National risk assessment 2023/2024 – Neobanks

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

Published by: The Swedish Police Authority
Registration number: A340.719/2024
Version: Revised version, May 2024
Printed: Police printing house Stockholm, September 2024
Graphic form: Blomquist Communication, blomquist.se

Summary

This is the fourth report from the coordination function on the risk assessment for money laundering and terrorist financing in Sweden. The scope of this report is limited to digital financial services (DFS) with a specific focus on services offered by neobanks. The 2023/2024 risk assessment aims to identify the potential threats, vulnerabilities and risks that digital financial services offered by neobanks may pose for the fight against money laundering or terrorist financing.

The term neobank has been used since at least the mid-2010s to describe fintech companies that use innovative features, high money mobility and rapid implementation of new technology to challenge traditional banks. In this report, the term neobank is used to refer to any business that offers services and products that are similar to traditional banks, but which primarily has a digital presence on the internet and which offers its services via apps and websites. Neobanks aimed at businesses often also offer accounting and invoicing services. Neobanks are also able to offer competitive prices due to, for example, lower fees. As a result, neobanks have become an attractive alternative on the financial market and the number of neobanks has grown at an increasing rate in recent years. At the end of 2023, there were approximately 30 operators under the supervision of the Swedish Financial Supervisory Authority that fit the above description of a neobank.

Neobanks can potentially be used for money laundering and terrorist financing because the services that some neobanks offer provide some degree of anonymity due to the ability to avoid stringent checks, which makes these businesses attractive to criminal actors. Neobanks have appeared in the Swedish Economic Crime Authority's preliminary investigations, where the ability to remain anonymous while utilising services means that neobanks are used for many transactions, often involving large sums of money. This often involves money laundering of criminal proceeds from tax offences and the payment of wages for "black labour" (illegal labour) and, according to the Swedish Tax Agency's tax investigations, as a way to hide income to avoid taxation. The Swedish Security Service also notes that neobanks appear to an increasing extent in its operations.

Threats and vulnerabilities are assessed on a four-point scale (1–4 where 4 is the highest). The risk of money laundering and terrorist financing is assessed by weighing threats and vulnerabilities, also on a four-point scale (1–4). The threat of money laundering and terrorist financing for neobanks is assessed as high (4). Vulnerability is assessed as significant (3), the second highest level. The above assessments are based on a number of identified threats and vulnerabilities, for example, the large number of parties and jurisdictions involved in transactions; impediments to the traceability of transactions; the lack of physical meetings in connection with the identity verification and customer due diligence process; and the ability to hide the identity of the true account holder, sender and recipient through, for example, the use of account gatekeepers.

Based on the identified threats and vulnerabilities, the risk for neobanks is also assessed to be significant (3). The fact that neobanks offer certain services that can be used for money laundering and terrorist financing erodes confidence in the financial system in general and neobanks in particular. Other consequences are that it is more difficult to detect and prosecute money laundering and terrorist financing in the sector, which in turn can lead to lower rates of prosecution and obstacles to tax investigations, which can ultimately lead to reduced tax revenues if taxation cannot be carried out correctly. The ultimate consequence of terrorist financing is the ability of actors to successfully carry out terrorist acts.

This report concludes with a number of recommendations, including the need for greater knowledge regarding neobanks and the risks they present, but also a number of recommendations on improved information exchange and reporting to the Financial Intelligence Unit and the Swedish Tax Agency, improved customer due diligence processes and the expansion of the reporting requirement for client funds accounts.


