected **terrorist financing** via cryptocurrencies has increased. One risk factor is the fact that the banks often have no access to information about how such financing is carried out and who is involved.

As geopolitical tensions intensify, **international sanctions** have become an increasingly important means of exerting pressure on foreign and security policy. At the same time, it has become increasingly difficult for operators to understand and apply the sanctions. Greater information is required here, along with cooperation and dialogue between the actors in the field of sanctions.

Bank robberies, cash in transit robberies and ATM attacks

There were no bank robberies in 2021, 2022 or 2023. This is a result that has not previously been recorded in 40 years of measurements. This reduction, and maintaining the figure at zero, is explained by the fact that the cash chain from the depository via cash in transit (CIT) companies to ATMs has been bolstered, banks have reduced manual cash handling over the counter and customers are increasingly using electronic payments.

There were also no CIT robberies in 2023. The last ten years has seen a marked decrease in the number of CIT robberies compared with the previous decade. The decrease can be explained by more effective protection systems, banknote staining, fewer transport operations and improved cooperation and preventive measures between CIT companies and the police.

Bankomat AB's ATMs were attacked on five occasions in 2023. This includes ATMs being exploded or cut through, but not the skimming of cards.

The assessment is that the threat of bank and cash in transit robberies persists, but that the number will remain at a low level in 2024, as will the number of attacks on ATMs.





Abuse, personal threats and violence against bank staff

Several employees and managers in the banks testify to a more aggressive tone and tougher customer behaviour in recent years. Banks are receiving indications that suggest that employees are feeling less secure, and surveys from Finansförbundet (Sweden's largest trade union for employees in the financial sector) show that employees are being subjected to threats and violence. The picture is not the same everywhere: some banks consider that threats and abuse are at roughly the same level as before, while others have noted a strong upward trend over the past year. It is difficult to explain this change – it may be the result of preventive measures that have been taken, an increased willingness to report or an actual increase. For those banks that have large branch operations, around half of the instances of abuse and threats are linked to physical branches, while the other half are directed at telephone banking.

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

Tools for dealing with threatening customers

The banks are today terminating more customer relationships. The reason for this is that more customers make unlawful threats against bank staff, and the

banks are also discovering more irregularities. When the bank terminates a customer relationship or refuses to allow a person to become a customer of the bank, an internal process is required to assess and anticipate possible threats both to the bank's branches and to employees. However, the threat scenario anticipated by the banks in relation to the termination of customer relationships has not materialised to the extent that was feared. The banks have been proactive in their security work, but they still need to be prepared.

The bank provides training in conflict management with discussion material for all employees working in branches and telephone banking. Employees can find themselves in difficult situations with financially distressed customers, and the banks are therefore also working with support functions.

Other tools for dealing with customers who are demonstrating poor behaviour include the bank calling or sending warning letters to the customer, explaining that it will not accept abusive behaviour towards its staff.

The banks are trying to develop methods to better understand and target their initiatives – is it a case of an illegal threat, an unnecessary expression, a raised voice, an upset customer or an unpleasant situation? The unsafe situations that arise in physical meetings with the customer tend to be repeated in online and telephone meetings. The shift from a normal tone of voice to being unpleasant is considered to be short. At the same time, the limits for what an employee may be prepared to accept vary for different individuals.

Different parts of the bank are exposed to threats in different ways

A threat scenario can be actual or perceived. The difficulty in assessing and communicating an actual threat scenario lies in the fact that it is hard to determine threats based on actual events, although the level of anxiety is still considered to have increased. If you live in a small town and meet customers in person in everyday life outside of your work, the situation is different compared to an employee working in telephone banking.

There is deemed to be greater awareness of the actual threat scenario at bank branches than at head offices, as staff at bank branches meet customers in person. However, the opposite can also apply for banks that have telephone banking and a head office, in which case the head office is more vulnerable. This is largely related to what contact channels are available for dissatisfied customers. If the bank has a branch operation, customers will often go to a physical bank branch. If the bank only has a visible physical headquarters, this will be more exposed compared to a telephone banking operation, which can be situated in different locations around the country. Decision-makers involved in money laundering and fraud investigations, which are often based in central functions, are also affected by the threat landscape.

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

An increasing number of public authority enquiries

Banks are receiving more and more public authority enquiries, for example in relation to transactions associated with criminal investigations. There are signs of increased anxiety among certain employees working with customer due diligence, reports of money laundering and fraud. The exposure of individual employees, rather than the bank, can lead to increased threats towards the individual.

In response to these threats, the banks are working to protect the identities of employees. E-mails are sent to a greater extent from central functional mailboxes, such as sakerhetsavdelningen@banken.se or kundkontakt@banken.se. Furthermore, external customer communications by fraud investigators are restricted. The banks have alternative aliases that can be used depending on sensitivity, for example when terminating a customer relationship, and the idea of introducing systems for aliases and procedures regarding this is being considered. It is very easy to find a person who has a unique name in Sweden, and the question here is whether a bank employee needs to display their name.





Increased efforts to combat crime in the form of additional checks, better awareness and follow-up can create frustration on the part of customers.

Employees do not want to represent the bank in legal contexts. This is due to a fear of being threatened and persecuted. Employees may consider it hard to report threats or crimes they have been subjected to in their work to the police, as this can lead to new threats. The bank cannot make such reports, rather this must be done by the employee who was affected by the threat. A report becomes a public document, with the employee as the injured party. The bank can ensure that support is available in the event of any trial, but many employees still experience a high level of insecurity in these situations.

Increased efforts to combat crime in the form of additional checks, better awareness and follow-up can create frustration on the part of customers. Ensuring a safe working environment for bank staff is not only the bank's responsibility, but also a part of a larger commitment for various actors in society to combat fraud and money laundering.

The Swedish Security Service raised the terrorist threat level from 3 to 4 in August 2023, and as a result the banks have urged their employees to be more vigilant, highlighting the importance of following the authorities' advice. Even though the banks themselves are probably not a direct target, the banks have conducted an analysis of the branches/sites in large towns and cities that are adjacent to potential targets. This has led to a review of business continuity plans as well as alternative travel routes for key personnel. Some activities have been accelerated in response to the change in the terrorist threat level, building on the banks' existing security and business continuity work.

Several banks have been the subject of demonstrations by groups that want to protest against the banks' operations, such as environmental organisations. This is not a problem for the banks, rather it is a natural

part of an open society. However, some of the protests and actions have involved individuals blocking entrances and exits, which risks complicating an evacuation, should one be required. This puts both staff and customers at risk.

NEED FOR ACTION

Due to the developments taking place, the Swedish Bankers' Association sees a need for the following measures and initiatives on the part of politicians and authorities.

- The requirements imposed on the banks by the authorities have contributed to an increased threat level in relation to bank employees. The banks are compelled to expose individual employees in the event of a police report, which increases the risk of threats. It should therefore be possible for the bank to file a police report in the event an employee does not wish to do so for some reason. In this way, the person making the report is neutralised, as it is the organisation's stance and not that of the individual employee. The bank can then select which individuals are to represent the bank.
- Banks, as a separate legal person, should also be given the opportunity to report straw men to the police.

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

The threat from insiders/enablers

Regarding the problems associated with enablers of crime, insiders are an ever-present factor requiring both vigilance and adequate measures.

The incentives to plant an insider/enabler in a bank are considered to be strong, as it provides greater opportunities for both fraud and money laundering schemes for criminals, as well as the opportunity for an antagonist to exert influence. An insider/enabler might be a person with a level of authority within the bank that makes it possible for an external antagonist (criminal group, foreign power, etc.) to carry out transactions and activities.

An insider might consequently be an active enabler, actively share information or have more of an advisory, coaching role. An insider is often a younger person with a connection to high-risk countries through their relatives, holidays or background. They are good at their job, and the gender distribution among enablers is even. The person often has accounts in another bank, receives income other than their salary and has their own mobile subscription.

It is not uncommon for external antagonists to seek contact with the bank's staff 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 negative contacts, for example including offers to conduct paid interviews on LinkedIn, is deemed to have increased over the past year. For example, criminals and other hostile parties also advertise for people who are prepared to introduce malware into the bank's systems. In this way, social

manipulation merges with the physical threat landscape through improper contacts that can subsequently lead to physical threats being made against employees. It is also possible that a person who has a connection to an external antagonist might apply for a job in a bank to enable crime.

Building security takes time

One question that arises is how the bank can protect employees from improper contacts from state actors or organised crime groups, for example. The security protection legislation, which affects a limited proportion of the bank's operations, regulates how this should be managed, but the threat exists across a wide range of activities, from fraud to how to circumvent sanctions. Background checks, which are primarily used at the time of employment, do not offer the same opportunities as a security investigation. In this respect, it is necessary for the banks to have sufficient means of control, both during the recruitment process and during the period of employment. Nowadays, the banks need to rely largely on the information provided by the jobseeker him or herself.

An insider/enabler can be a bank clerk who receives payment from criminals to ensure that the criminals' transactions and activities can be carried out without problems. They could also be a bank employee who is being subjected to threats. Vulnerabilities can also exist through family relationships, with the result that the exercising of the position, which is based on suitability, can be assumed to be negatively affected.





Preventing, deterring and detecting internal crime is an important part of a bank's security work.

Some approaches require an enabler on the inside

Some approaches cannot be carried out without an enabler on the inside who has knowledge of the bank's products, services and procedures. The enabler assists the criminal with confidential information that facilitates the implementation of the criminal scheme. This may involve information about procedures and processes, rules for granting credit and rules regarding monitoring transactions. 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/enabler in the case of repayments.

The banks may need to become more vigilant about the risk of insiders being used. The banks can also work together to ensure that an insider, after being discovered, is unable to find employment in a new bank and continue their enabling activities there. The increased mobility on the labour market raises the issue of whether there should be some form of right of notification between banks in order to deal with the challenge of insiders.

Need for information from law enforcement authorities

One problem in relation to detection and adequate measures is that, in many cases, the banks do not receive sufficient, timely information from law enforcement authorities who suspect the presence of an insider in a bank. Since insiders often use private communication channels to illegally disseminate information and communicate with criminals, the law enforcement authorities are best placed to detect such activities. This is due to the fact that, during preliminary investigations, it is often possible to e.g. obtain information and secret coercive measures from mobile phones/computers. It is important for this information (which may be "surplus information"

within the preliminary investigation) to be brought to the attention of the banks, as soon as the legal conditions exist. Without this information, it will be significantly more difficult for the banks to take adequate action.

Even though, in February 2024, the Swedish Security Service has highlighted threats from Russia, China and Iran in particular, the difficulty with insiders is that it could be anyone. Approaches to dealing with this threat range from technical verification options to measures that are implemented to ensure that all employees feel safe reporting abnormal behaviour, secure in the knowledge that they will not be perceived as informers.

The banks' own control mechanisms

Preventing, deterring and detecting internal crime is an important part of a bank's security work. The banks' internal control mechanisms are extensive and consist of entry and exit logs, following up customer searches, authorisations, documentation requirements, etc. In order to reduce the vulnerabilities of the business or of individuals, and to protect both the business and employees against the risk of being exploited by criminal actors, the security departments also need to be involved in the internal investigation process in cases of misconduct and rule violations.

The assessment is that insiders/enablers are a threat from organised crime that exists internally in the banks and that will persist in 2024. Given the increased international conflict landscape and political tensions in relation to Swedish interests in recent years, certain state actors have a heightened interest in insiders/enablers.

Security policy developments and preparedness

Since Russia's illegal annexation of Ukrainian Crimea in 2014, Sweden's security situation has gradually deteriorated. Swedish security policy has been based on a regulatory-based regime that originates from international law, rules and agreements. Due to Russia's invasion of Ukraine in February 2022, the European security order has ceased as a common system.

Grey zone

Nowadays, the threat from foreign powers is largely characterised by so-called grey zone problems, with warfare that today can be described as mostly contactless, i.e. conducted via remote warfare and global reconnaissance. Grey zone is a concept in which neither "war" nor "peace" prevails. Grey zone activities are a collective term for antagonistic influence activities such as manipulating information, projecting power in different ways, intentionally violating a country's airspace, cyberattacks, etc. The purpose of grey zone activities against Sweden is to try to influ-

NEED FOR ACTION

Due to the developments taking place, the Swedish Bankers' Association sees a need for the following measures and initiatives on the part of politicians and authorities.

- The governance and management of the contingency work in the sector needs to be improved. The sector's authorities, along with the companies, need to develop a clear common vision for the financial sector's contingency work. This vision must be firmly anchored and be able to be understood by all authorities and companies in the sector, so that everyone is working on the basis of the same assumptions in their ongoing work.
- The identification of vital societal functions and critical infrastructure in the sector, which was carried out in 2023 under the management of the Swedish Financial Supervisory Authority, needs to be concluded and clearly communicated to all actors in the sector, not just those that have been involved in the work. The plan for 2024 also needs to be clearly communicated. There are currently many companies in the sector that are unsure about what contingency work is actually in progress. Clear, sector-wide priorities therefore need to be established and communicated. The areas of focus that are deemed to be particularly important for increasing the overall capacity and impact in the sector should be prioritised.

ence Swedish decision-making and reduce our freedom of action. It can be related to damaging trust, undermining our values, dividing us and weakening our resilience, or disrupting socially important functions such as banking.

Swedish banks today make up a large part of the Baltic countries' financial infrastructure, which also affects the threat landscape. The risk of antagonistic grey zone activities aimed at influencing banks and financial infrastructure is therefore considered to have increased. The banks are used to protecting operations against various threats, and to carrying out planning and training in order to manage and resume operations in the event of disruptions and incidents. Russia's invasion of Ukraine shows how quickly things can change, and that long-term contingency work is required in Sweden in order to manage developments outside the country.

The sector's contingency work

The banks participate actively in existing private public partnerships such as FSPOS, as well as in the contingency-enhancing activities that have been initiated by the Swedish Financial Supervisory Authority and the Swedish Central Bank.

Sweden also has a national cybersecurity centre, which has been created with the aim of reinforcing Sweden's ability to prevent, detect and manage antagonistic cyber threats and promote a greater exchange of information between private and public players. The financial sector has been collaborating with the centre since 2022. The aim is to strengthen cybersecurity within the financial sector, and jointly to increase Sweden's resilience to cyber threats. The banks need to receive intelligence and information about the security threats to Sweden and the Swedish financial sector.

The assessment is that Sweden's security situation and the deteriorating threat landscape are affecting the banks.



Information security and cybersecurity threats

In 2023, the threat landscape in the field of information and cyber security has continued to be driven by the threat from criminal groups and state-sponsored actors, in particular due to Russia's war of aggression against Ukraine. For the banks, digital warfare and other types of hybrid threats are part of the new normal. Cyberattacks hit companies and organisations on a broad and opportunistic scale, and there is often no direct target. The ones that are hardest hit are those that have not carried out long-term, structured work in respect of their cyber security.



Increase in ransomware attacks against Swedish businesses

In 2023 and early 2024, ransomware attacks, i.e. ransomware that encrypts its victims' data until a ransom is paid, have affected a large number of businesses and therefore attracted a great deal of public attention. Among those affected are the Church of Sweden, the IT company TietoEvry and various Swedish municipalities. The attack on TietoEvry affected a large number of the company's customers and is an example of what can happen when concentrations of critical services are built up at individual suppliers. Swedish banks that have outsourced parts of their IT operations need to have a good awareness of the concentration risks to which they are exposed.

In the banking sector, the ransomware attack on the major Chinese bank ICBC and their US branch in November 2023 was particularly noteworthy. The attack affected the U.S. Treasury bond market, and ICBC needed to inject USD 9 billion into the system to manage unsettled deals. Other examples of ransomware attacks on the financial sector include the attack on ION, which affected derivatives trading in February 2023, and the attack on Equilend in January 2024, which affected securities trading. Several European banks and other companies experienced losses of information in connection with the vulnerabilities that were discovered in the MOVEit application in June 2023.

In other words, there has been a slight increase in cases where financial companies have been hit by ransomware attacks. The increase is taking place from a low starting point and it is still assessed that banks have higher security and a more developed understanding of cybersecurity risks and threats than other types of companies and government agencies. The banks have been working on these issues for many years, as the threat landscape has shifted from the physical to the digital world. Another explanation may be that a successful ransomware attack that locks the bank's system also hampers criminals' ability to blackmail the bank for money.

There is a continuing trend of criminals not needing to develop their own ransomware, as they can buy a ready-made solution, "ransomware as a service", and then use it to attack their targets. In addition, data is not only encrypted, but criminals also steal data in connection with the ransomware attack and threaten to post the information publicly on the internet unless the ransom is paid. This type of organised crime is evolving towards resembling legitimate businesses. Among those that use ransomware, it can be difficult to distinguish between state-sponsored actors and criminal groups. It is also likely that criminal groups are sometimes acting on behalf of states.