L250.50
Cryptocurrency Price
Since last week

Contents

Summary 3

1. Introduction 6
- 1.1 Purpose and goals 6
- 1.2 The coordination function 6
- 1.3 Boundaries 7
- 1.4 Method 7
- 1.5 Target group 7
- 1.6 Regulations 7

2. Neobanks 8
- 2.1 What is a neobank? 8
- 2.2 How does an individual become a customer of a neobank? 9
- 2.3 Products and services 10
- 2.4 Virtual IBAN 11
- 2.5 White labelling 12

3. The prevalence of neobanks in investigations 13

4. Legal regulations 16
- 4.1 Businesses authorised by the Swedish Financial Supervisory Authority 16
- 4.2 Companies with authorisation from foreign supervisory authorities within the EEA 18
- 4.3 Money laundering regulations and the Swedish Financial Supervisory Authority's money laundering supervision 19
- 4.4 EBA guidelines 20
- 4.5 Reporting to the Financial Intelligence Unit of Sweden 20

5. Risk assessment and impact assessment 21
- 5.1 Definitions of threats, vulnerabilities and consequences 21
- 5.2 Starting points for assessments 22
- 5.3 Threat and risk assessment for the banking sector from NRA 2020/2021 22
- 5.4 Threats linked to neobanks 23
- 5.5 The vulnerabilities of neobanks 24
- 5.6 Risk assessment and impact assessment 30

6. Recommendations 32

1. Introduction

This is the fourth report from the coordination function on the risk assessment for money laundering and terrorist financing in Sweden. The report covers digital financial services and is limited to neobanks, the services and products they offer, and the associated risks and consequences of money laundering and terrorist financing.

It is important to take a risk-based approach in the work to combat money laundering and terrorist financing in order to achieve an effective, resource-efficient regime where different parts of society work together. In Sweden, actors from a variety of segments are affected, with supervisory authorities, law enforcement agencies and operators (private actors) being the most relevant. The fight against money laundering and terrorist financing does not occur exclusively within national borders; it is a global effort that includes cooperation within the Financial Action Task Force (FATF), and at EU level, through legislation, guidelines and recommendations.

Under the Money Laundering and the Financing of Terrorism (Prevention) Act (2009:62), the coordination function shall work to continuously identify, map and analyse risks and methods for money laundering and terrorist financing in Sweden. In addition, the coordination function shall compile (annually or in response to new risks or changes in the risk profile), update and publish national risk assessments for money laundering and the financing of terrorism to the necessary extent.

1.1 Purpose and goals

The area "banking or financing activities" was included in the 2020/2021 national risk assessment.[1] Although neobanks are not specifically mentioned in the previous risk assessment, the assessment is that they are part of the same sector because they conduct bank-like activities. In the previous risk assessment, for example, the ability of actors to remain anonymous was identified as a risk linked to banking or financing activities, for example, through the use of gatekeepers, straw men or false documentation. Another risk identified in the sector was the ability of criminal actors to quickly carry out transactions by using several different products. The significant risks that were highlighted in that report revealed the need for a deeper understanding of neobanks and the associated risks.

The national risk assessment for 2023/2024 aims to identify potential threats, vulnerabilities and risks associated with the digital products and financial services offered by neobanks. The goal of the 2023/2024 risk assessment is to develop recommendations for risk management based on the identified threats, vulnerabilities and risks.

1.2 The coordination function

Within the Swedish Police Authority, there must be a coordination function that works to address money laundering and terrorist financing.[2] The coordination function consists of the following 16 authorities: The Swedish Companies Registration

1 Report, The coordination function (2021). "National risk assessment of money laundering and terrorist financing in Sweden 2020/2021".

2 The Money Laundering and the Financing of Terrorism (Prevention) Act (2009:92), shortened to the Anti-Money Laundering Act.

Office, the Swedish National Council for Crime Prevention, the Swedish Economic Crime Authority, the Swedish Estate Agents Inspectorate, Swedish Financial Supervisory Authority, the Swedish Enforcement Authority, the County Administrative Board of Skåne, the County Administrative Board of Stockholm, the County Administrative Board of Västra Götaland, the Swedish Police Authority, the Swedish Inspectorate of Auditors, the Swedish Tax Agency, the Swedish Gambling Authority, the Swedish Security Service, Swedish Customs and the Swedish Prosecution Authority. The risk assessment is the result of a joint effort between the members of the function.