Banks should continuously monitor and evaluate the ransomware threat and look to improve their protective measures. In the event of an attack, the bank must have developed measures to enable them to detect, manage and restore operations. Large-scale ransomware attacks on the financial sector could have a huge impact. Studies and analyses carried out by the International Monetary Fund (IMF), the European Systemic Risk Board (ESRB) and the Swedish Central Bank indicate that a sufficiently large cyberattack on the financial sector could threaten financial stability.

Destructive malware

During its war of aggression against Ukraine, Russia has repeatedly used destructive malware, known as “wiper malware”, with the aim of destroying systems and data in critical infrastructure. Ukraine has been successful in defending itself. In the 2023 threat assessment, the threat to Swedish banks was described as the banks having an indirect risk exposure, as a result of the fact that attacks risk spreading to other players and to geographic regions other than the intended target area. This type of uncontrolled spread of destructive malware does not appear to have occurred during the period. There have also not been any reports of Russian threat actors carrying out destructive cyberattacks against Western banks and financial companies. Despite this, there is every reason for the banks to continue to monitor this area.

Denial-of-service attacks

During the period, Swedish banks have continued to be exposed to denial-of-service attacks, designed to affect the availability of online banking services. Actors linked to foreign threat actors and criminal organisations have carried out denial-of-service attacks on businesses and companies in NATO countries and their allies, including Sweden and the banks. The attacks have often had a very limited effect. The purpose of the attacks is considered to be the impact of information on society and citizens, by trying to demonstrate that socially important financial services are at risk. The assessment remains that the banks’ protection has worked well, and the attacks have not had any major impact on online banking services.

Sabotage of infrastructure

The 2023 threat assessment noted the sabotage of the Nord Stream 1 and 2 gas pipelines in September 2022, which highlighted the threat to critical infrastructure arising from the security situation in the immediate area. During the reporting period, the threats have been made more tangible by the suspected sabotage of the Balticconnector gas pipeline between Finland and Estonia as well as a telecommunications cable between Sweden and Estonia. It has also been reported in the media that foreign powers are mapping critical infrastructure in the Baltic Sea region. The Swedish



Banks should continuously monitor and evaluate the ransomware threat and look to improve their protective measures.

banks need to continue focusing on reviewing their dependence on critical infrastructure. They need to plan for the possibility of further enhancing their resources and capacity, such as electronic communications and electricity supplies. This is also in line with the total defence and contingency work that is now being intensified, both in the financial sector and nationally.

Risks in the IT supply chain

The banks use IT suppliers, cloud services and publicly available software in their operations. Risks associated with this include malware that can be spread through established supply chains, as well as the fact that vulnerabilities are discovered by threat actors who immediately use them to attack systems before they can be rectified. Vulnerabilities of this type are usually referred to as zero-days. Attention has been drawn to a number of such vulnerabilities globally during the year. Some of the more high-profile cases have occurred in software such as MOVEit, VMware and Citrix NetScaler. Zero-days also affect software that the banks’ IT functions employ in their support operations.

These vulnerabilities also pose a significant risk to the banks, as they enable attacks in areas where there are no defence mechanisms. The number of vulnerabilities also appears to be on the rise, in addition to the fact that they are being exploited more rapidly than in the past, which gives the banks less time to react. The banks also need to continue actively monitoring and addressing non zero-day vulnerabilities. All in all, this is increasing the pressure on the banks’ IT functions, which in turn is entailing a need to provide resources to manage the risks.

Artificial intelligence and deep fakes

Fake videos, images or audio that are so elaborate that they appear to be genuine are generally referred to as “deep fakes”. The development of artificial intelligence is both accelerating the development of deep fakes and making them even more difficult to see through. The use of deep fakes for fraudulent purposes represents a growing threat in society.

Within banking, for example, deep fakes could be used as a tool for social manipulation, by imitating people in executive management positions in contacts with e.g. bank staff in the field of payments. The aim could be to make fraudulent payments.

This threat area is probably still in its infancy and will no doubt evolve in the coming years. The banks need to develop their capabilities to be able to deal with this threat. This might involve training staff, for example, as well as using technology to detect deep fakes.

Phishing and banking trojans

Malware or links to malware via e-mails to bank employees are a common threat. Another approach is “spear phishing”, i.e. phishing that targets selected individuals at the banks. Spear phishing has been used, for example, to target employees within the banks who may have higher IT access rights. LinkedIn has been used to map the banks’ IT employees, who have then been sent 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 establishing a foothold in the banks’ infrastructure. At the same time, it is still common for phishing to be conducted that is not targeted at selected individuals at the banks, but that it is more opportunistic in nature. Phishing attempts can also be aimed at the staff of IT suppliers as a potential means of attacking the banks.

The assessment is that malware via phishing continues to be a high risk for the banks. Exercises and training for staff to enable them to detect phishing e-mails as well as technical solutions to block phishing e-mails remain important countermeasures.

The occurrence of banking trojans has increased slightly during the year, but it is considered that Swedish banks and bank customers have not been particularly affected. Banking trojans that infect mobile phones and mobile banking solutions are often designed to steal customers’ login credentials. Banking trojans developed for Android phones are still more common than for iOS phones. Bank customers have had their mobile phones infected by downloading apps that contained malware.

NEED FOR ACTION

With a deteriorating security policy situation and increased cyber threat, the Swedish Bankers’ Association considers that there is a need for a series of coordinated measures and initiatives from government, authorities, the business sector and other parts of society:

- The exchange and use of information between public authorities and the business sector needs to be further developed. The banks need more and faster intelligence regarding potential cyber threats and vulnerabilities. At the same time, the banks are prepared to contribute their expertise in this area. The Swedish Bankers’ Association appreciates that the collaboration with the National Cyber Security Centre and the Financial Forum has been made permanent. However, it is clear that cooperation between the authorities has been hampered due to the lack of a clear principal for the centre. The Swedish Bankers’ Association therefore takes a positive view of the inquiry, which in the spring of 2024 will propose the National Defence Radio Establishment (FRA) as the principal for the centre.
- The Swedish Bankers’ Association is anticipating considerable challenges for the banks when regulations, both within the EU and national regulations, will overlap in areas relating to security, preparedness and resilience. The focus of the banks’ work will then be targeted at the administration and interpretation of terminology and definitions, as well as the mapping and ranking of different regulations, rather than on practical activities aimed at strengthening resilience. It is important to ensure that similar activities are not subject to several different regulations.

The assessment is that the threat landscape in the field of information and cyber security is becoming increasingly sophisticated, and that it is being influenced by criminal groups and state-sponsored threat actors. The cybercrime-related threats are becoming increasingly complex and collaborative. An increase in the number of ransomware attacks and zero-day vulnerabilities has been noted during the period. In the cyber field, the threat landscape can also be influenced by a hostile party who is persistent and driven, and who sees opportunities linked to the development of security policy.



Fraud and financial crime

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

According to the Swedish Police, 235,665 fraud offences were reported in Sweden in 2023, which represents an increase of 42,274 crimes, or 22%, compared with 2022.

Proceeds of crime from fraud on the rise

Prior to the past year's increase in the number of fraud offences reported to the police, the number of such reported offences had decreased by about 25 per cent over four years. The reason for this decrease is the implementation of PSD2 (the second payment services directive). The requirement for strong customer authentication in the PSD2 technical standard that came into force on 1 January 2021 resulted in a substantial decrease in the number of card frauds, mostly in respect of "Card Not Present" offences, when the physical card is not present during a transaction. The increase in the number of fraud offences reported to the police in the past year includes a significant increase in several modus operandi, although certain types of crime are decreasing, according to the Police.

Although the number of frauds reported to the police decreased by 25 per cent between 2018–2022, the gains made from fraud are increasing over time, according to the Swedish Police (report *The deadly frauds*, page 11, Ref. no.: A554.314/2022). The increase in the gains made from fraud can largely be explained by the marked increase in fraud involving elements of social manipulation, such as telephone / vishing fraud. Proceeds from crime relating to fraud were estimated at approximately SEK 4.2 billion in 2020, approximately SEK 4.6 billion in 2021, approximately SEK 5.8 billion in 2022 and approximately SEK 7.5 billion in 2023, according to the Swedish Police (report *Proceeds of crime from fraud offences 2022*, page 2, Ref. no. A232.846/2023 and report *Proceeds of crime from fraud offences 2023*, page 2, Ref. no. A233.272/2024).

In 2019, a total of 5,285 vishing frauds were reported to the police. By 2023, this number had risen to 29,347, an increase of 555 percent. At the same time, the number of major investigations into the crime clusters that are suspected of being responsible for a large proportion

of these vishing scams has decreased from ten investigations in 2019 to one (1) investigation in 2022, according to the Swedish Police (there is no data regarding the number of major investigations for 2023).