The work to compile this year's risk assessment has mainly been carried out in a small project group consisting of members from the Swedish Police Authority through the Financial Intelligence Unit, the Swedish Financial Supervisory Authority, the Swedish Economic Crime Authority, the Swedish Tax Agency and the Swedish National Council for Crime Prevention.

1.3 Boundaries

This report is limited to neobanks, their structure and the services they offer. There is no clear or legal definition of a neobank. In this risk assessment, the term neobank is used to refer to any business that conducts banking or bank-like activities, but which primarily has a digital presence on the internet and which offers its services via apps and websites. Unlike traditional banks, a neobank typically has no physical branches.

The businesses included in the definition of a neobank do not necessarily need to have authorisation to conduct banking activities but can include payment institutions or electronic money institutions (below referred to as e-money institutions). The defining characteristic for inclusion in the definition is instead the products and services the business offers, which are often very similar to the products and services offered by traditional banking operations, regardless of the type of authorisation.

1.4 Method

This national risk assessment was based on FATF's method for the risk assessment of the threat of money laundering and terrorist financing.[3] The report is based on quantitative data and qualitative reasoning based on the expert knowledge of the participating authorities.

1.5 Target group

The intended recipients of this risk assessment are mainly the Government Offices, members of the coordination function and operators who are directly and indirectly covered by this risk assessment.

1.6 Regulations

Money laundering and terrorist financing are regulated in both administrative and penal legislation. The administrative regulatory framework, the Money Laundering and the Financing of Terrorism (Prevention) Act (2017:630), is central and aims to prevent and combat the use of financial activities and other business activities for the purposes of money laundering and the financing of terrorism. The penal framework aims to prosecute individuals who engage in money laundering or terrorist financing and is mainly embodied in the Act on Penalties for Money Laundering Offences (2014:307) and the Terrorist Offences Act (2022:666).

3 See the FATF's website for more information, fatf-gafi.org

2. Neobanks

2.1 What is a neobank?

The term neobank has been used since at least the mid-2010s to describe fintech companies that use innovative features, money mobility and rapid implementation of new technology to challenge traditional banks. In order to respond to their customers' needs and preferences, neobanks often introduce new functions, products and services at a much faster rate than traditional banks. As neobanks have lower costs associated with physical infrastructure (e.g. no physical branches), they can often also offer competitive prices (e.g. lower fees). As a result, neobanks have become an attractive alternative on the financial market, and the number of neobanks has grown at an increasing rate in recent years.

In order to start a neobank domiciled in Sweden, operators need to obtain authorisation from the Swedish Financial Supervisory Authority. Neobanks are also obliged to comply with financial regulations. They are obliged to protect customer data, comply with anti-money laundering regulations and maintain robust measures to ensure the security of transactions and customer information.

Only institutions with authorisation to conduct banking activities may call themselves "bank", but as there is no legal definition of a neobank, actors without authorisation to conduct banking activities may also use the term neobank. One difference is that a "bank" must be connected to at least one payment system, either via clearing systems such as Bankgirot or via card systems such as Visa and Mastercard. At the same time, it is possible for a business without authorisation to conduct banking activities to cooperate with a business that has this authorisation and to use this as a strategy to offer additional services.

According to the Swedish Financial Supervisory Authority's assessment, at the end of 2023, there were approximately 30 banks, payment institutions and e-money institutions that could be considered Swedish neobanks based on the definition used in this report. These 30 neobanks have authorisation from the Swedish Financial Supervisory Authority and are under the authority's supervision. However, Swedish consumers can be customers of foreign neobanks that seek authorisation from another EU country to be able to offer their products and services on the European market. European neobanks that are registered in other countries, but are active in Sweden, are not under the supervision of the Swedish Financial Supervisory Authority.