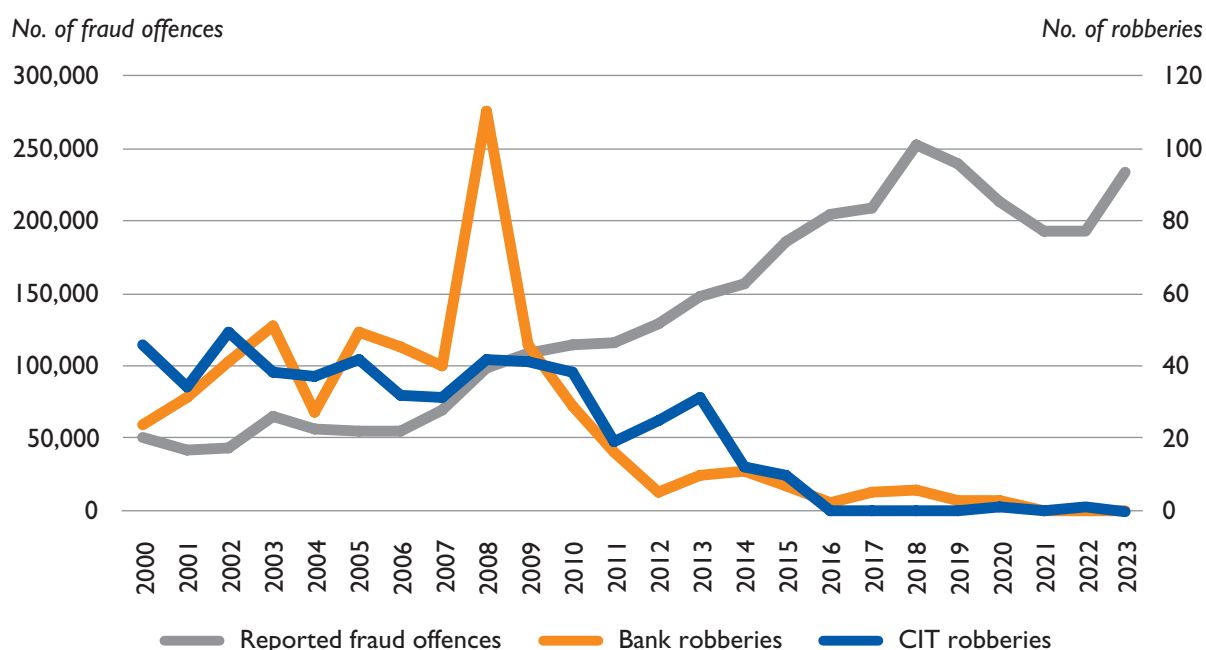
Organised crime with a high level of violent capital is currently influencing banks by acting as a "full-blown criminal organisation", impacting the areas of physical security, fraud and money laundering where the different elements are intertwined. According to the Police, almost half of the fraud offences can be linked to organised crime and gang crime. The funds are used for investments in both criminal environments and in the legal economy.

New products and third party vendors

One of the main challenges is that the development of services and digitalisation are progressing very quickly, which means that the threat landscape is also changing rapidly. The speed of these developments, in turn, requires real-time protection regarding information sharing. There is a growing need to share technical information such as cookies, IP addresses, information about vulnerabilities and targeted attacks. The banks are continually taking down fake websites, which demands additional skills and resource management.

The bank needs to understand what threats and vulnerabilities to both fraud and money laundering the new products entail, and to develop countervailing measures. New services and products are not always developed by the bank itself, rather this can take place in collaborations with other actors or be performed by third parties. It is necessary to strike a constant balance between versatility and customer friendliness on the one hand, and steadiness and increased security on the other. The development process is

Number of frauds and bank and cash in transit robberies (2000–2023).



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

strongly business-driven, and the customers expect the bank to offer new products and services in line with technological developments. Developments are also affected by political incentives, such as PSD2, which mean that the bank has less opportunity to implement relevant countermeasures.

With PSD2 and service deliveries based on third parties' access to accounts and data, which the banks refer to as "open banking", several parties have been added in the payment chain, entailing new risks and challenges. For consumers, it can be difficult to understand what they are giving their consent to and which actor has access to customer data. There is currently no clear specification of requirements in relation to third parties. Not everyone has the control in respect of the end customer that the authorities require the bank 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.

Legislation impacting the area

Currently, the EU is proposing a law regarding moving from "open banking" to "open finance", which can open the banks' infrastructure to even more actors in various financial services in addition to payments and account information. "Open finance" allows more financial operators to access and have the potential to share a large volume of financial data.

This means that more of the bank's customer data may be used by third parties in a number of financial

services within the EU with the customers' consent, i.e. not only for payments, but also for mortgages, loans, savings, pensions and insurance. 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.

Highlighted risks include cybersecurity risks, fraud and financial crime. The customers' knowledge and awareness about how products and services work, as well as how data is stored, used and distributed, are therefore all important issues. It is equally important for the same requirements to be imposed on all players within "open finance".

Another legislative proposal is the European Commission's proposal regarding changes to the regulatory framework for payment services. This will result in a Payment Service Regulation, which will be directly applicable in Sweden. This proposes mandatory reimbursement from the bank in the event of fraud where the fraudster is impersonating a bank employee. A shift in the division of responsibilities towards the bank having to compensate for more fraud could lead to an increase in "friendly fraud", where the customer claims to have been a victim of fraud. A further problem arises if the burden of proof lies with the bank, where all the technical and other data is pointing to the transaction being authorised.

With guaranteed reimbursement in the event of fraud, payment service users might be less concerned about security. Reduced attention to online risks could spill over into the use of all types of digital services, resulting

in payment service users becoming more vulnerable to cyber risks. This also removes the incentive for other stakeholders (telecoms and social media/online platforms) to collaborate with banks, as the entire financial burden is then borne by the banks. In order to address the problem effectively, the focus should instead be on preventive measures.

Another proposal from the EU is for payments to take place increasingly rapidly, so called instant payments. New rules will be entering into force in 2024 regarding payments in euros. These new rules require payment service providers to offer their customers instant payments in the same channels where they are offered regular account transfers in euros. In this context, channels refer primarily to internet banking, mobile banking and telephone banking. This is a worrying development, as instant payments entail a number of challenges in respect of fraud and financial crime. These challenges will grow if instant payments become available as an option for more types of payments. In order to balance these challenges and limit the risk of increases in the amount of fraud, the banks need to put new systems and new working methods in place with the aim of detecting and stopping fraud, while at the same time raising customer awareness about the risks associated with instant payments.

The banks have historically had the capacity to fend off fraud offences, but PSD2 and the digitalisation of society have altered the situation. The card payments' business model, infrastructure and risk distribution have previously served as a kind of protection for consumers. However, as the demands increase for e-commerce to use the bank's security solutions to a greater extent, the demands on customers are also increasing, both to be able to use the digital tools and to be able to withstand various forms of attempted fraud. As a consequence of the increased authentication demands within e-commerce, criminality has been driven towards methods involving a larger degree of social manipulation, such as telephone fraud. The customer is either tricked into surrendering information, or they are misled into carrying out a transaction themselves at the fraudster's request (a so-called authorised transaction under PSD2). The threat landscape has consequently changed and it is necessary for the preventive measures to be adapted.

The main fraud threats

Swedish consumers and companies are currently exposed to many different forms of attempted fraud. Everything from phishing for login credentials (e.g. e-identification and security device) to the distribution of malware via e-mail, text messages and websites. Consumers and companies are also exposed to romance, investment, vishing, smishing, credit and BEC fraud (Business E-mail Compromise scams, such as CEO fraud), as well as ID theft and advertising and social media scams.

Both consumers and businesses are increasingly being subjected to fraud with the aim 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 eID or security device.

The main fraud threats in 2023 have been vishing, smishing, investment, romance and credit scams. The methods used are explained below.

- **Vishing fraud (telephone fraud):**
The fraudster calls a consumer who, during the phone call, is tricked into either giving up codes from their security device or identifying themselves/signing orders with their eID. Nowadays, the customers are often tricked into carrying out the transactions themselves, for example under the pretext that money needs to be transferred to a "secure account".
- **Smishing fraud (fake text messages):**
The fraudster sends the consumer a text message containing information that is designed to get the customer to do something. The fraudster's intention is to create a stressful situation where the customer has to act quickly. For example, the customer may be urged to call a phone number, install software or follow a link and provide information. Common approaches include text messages containing information about "suspicious activity on a card or account", or text messages from "Mum who has changed her phone and needs help".
- **Romance fraud:**
The consumer is contacted and approached by a fraudster. The fraudster seeks to contact people in situations where they are vulnerable, and love is a strong driving force.
- **Investment fraud:**
The fraudster contacts a consumer and offers a fictitious investment opportunity, always with elements of high returns at low risk.
- **Credit fraud:**
The fraudster applies for a loan on false grounds. Examples might include false documentation, incorrect information or the fact that the customer has no intention of repaying the loan. The identity used may be from a person who has emigrated, be assigned to another person or be fabricated.