Based on the definition of neobanks used in this report, the 30 neobanks above include the following types of operations.

1. **Neobanks with authorisation to conduct banking activities,** which have been started as fully digital banks and have thus never had any physical branches. This type of neobank usually offers a wide range of products and services and is often very similar to a traditional bank in the products and services it offers.

2. **Neobanks that are considered a payment institution,** which, for example, offer payment cards and enable deposits and withdrawals using the card through an interface within the framework of the neobank's authorisation. In the event that a neobank also wants to provide credit or savings products, this can be done through a cooperation agreement with a bank that holds the necessary authorisation through a "white labelling" arrangement.

3. **Neobanks that are considered e-money institutions,** which are often aimed at business customers both within and outside of Sweden. In addition to issuing electronic money, neobanks in this category may provide payment transactions through credit, business accounts, payment cards and invoicing services.

2.2 How does an individual become a customer of a neobank?

Neobanks are often characterised by a high degree of technological innovation, which enables a rapid onboarding process.[4] One difference between traditional banks and neobanks is how quickly a new customer can open an account, even though operators in both categories are obliged to follow the same regulations regarding the customer due diligence process.[5]

Becoming a customer and using accounts in neobanks is usually a simple two-step process. The first step is to register as a customer, which is often a quick process that only requires a mobile number or an email address. Speed and convenience are often highlighted as a competitive advantage. The second step is the verification of the customer's information. In this step, the customer usually sends a digital copy of an identity document and a photo. Some neobanks do not use the two-step process; identification is done exclusively through e-identification. In both cases, there is no physical meeting in the process between the neobank and the customer. A traditional bank has the option of calling the customer in for an in-person customer meeting to verify the customer's information. Neobanks are not set up to engage in this kind of process, as they generally do not have physical branches.

For business customers, the onboarding process varies significantly between operators. In its simplest form, representatives of the company are only required to have an email address in order to become a customer of a neobank. Experience from supervision and other information from authorities have shown that there are also neobanks that use processes for potential business customers that include the identification of signatories, verification of the beneficial owner and checks of company information against external registers.

4 The onboarding process is the customer verification procedure for a bank or other financial institution.

5 The customer due diligence process is the process operators use to identify their customers and assess their risk profile. The Money Laundering and the Financing of Terrorism (Prevention) Act (2017:630) sets requirements for such a process.

2.3 Products and services

A neobank's products and services are only offered digitally. Accounts, payment cards and credit are some of the most common services offered by many neobanks. Neobanks often offer both physical and virtual payment cards. Virtual payment cards work like physical payment cards, but the card details are only available digitally. Virtual payment cards can be made available to a customer immediately after registration, but before the information provided by the customer has been verified by the operator. Some neobanks also allow customers to immediately open accounts without, for example, income requirements, as well as access to payment services before the customer's information has been verified.

Other services offered by neobanks include investment advisory services, financial overview, various options to invest in stocks or precious metals, currency exchange and management of cryptocurrencies. Several neobanks started as cryptocurrency trading platforms and offer their customers cryptocurrency wallets, where they can link payment cards to their cryptocurrency wallets. Often, customers can also move cryptocurrencies within the neobank and to and from external wallets.

Some neobanks offer additional services, for example, joint payment accounts with multiple account holders. This allows account holders to use payment cards linked to the account, divide and distribute payments and make rapid transfers to other accounts in the same neobank. Transfers can be carried out quickly, for example, by scanning QR codes or by entering the recipient's email address or a username. Some neobanks also allow their customers to connect their payment cards to various payment solutions such as Google Pay or Apple Pay. The services and other products offered by neobanks are described in more detail in the Financial Intelligence Unit's report on neobanks.[6]

For some neobanks, services that they are not able to offer themselves (e.g. due to limitations in the authorisations they hold) can be offered through cooperation agreements with other providers through "white labelling" arrangements (see section 2.5 on white labelling). For example, payment institutions are not authorised to offer deposits through savings accounts within the framework of the authorisation granted by the Swedish Financial Supervisory Authority in accordance with the Payment Services Act. Instead, these operators can offer savings products through a cooperation agreement with a bank, to which the payment institution can refer savings customers. Other examples are cases where external parties provide payment cards or cryptocurrency wallets.

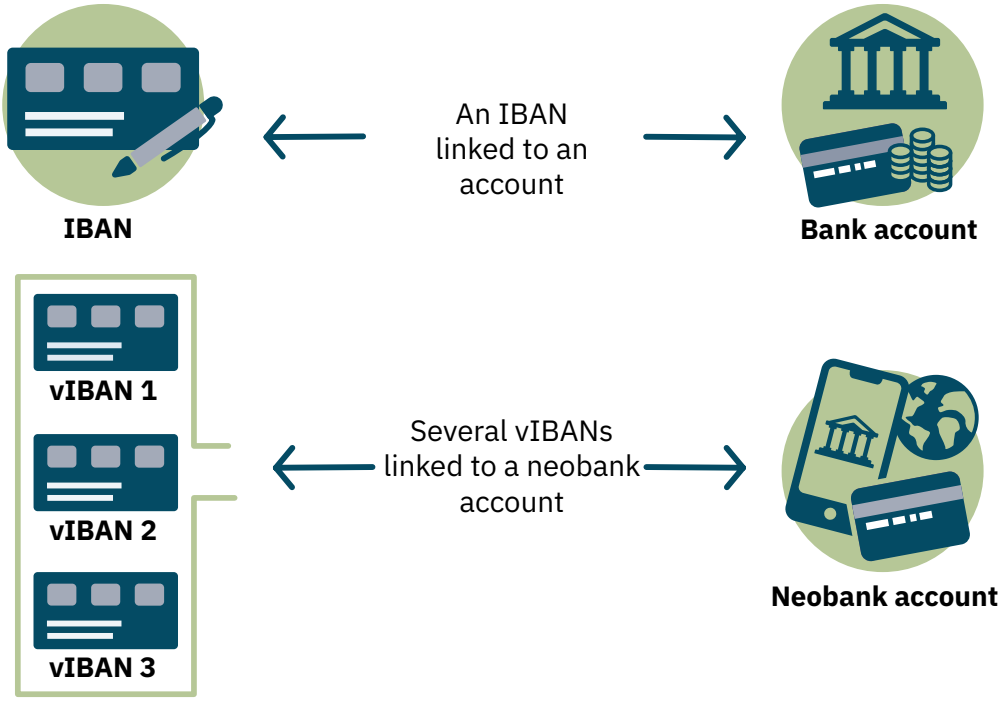
As business customers are an attractive segment, a number of neobanks provide solutions specifically targeted to businesses. The number of neobanks that exclusively target business customers is growing rapidly. There are some Swedish neobanks that fit this description, but also some foreign neobanks that are both established in Sweden and specifically target the Swedish market. The difference between neobanks that primarily target business clients and neobanks that target private individuals is mainly reflected in the payment volumes of the transactions that business customers carry out and the amount of credit offered to business customers compared to private individuals. Another difference is that business customers are offered additional services, such as bookkeeping, invoicing services and virtual IBAN.

6 Report, Financial Intelligence Unit (2022) Neobanker (Neobanks).

2.4 Virtual IBAN

The International Bank Account Number (IBAN) is a global standard for identifying bank accounts and is mainly used for international payments. Neobanks often create virtual bank accounts for its customers. Virtual IBAN (below referred to as vIBAN) is an identification system that assigns these virtual bank accounts a unique IBAN code. vIBAN is used as an identifier for the virtual bank account and facilitates the execution of transactions. One important difference between traditional IBANs and vIBANs is that each individual IBAN is usually matched with only one bank account, which means that there is only one bank account linked to each individual IBAN number. In the case of vIBAN, on the other hand, several numbers are normally linked to the same bank account (Figure 1). This type of account is described in more detail in Section 5.5.6.