Social manipulation on the rise

The common denominator in the fraud schemes is the attempt and 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 personal. Consumers and businesses have become more vulnerable to fraud offences, at the same time as the consequences for the victims have become greater, and this is also affecting the banks.

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 the traceability being high.

There has been a growing trend in the past year for fraudsters to try to persuade customers to carry out authenticated transactions, by telephone, e-mail or text message. Scams affect all target groups, and current events in the outside world are often used as bait.

Another trend relates to an increase in the number of customers being repeatedly subjected to fraud. One of the reasons for this is that fact that data relating to these customers is spread between different criminal organisations or is simply reused. The most common recovery scam is where victims of crime are misled into believing that they can recover money from a previous investment scam. However, the banks are also noticing an increase in cases of customers who have been tricked through telephone scams being repeatedly targeted.

A growing challenge is where, for various reasons, vulnerable customers do not carry out the fraudulent transactions directly to the intended final recipient, but rather send the money, either voluntarily or on request, via other customers and/or institutions in one or more stages. This leads to difficulties in respect of the division of responsibilities, investigation and reporting.

Hybrid modus operandi dominating

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

The trend of scams where the customer has approved the transactions on internet or mobile banking entails a more complex problem for the bank, both when it comes to monitoring and understanding what has happened. The banks are devoting a great deal of time and resources towards talking to customers who have been subjected to such scams.

Another trend over the past year is where business owners and users with access to multiple commitments, such as accountants, have become more vulnerable. The fraudsters’ modus operandi are becoming increasingly difficult for the victim to see through. For example, new technology is being used to lull the victim into a false sense of security. The return from such crimes is often several hundred thousand kronor or more. In the worst-case scenario, scams can lead companies to bankruptcy. This is due to the fact that business owners do not enjoy the same basic protection as consumers against financial losses as a result of crime.

Customers are also tricked into installing remote control software on their phone or computer, giving the scammer full access and control over the screen and keyboard. In this way, the scammer can post transactions in the customer’s bank, which the customer is then tricked into signing. To counteract this, the banks are working on analysis of behavioural patterns regarding how customers use computers and apps.

The trend is similar when it comes to card fraud, i.e. that more and more fraud is occurring where the transactions have technically been approved by the payer. An example of a situation where customers are subjected to social manipulation relates to digital wallets. This method involves customers being tricked into sharing authentication and signing information with fraudsters, who instead connect a card to a digital device under the fraudster’s control. The fraudster often pretends, by e-mail or text message, to be from a bank, public authority, the police or a shipping company, directing customers to an interface where the customer has to fill in their information.


Artificial Intelligence (AI)

The fraudsters are already using an automated and robotised approach, and the banks need to monitor the trend as regards the fraudsters’ use of AI. Banks are witnessing automated conversations in some scams via social media and chat apps.

The banks are anticipating improvements in the quality of language and design, as well as scalability in future phishing, smishing and vishing schemes. There is a risk that the methods used against business owners, such as BEC scams and CEO fraud, will be reinforced with AI elements, for example through voice cloning, recorded messages, etc. It may become increasingly difficult for a bank to assess whether a customer who is the victim of fraud has communicated with a real person or not.

All banks inform their customers about how the bank’s services work, but information alone is not enough to reverse the social manipulation trend. There is no one change that can resolve the challenges with social manipulation, rather it is a case of, in addition to the banks’ own measures, working with a number of preventive and collaborative measures (see the section “Need for action” below).





Fraudsters are becoming increasingly skilful at mapping their intended victims in various target groups.

Better data sharing leads to better risk assessments

As customers today complete many banking tasks themselves, it is becoming increasingly important for the bank to be able to interpret customer behaviour and detect anomalous behaviour. The banks work systematically with preventive methods, such as limits and restrictions within products, as well as active monitoring based on the behaviour of customers aimed at managing the risks that exist.

If the legislation were to allow more data sharing between operators in society, for example of straw man registers and IP addresses, this would contribute to better monitoring through better risk assessments, both in the preventive work and in the banks' monitoring activities. The more information and data points the banks can share with each other, the greater the preventive effect.

When the banks do not manage the technical interface through their app or website, they receive less data for their fraud monitoring activities. Transactions to collection accounts are more difficult to monitor, compared to payments and transfers. If the bank is unable to see the recipient accounts, it becomes more difficult for the bank to monitor money laundering and fraud.

Developments in real-time payments involve both the same risks and some new ones. Real-time payments require the ability to both adjust limits and block transactions, as well as to balance versatility, security and steadiness. Since monitoring can only eliminate a small proportion, precise prevention tools are also required.

As customers today complete many banking tasks themselves, it is increasingly important for the customer to be able to handle the digital tools. The bank must provide training and information to the customer about how products and services work.

Home visits continuing

The number of home visits by fraudsters claiming to be bank officials, police officers or home care workers continues to be a problem. 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, security device or e-identification.

There is a real risk that the number of home visits and personal risks will increase when the bank blocks the potential for other approaches, and this needs to be considered as part of the work of combating fraud.

More people with weaker technical skills were exposed to higher risks during the COVID pandemic, as they were forced to use digital tools to a greater extent. This is not necessarily related to age, but to the lack of social gatherings where people could talk about these issues, resulted in greater ignorance. Home visits are increasing, although the numbers are small.

Scammers map their victims

A trend that has intensified in recent years is the fact that fraudsters are becoming increasingly good at mapping their intended victims in various target groups. Through information from search services, fraudsters can gain access to a person's personal identity number, address, income, etc. Using this information, the fraudster builds up a credible story with the aim of manipulating the intended victim. Fraudsters often hide behind "spoofed" phone numbers, i.e. masked numbers where the fraudster chooses which phone number is to be shown in the recipient's display, to try to make it look like it really is the bank that is contacting its customers.

Customers are rarely familiar with the way technology works, including the nature of remote control software. Technological developments are set to pose even greater challenges for both banks and customers when it comes to distinguishing between what is fraudulent and what is genuine.

One trend in the wake of these technological developments is “crime-as-a-service”, where information is shared and sold between criminal actors. Criminal schemes, malware, links, websites and customer information are sold on in several stages, and the fraudster does not need to possess solid technical expertise to be able to use these instruments of crime. In addition, there is an increased risk of fraud that is preceded by infringements at external parties, where the customer’s information is manipulated. If a bank bases its risk assessment on data from the external party, it will be inaccurate.

Credit fraud

Credit fraud has long been an extremely widespread phenomenon, which is now made easier by rapid digital loan application procedures, often within the framework of the emerging instant and unsecured loan markets. Tying together an understanding of the different types of credit fraud – in all parts of the credit process, from application to repayment – is challenging.

Regarding the perspective of the private customer’s application for the credit, the number of fake employer’s certificates, payslips, manipulated bank statements and measures designed to influence the outcome of credit applications remains at a high level.

In the case of corporate credit, it is often a matter of taking out a wide variety of loans in parallel during the period a company can be used as an instrument of crime, i.e. during the time that incorrect information about creditworthiness is indicated in the checks carried out by creditors. This relates to taking out regular business loans, other more rapid business loans, as well as making large purchases on credit of expensive goods such as machinery, equipment or vehicles. There is generally a straw man who is representing the company taking out the credit.

Since creditors always need to conduct some form of check regarding the existence, creditworthiness and ability to pay of the person or company, it is important to manipulate the system so that their creditworthiness appears better than it actually is.

One common scheme involves a person taking out as many and as large loans as possible from different creditors in a short period of time, with no intention of repaying them, and often with the intention of staying away or leaving the country. The fraudster takes advantage of the fact that the different lenders are not able to exchange information, i.e. before the time when the data starts appearing in the credit data. This can apply to both regular loans and purchases on credit.

Another common scheme is where a person takes out long-term loans, such as mortgages, on false grounds. Individuals who do not have a credit rating create a false picture of their financial position. As long as the person adheres to the agreed loan terms, the chances of the fraud being detected are often low.



Payments, instalments and the redemption of credit represent another risk area. All credit payments should be checked against due diligence data. When it comes to the customer's payment of the credit, there is a risk that the bank will receive funds from money laundering operations if the origin of the funds is doubtful, placing the bank in a difficult situation on how to manage the customer relationship. There is also a danger of cases becoming complex very quickly.

Countering credit fraud requires a large amount of resources and extensive analysis work. In addition, it is necessary to manage customers, provide staff training, implement changes in processes and conduct monitoring. Examples of credit fraud within consumer credit include e.g. straight rollers/bust out, i.e. people who take out several loans in a short space of time with no the intention of paying. Analysis of straight rollers have resulted in changes to onboarding processes, with the aim of detecting warning signs at an early stage. Estate agents are increasingly acting as enablers, above all in residential transactions on the private side, but also on the corporate side.

As credit fraud is based on one or more false items of information, a number of banks have started to use external services to check customers' income data. Nowadays, false information about income is also registered with Swedish authorities, which makes it more difficult for the banks to rely on and assess the reliability of the information regarding identities and family relationships. Since it is easy to change data that has been reported to authorities, the control mechanisms are partially being eliminated. Given this development, all stakeholders need to increase their training efforts, thereby raising the level of knowledge regarding credit fraud.

Straw men enabling fraud

In this context, straw men are enablers of financial crime, and the number of straw men in Sweden remains a problem. One problem is that criminals who are discovered in one bank quickly change to another bank and continue their criminal activities. The banks work in a structured way to analyse and counter-act the opportunities for the straw men to conduct repeated criminality.

Young people are often exploited and used as straw men, which can be a gateway to more serious crimes. One scheme might be where the young person is lured with the promise of earning SEK 10,000 quickly, as long as they receive and forward SEK 250,000. This can subsequently lead to threatening situations when the young person wants to pull out.

There are many straw men operating in Sweden. In total, more than 80,000 people have been registered as being suspected of fraud offences during the period 2018–2021, according to the Swedish Police's report entitled The deadly frauds, but the number of unreported cases is likely to be even higher. It is quite clear that a functioning flow of information is required between the banks and the Police, to increase the effectiveness of law enforcement.

Another way of recruiting straw men is to first subject the person to an investment scam. The person is manipulated into making an "investment" in the belief that it will yield high returns. The person is first tricked in relation to small amounts, although these often quickly escalate to larger amounts. When the customer exhausts their own funds, they are encouraged to borrow money to invest further. The customer risks ending up in a desperate situation, where they will do anything to get their money back. In the end, the customer risks allowing themselves to be used as a straw man to "save the investment", by receiving and



There are many straw men operating in Sweden.

forwarding money. This money may come from other affected customers, which in the long run can entail money laundering. Cryptocurrencies are often used to move money in phishing and investment scams.

The approaches used are changing

The methods used are constantly being adapted to the conditions. There was an increase in card fraud in 2023, which can be explained by the fact that fraudsters are finding ways of getting around strong customer authentication through card acquirers outside the EU. Other recurring problems include subscription traps, fictitious offers on Facebook and Instagram ad pages, goods that are not received and the existence of many fake websites. In the first few

months of 2024, it appears that the number of instances of card fraud is stabilising.

The strengthened issuing process of Mobilt BankID (through an online check against the Police's id-documents, passports and national id-cards) has resulted in a significant reduction in the number of unauthorised transactions in 2023.

The assessment is that the risks of fraud and financial crime remain high and are rising. The threats are becoming increasingly complex and collaborative, with more and more technical elements in combined approaches in the same criminal scheme.

NEED FOR ACTION

To counter this development, the Swedish Bankers' Association sees a need for several measures and initiatives on the part of politicians and authorities (in addition to the measures the banks can take themselves).

- The legislator should restrict the publication of personal data online. For example, it is currently far too easy to map single elderly people with good finances.
- Telecommunications operators working in Sweden should be required to make it more difficult/impossible to mask telephone numbers through an anti-spoofing infrastructure for phones and text messages, like the one that already exists for phones in Finland as well as the planned proposals for text messages.
- The proposals set out in the ID card inquiry (SOU 2019:14), to reduce the number of issuers of physical id-cards and to improve banks' ability to verify id-documents, should be implemented. The physical id-document connects the physical with the digital in two directions: first when the bank issues the BankID, and then as an extra verification option when the eID is used based on the bank's risk monitoring.
- The Police Authority should provide an API to their RES-system for the banks to use in their identity checks at bank branches, as well as in their role as issuers of e-identification (BankID).
- The banks should also be able to exchange information with each other more easily. A flow of information between the banks and the Police is required to achieve a preventive effect, such as a list of straw men containing information from the Police's money laundering register, for example. The purpose of this is to reduce the straw men's room to manoeuvre.
- The Police should provide information about the known risks and criminal modus operandi that they are aware of and that they want the banks to consider in their transaction monitoring activities.
- The Police Authority should develop solutions for victims of crime to report crimes digitally. Due to current limited opportunities to report crimes to the Police, there is risk of there being many unrecorded crimes, as many victims of crime are forced to call 114 14, where the waiting times can be long.
- The Police needs to ensure a higher level of solving fraud crimes. The number of solved frauds has decreased the last ten years and was around 2.5 percent in 2023. Today, approximately 1 percent of police resources work with fraud even though fraud constitutes more than 16 percent of all reported crime. Analytical police resources should therefore be prioritized for this volume crime.
- The government should develop and implement a national strategy against fraud. The strategy should include various sectors such as banking, telecoms, internet technology, police resources and systems, new legislation, and regulation etc. For example, the Financial Supervisory Authority should publish aggregated statistics on fraud that the banks and others report.



Any proceeds of crime that cannot be converted has, in principle, no value.

Money laundering

In practice, money laundering encompasses a range of different money laundering measures. These may involve transactions between different bank accounts, as well as other actions such as the use of fake documents that represent a value. It is not uncommon for money laundering to be preceded by complex criminal schemes. A person who is guilty of money laundering according to the law is convicted of money laundering offences or commercial money laundering.

As far as the banks are concerned, money laundering normally takes the form of transactions between different bank accounts involving the proceeds of crime. Good due diligence practices and effective, up-to-date monitoring of account transactions are therefore the most important tools enabling the bank to detect and prevent money laundering. The monitoring is performed on an ongoing basis, with the aim of detecting abnormal activities and transactions.

Of all the money laundering detected in Sweden, the vast majority is judged to take place through the regular financial system. It is also conducted through cryptocurrencies, the gambling market, “hawala banking” (an alternative payment system primarily for international money transfers outside the banking sector) and the trade in goods and services. There is an element of uncertainty regarding the statistics, partly as a result of the number of unreported cases when it comes to more complicated criminal practices, for example in the retail sector.

In 2023, a total of 56,136 reports of suspicious activity were submitted to the Financial Intelligence Unit (FIPO), which was a rise of 24 percent compared to 2022 (45,113) and more than twice as many as in 2020, according to FIPO’s statistics. Banks account for the

overwhelming majority of the reports. In total, the financial sector accounted for 90 percent of the reports in 2023, while the gambling sector accounted for 9 percent.

The main money laundering threats

Since money laundering is a broad concept that covers all turnover of the proceeds of crime, the nature of the money laundering issue is largely governed by what type of crime is affecting society at a particular time. Certain types of crime traditionally generate a large amount of proceeds. Any proceeds of crime that cannot be turned over are, in principle, of no value.

Criminals often demonstrate great ingenuity and creativity when it comes to finding new ways of laundering money. This may involve investing the proceeds where there are considerable commercial interests but insufficient controls. There are also unregulated areas, such as cryptocurrencies, where money laundering basically cannot be monitored. Furthermore, the international payment system is sometimes 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 the Swedish authorities, or where the cooperation that exists does not work effectively. Since the banks can only see a certain part of a transaction chain, and only have limited opportunities to exchange information with each other, money laundering of this type is difficult for the banks to detect.

The continuous threat of money laundering persists – it is related to laundering the proceeds of crime from areas such as fraud, narcotics offences and tax offences. As we have seen, this can take place in many differ-

ent ways and it is a challenge to get an overview of the current trends. In terms of amounts, the greatest money laundering threats are associated with organised crime. Organised crime has different conditions for laundering money, with advanced schemes and in a more systematic way, compared to persons who launder smaller amounts occasionally.

The national anti-money laundering regime contains shortcomings, which means that in certain cases the state acts as an enabler for the activities of criminals and money laundering. Many rules are designed according to conditions that are no longer relevant, while existing phenomena are not covered by current regulations.

Furthermore, authorities are not sufficiently adapted to the threats from organised crime, as shown, for example, in poor or non-existent controls, which enables welfare crime.