Figure 1. IBAN and vIBAN and how these are linked to different accounts.



2.5 White labelling

"White labelling" is common practice in many different sectors and means that companies purchase and market products that have already been developed as their own, under their own brand and according to their own terms and conditions. In the financial services sector, it is typically used by financial institutions, where the banks' APIs[7] are used to develop their own platforms for financial services and products, using the existing infrastructure of the licensed banks. This practice is particularly common among fintech companies and neobanks that are not authorised to conduct banking activities in their own operations.

Neobanks that are not authorised to conduct banking activities and are structured as "white label" banks therefore seek cooperation agreements with established banks with the necessary authorisation, which then assist with the regulatory and legal aspects of the collaboration. These neobanks, which are often payment institutions or e-money institutions, are able to use this strategy to offer products that fall outside the scope of their own authorisation.

Through the authority's experience in supervision, the Swedish Financial Supervisory Authority has noted that it is becoming increasingly common for financial services companies to use this type of collaborative arrangement to offer their customers products that the company does not have authorisation to provide. Through cooperation agreements with established banks, these neobanks can offer, for example, savings products under their own brand, which according to Swedish legislation can only be offered by banks with authorisation to conduct banking activities. In the neobank's marketing, it is often not obvious to the target customer group that it is actually another bank that the customer will enter into an agreement with. Another example is where a company that does not have authorisation to offer credit brokerage services enters into a cooperation agreement with a lender and provides its platform for credit brokerage services.

Depending on how the cooperation agreement is structured, the parties can, for example, agree to carry out parts of the customer due diligence processes or credit assessment processes on behalf of the other party. In terms of money laundering, these arrangements raise questions about risk ownership and the division of responsibilities in the customer due diligence process and transaction monitoring, in that cooperation agreements and the intermediation of bank-like services are not currently specifically regulated under Swedish law.

7 According to the Swedish Tax Agency's definition: The abbreviation API stands for Application Program Interface. API is a now standardized way of transmitting information that we use on a daily basis, perhaps often without even being aware that we are using it. For example, APIs are used in our mobile apps to provide everything from weather forecasts to exercise schedules, or to provide accounting systems with balances from a bank.

3. The prevalence of neobanks in investigations

Neobanks appear in the Swedish Economic Crime Authority's preliminary investigations. Of course, neobanks with a large number of customers appear in the preliminary investigations to a greater extent, but smaller neobanks also appear in these investigations. The neobanks cited in the preliminary investigations are also registered in a number of different countries, both in Sweden and abroad. However, the neobanks that appear in Swedish investigations are predominantly foreign neobanks. Several investigations and reports have shown that criminals in organised crime often use businesses as tools to commit financial crimes and launder money.[8] Neobanks that directly target businesses also appear relatively frequently in the preliminary investigations.

Neobanks appear in the preliminary investigations in the same way as traditional banks, that is, people and companies have accounts through which they send and receive money. The investigations show that neobanks are used in money laundering schemes where criminal proceeds are transferred to accounts in neobanks, either directly, via regular bank accounts, or by using various payment platforms. The criminal proceeds are then transferred to accounts in the neobank that are either held by the principals behind the criminal scheme or by other persons. These schemes often involve a large number of transactions and large sums of money, and neobanks are often used in the first step in the money laundering process. The criminal proceeds can then be used or invested. Many neobanks also act as a cryptocurrency exchange, which provides additional opportunities to conceal the origins of criminal proceeds.

The approaches used to launder criminal proceeds change and develop as new payment solutions emerge, and new players enter the market. The Financial Intelligence Unit of Sweden's analyses show that criminal actors frequently use neobanks,[9] for example, to vary their money laundering schemes, layer money and spread out their assets.