Money laundering with the aid of companies

In recent years, it has become increasingly common for companies to be used as instruments in the context of organised financial crime. New companies are registered or existing companies are acquired. A straw man is often placed on the company's board of directors. In many cases, the straw man has no knowledge of the company's activities. The company is instead controlled by other individuals who do not want to appear in public and thereby risk being held accountable for the financial crimes committed with the help of the company. The company's operations may be wholly or partially criminal. If this criminal activity only makes up part of an otherwise legitimate business, it is difficult for both banks and the law enforcement authorities to detect.

In order for an outwardly legitimate company to be able to operate, a number of different initial measures need to be implemented. For example, the company's representatives and operations need to be registered with the Swedish Companies Registration Office. It is also generally a prerequisite for a business account to be opened with a Swedish bank and for an accounting consultant to be hired, at least if the criminal activity is to have a certain duration. In such cases, money laundering through a corporate account can be difficult to detect.

Welfare crime

Whenever new grants or subsidies are established, they attract interest from criminals – something that has been clearly demonstrated by the payments of financial subsidies during the Covid pandemic, electricity support as well as various financial subsidies related to environmental promotion measures.

The exploitation of the welfare society by criminals, adding up to very large sums, poses a particular challenge for the banks as the payments are coming from highly trusted senders, i.e. public authorities. It is difficult for a bank to check whether there has been

an underlying crime, where the authorities have been tricked into making payments on incorrect grounds. The recipients also tend to be ordinary people or companies, where there is no reason to suspect that they would not be entitled to receive the money.

The checks must therefore be performed in the first instance by the determining or paying authority. As of 2024, a new authority, the Swedish Payments Agency, has been established. The Swedish Payments Agency is tasked with checking payments from the welfare systems, and is consequently expected to contribute to a reduction in money laundering that has been preceded by welfare crime.

The real estate market and housing associations

The real estate market is attractive when it comes to money laundering, as property can be used in many different ways and requires large investments. This means that a large amount of money obtained from crime can be laundered with a single purchase. The property can then be employed for your own use, rented out or resold. 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 the banks' investigations into suspected money laundering.

There is a risk that, as a result of commercial interests, real estate agents will fail to carry out anti-money laundering-related checks, or will perform such checks without sufficient rigour. In general, there is an interest in property transactions being carried out quickly, which is generally in conflict with the execution of checks. In an increasingly pressurised and competitive real estate sector, it is important not to deviate from the requirement to carry out appropriate checks.

Housing associations are vulnerable to money laundering. Money laundering schemes exist where values can be transferred between different individuals through under- or overvaluation of the item when buying or selling. Mortgages that are granted under false premises can be used to finance these schemes.

Crypto assets, payments and currency exchange

Crypto assets, including cryptocurrencies, are a relatively new sector that is extremely vulnerable to money laundering. The market is global and volatile. Several of the world's largest players are registered in countries with a lack of anti-money laundering regimes or with privacy rules that prevent transparency. Cryptocurrencies are often used as a means of payment by criminals in illegal trading, for example on the Darknet (the non-indexed internet), and in ransomware attacks. Several cryptocurrency exchanges offer the potential to pay using a bank card, which entails a connection between the traditional financial system and the crypto market.

One money laundering risk that has increased in scope is associated with the fact that payments using cryptocurrencies have become an increasingly common means of payment, both in the retail sector and between individuals. With an increased focus on cryptocurrencies, there is also greater risk awareness in relation to receiving them as a means of payment.

Particular high-risk groups are those that provide services related to cryptocurrencies, including payment intermediaries and currency exchangers. These operators are currently not subject to the same extensive rules that apply to banks, and some are still completely unregulated. In many cases, they have poor 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 current risk that is difficult to overlook is the fact that countries and other actors are using cryptocurrencies to circumvent international sanctions. Cryptocurrencies have proven to be useful in replacing globally viable currencies, such as the US dollar.

In the long term, international cooperation with corresponding regulations, definitions and standards can be expected to be crucial when it comes to controlling the crypto market and thereby reducing the risks of money laundering.

Although the turnover of crypto assets is vulnerable to money laundering, it also provides greater opportunities for analysis of the situation as regards the turnover of cash, for example. This is because a large amount of data about transactions involving crypto assets is public on the internet. Analysing this data represents both an opportunity and a growing challenge for stakeholders on the market and law enforcement agencies.


The EU's new Markets in Crypto-Assets Regulation (MiCA) will enter into force in December 2024. Among other things, MiCA aims to facilitate legal certainty for companies and to attract more investments to EU countries. The EU is now becoming the first large scale jurisdiction in the world that is imposing comprehensive regulations on the crypto market. It remains to be seen what effect MiCA will have in practice in relation to the EU's and the global crypto market.

Payment transfers and currency exchange activities carried out professionally or otherwise on a large scale are also vulnerable to money laundering. There are examples of such businesses that are run by criminals. As they make use of the banks' payment infrastructure, they affect the vulnerability in the bank.

Cash

Cash-intensive operations are associated with a high level of risk. Cash is still an attractive means of payment in the illegal economy because traceability is very poor. A large proportion of the trade in drugs and illegal services is paid for in cash. Despite the fact that the use of cash is generally decreasing across the EU, there is an increasing need for banknotes, demonstrating that cash is still an important tool as a value preserver. The banks generally have good control over direct deposits and withdrawals made to the 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 taking action.

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. In the event money laundering is suspected, the banks may need to take measures such as refusing to take cash from certain foreign currency exchangers.



Cash is still an attractive means of payment in the illegal economy since traceability is very poor.

Luxury goods

The market for goods and services in the luxury segment, such as cars, jewellery, watches, gold, designer clothes, travel and hotels, has grown over time. This market attracts criminals, both as an instrument for turning over or laundering money, and as an investment for criminal assets. The payments are often made in cash or using other means with an unclear background. Many of the luxury goods are easy to move between different countries and to resell while retaining their value. In this way, they can be used to transfer values without sufficient traceability.

A common arrangement is to buy a luxury item in cash from a merchant and subsequently return it to the same merchant. The merchant then does not have as much cash available, rather the money is refunded by deposit in a card account (in violation of the card regulations). In this way, cash with a criminal background is able to enter the financial system.

Gambling

The gambling sector entails a high risk of money laundering. Gambling accounts can be used for money laundering purposes in such a way that the

money is stored and mixed together with other funds. This, in turn, means that when withdrawals or transfers are made from the gambling accounts, the money's origins can appear legitimate. The gambling sector also handles cash to a relatively large extent, which, as stated above, is associated with particularly high risks of money laundering.

Gaming companies can be both online-based and traditional casinos at physical addresses. Online-based companies are often located in low-tax countries. Although the market is regulated and subject to the anti-money laundering regulations, there are several unlicensed companies.

The assessment is that as long the criminality that generates financial proceeds continues to take place at a high level in society, the risk level as regards money laundering remains high. The banks are constantly trying to limit their risks, primarily through good Know Your Customer (KYC) procedures and appropriate transaction monitoring.

NEED FOR ACTION

Due to the developments taking place in the field of money laundering, the Swedish Bankers' Association sees a need for a number of measures and initiatives on the part of 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.
- Organised crime takes advantage of the fact that banks are unable to share information between themselves. When criminals are discovered in one bank, they immediately change to another bank and continue their criminal activities there. As a result, in order for the measures to combat money laundering and terrorist financing to be effective, the banks need to be better able to share information about suspicious customers, transactions and activities with each other.
- The new rules regarding cooperation and the exchange 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 thereby achieve results.
- 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 it being exploited by organised crime. This applies, for example, to the Swedish Companies Registration Office's register of representatives and beneficial owners of legal entities, as well as other registers that the Office maintains.
- Measures need to be implemented to limit the occurrence of enablers. For example, this may include the Swedish Companies Registration Office tightening its controls, conditions being made more difficult for business intermediaries when it comes to transferring companies to criminals, or criminals not being given access to accounting services.
- The police's Financial Affairs Department needs to have sufficient resources to rapidly handle and provide feedback on all suspicious transaction reports submitted by the actors covered by the AML framework. If decisions to freeze assets are not taken promptly, there is a risk that criminal money will be transferred beyond the control of banks and authorities.



Crypto currencies are attractive for terrorist financing.

Terrorist financing

A key risk factor in relation to terrorist financing is the fact that the banks do not have access to sufficient information about how such financing takes place, nor about the identity of the individuals and companies involved. A lack of information about what the banks should be reacting to and looking out for makes it difficult to detect suspected terrorist financing.

In recent years, the number of cases of suspected terrorist financing via cryptocurrencies has increased. Such currencies are attractive for terrorist financing, in part due to the absence of uniform and universal regulation and supervision of the crypto industry.

Certain more extensive and complex criminal schemes, including international tax crime (e.g. VAT carousels, which have affected Sweden to a significant extent in recent years), require considerable organisation and large initial investments. These investments frequently amount to tens or hundreds of millions of kronor. Criminal investments on this scale may derive from international criminal networks, which in turn may be suspected of having links to terrorism and its financing. The proceeds of crime go back to the international criminal networks abroad in various ways and are

consequently difficult to trace. As far as the banks are concerned, the risks are difficult to detect, partly because the turnover normally appears legitimate and the paying body in this case is the Swedish Tax Agency.

Another risk factor in relation to terrorist financing is crowdfunding. This is a form of investment in which a large group of individuals with small sums finances a business or project. Crowdfunding platforms enable private individuals to launch various types of online fundraising on an international level. For the bank, it is very difficult to distinguish legitimate fundraising activities from those that take place with the underlying intention of financing terrorism. For obvious reasons, this purpose is not apparent to the outside world.

The assessment is that increased information sharing and information relating to modus operandi for terrorist financing can limit the banks' risk of participating in transactions constituting such financing.

International sanctions

International sanctions – or restrictive measures – are part of the EU’s Common Foreign and Security Policy. With an increased 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 sanctioned party, in line with a particular agenda on the part of the party imposing the sanctions. For example, this may relate to human rights or peacekeeping purposes. Sanctions are directed at governments or state apparatuses, an identified group/organisation, individuals or companies. This, in turn, can lead to the sanctions giving rise to changes at a political or state level. Sanctions are an alternative to more intrusive measures, i.e. if the sanctions do not have the desired effect.

Sanctions are issued by a number of different countries. Important international actors are the UN, the EU, the United States and the United Kingdom. Sweden does not currently issue its own sanctions, but 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, in order to avoid serious commercial risks and, in the long run, risks to Swedish society’s need for functioning banking operations.

Sanctions may be targeted at:

- governments of non-EU countries
- entities (companies) providing funds for the policies being targeted by the sanctions
- groups or organisations, such as terrorist groups
- individuals who support the policies being targeted by the sanctions, who are involved in terrorist activities, etc.

At times, sanctions do not only cover listed entities, but also other entities related to the listed entities. This may mean that ownership structures and informal structures for the control of a sanctioned entity need to be analysed in order to comply with the sanctions. Furthermore, sanctions may be aimed at a certain type of product or service that is legitimate in itself, but which the sanctioned party may use for undesirable purposes in order to strengthen their capabilities or finances.



Sanctions have become an increasingly important means of exerting pressure on foreign policy.

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

In recent years, sanctions have become increasingly difficult to comprehend and apply in a uniform and effective manner for the many operators that have to comply with the sanctions. It is not only the banks that need to comply with the sanctions. For example, the entire industrial sector needs to be constantly vigilant in order not to risk violating sanctions.

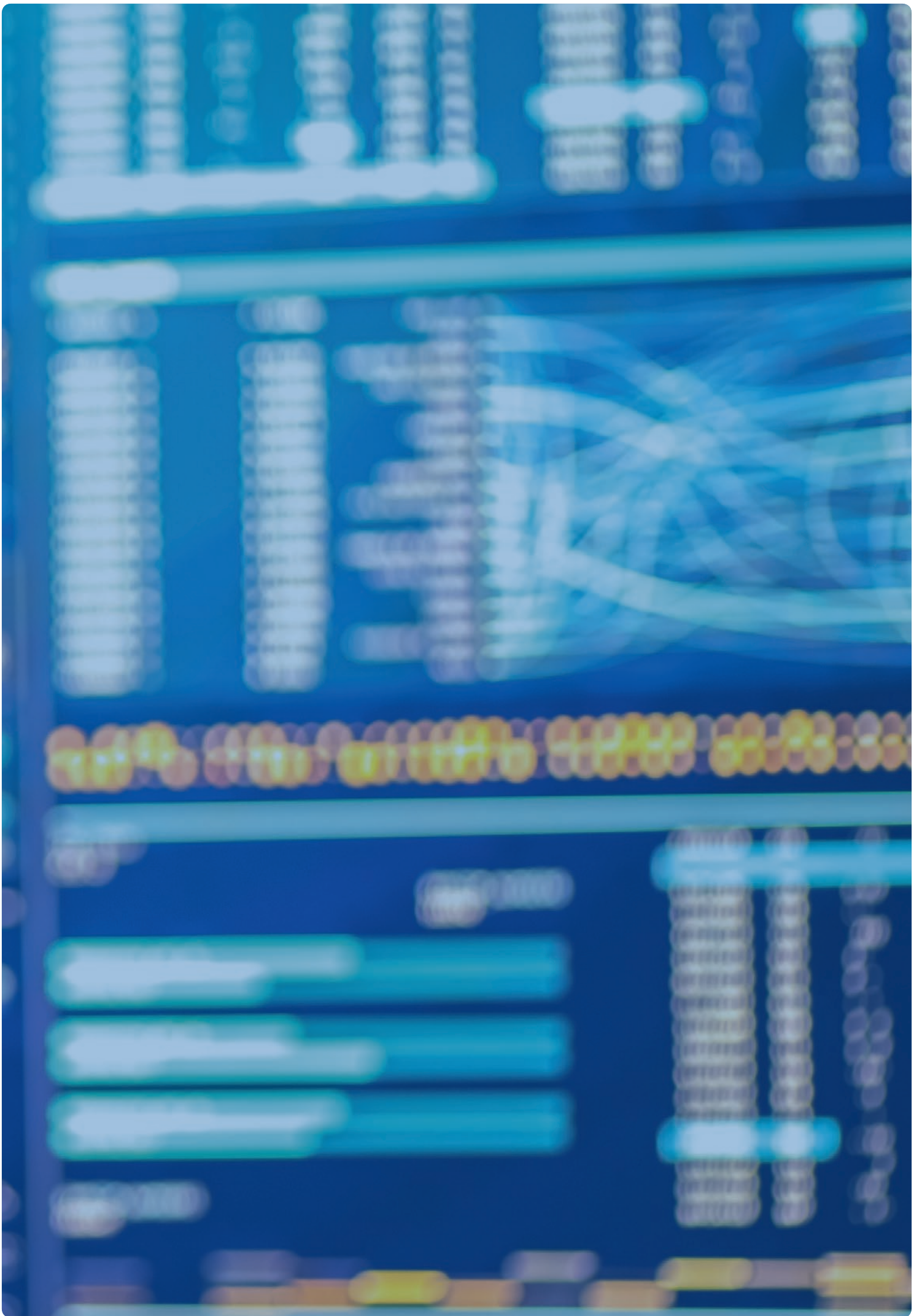
Since Russia's annexation of the Crimean Peninsula in 2014 and the invasion of Ukraine in 2022, the EU has been imposing an unprecedented amount of sanctions on Russian interests. The sanctions are intended, in various ways, to limit Russia's capabilities and to stress that the country's behaviour is unacceptable. The sanctions include travel bans, the freezing of significant Russian assets and an oil price cap on Russian oil exports. By the end of 2023, the EU had decided on a total of twelve packages of sanctions against Russia. Further expansions of the sanctions imposed on Russia are anticipated in 2024.

At the same time, there has been an increase in large-scale, systematic evasion and circumvention of the sanctions by Russia. With the help of foreign interests, Russian actors have found ways, for example, to import advanced technology that can be used in the war industry or to receive the market price for oil. By changing the names of companies, falsifying documents, front men, etc., attempts are being made to conceal who actually owns or controls companies. The sanctions imposed on Russia are now largely aimed at trying to deal with evasion and circumvention, and this is likely to remain a priority within the EU in 2024.

Collaboration in the field of sanctions

Large-scale and systematic sanction violations are placing increased demands on both operators and authorities within the EU. Having an awareness and an understanding of the problem is fundamental. Increasingly extensive sanctions and an increasingly complex and risky situation are posing major challenges when it comes to collaboration in respect of sanctions. Without the support of the relevant authorities and a dialogue between the actors in the field of sanctions, for example, it is difficult for operators to understand their risk exposure and obtain the necessary information in order to apply the sanctions appropriately and effectively, so as to achieve the political objectives.

The assessment is that an increased conflict landscape and ever greater geopolitical tensions in various parts of the world are leading to increasingly extensive and complex sanctions. This is placing increased demands on banks and other operators. In order for the sanctions to be applied effectively, to achieve their objectives and to combat sanction violations, it is necessary to achieve increased collaboration and dialogue between the different actors in respect of sanctions.





Design and graphic production: www.luxlucid.com Stockholm, May 2024



Svenska
Bankföreningen
Swedish Bankers' Association

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