In tax investigations and tax crime investigations, the Swedish Tax Agency has highlighted the fact that neobanks are used in connection with tax evasion. The construction and trade industries regularly appear in the investigations. In these cases, the tax evasion schemes take many different forms, but what they all have in common is that one or more neobank accounts have been used in the criminal scheme. One example is that employees from other EU countries or third countries are employed by foreign subcontractors operating in Sweden, but do not report that they are operating in Sweden. This means that the companies are unknown to the Swedish authorities. In the first step, compensation for "black labour" has been paid to the

8 The Swedish National Council for Crime Prevention 2015:22 *Penningtvätt och annan penninghantering. Kriminella, svarta och grumliga pengar i legal ekonomi* (Money laundering and other money management – Criminal money, black money and murky money in the legal economy); The Swedish National Council for Crime Prevention 2016:10 *Kriminell infiltration av företag* (Criminal infiltration of companies); The Swedish National Council for Crime Prevention 2019:17 *Penningtvättsbrott. En uppföljning av lagens tillämpning,* (Money laundering. A follow-up of the application of the law); SOU 2023:34 *Bolag och brott– några åtgärder mot oseriösa företag* (SOU 2023:34 Companies and crime – measures to prevent rogue companies).

9 Report, Financial Intelligence Unit of Sweden (2021) *Financial Intelligence Unit of Sweden's 2021 annual report.*

foreign subcontractor who has then transferred the salary to the employees' neobank accounts, without paying the required fees (tax evasion).

There are also examples where individuals with unlimited tax liability[10] in Sweden have had salaries from foreign employers deposited into accounts in foreign neobanks. This occurs without a statement of earnings being submitted to the Swedish Tax Agency.

In these cases, there is a high risk that salaries and other compensation will not be taxed correctly. In the case of a tax investigation, for example, a Swedish person who has emigrated and is resident in another EU country has received payment from a Swedish company for consultancy work. Payment for the services has been deposited directly into an account held with a foreign neobank, and the amounts have not been reported in the person's income statement in Sweden. Within the OECD and the EU, there are regulations on the automatic exchange of data (CRS data and DAC2 data) on financial accounts for tax purposes between the tax authorities in different countries.[11] Within the framework of CRS and DAC2 regulations, financial institutions in different countries must report on the accounts held by persons and companies with their tax domicile in another country. The Swedish Tax Agency has highlighted the fact that some countries do not classify neobanks as financial institutions that are obliged to report financial accounts, which means that the purpose of the regulations is undermined. There are therefore multiple risks: first, the risk of tax evasion, and second, the risk that money laundering will not be detected by the Swedish Tax Agency.

The Swedish Security Service's assessment is that the occurrence of neobanks is increasing among the individuals who appear in the agency's intelligence activities. The ability to remain anonymous due to less stringent checks and the opportunity to make funds immediately available are important factors in the increasing use of neobanks. One concrete example is the case of a person suspected of planning a terrorist attack, who used a large international neobank to send money to people in other countries. This individual deposited money into their account, and other people were able to make withdrawals from the account in other countries, both through card purchases and cash withdrawals. In this case, it was a high-risk country in which most Swedish banks do not carry out transactions. The money was reportedly being provided for travel, but also for food and living expenses for individuals involved in the planning of terrorist attacks.

In the experience of the Swedish Financial Supervisory Authority in its supervision of institutions which, like neobanks, are driven by technological development and which are associated with similar risks, these institutions have relied on inadequate customer due diligence measures. These measures have been assessed to be inadequate given the increased inherent risk of money laundering and terrorist financing that these operations can be connected with.

The reliance on inadequate customer due diligence measures, combined with the flexibility and agility of digital banking services, which allow multiple transactions to be carried out every day, leads to increased risks for both money laundering and terrorist financing, as well as for other types of crime, such as fraud.

10 For natural persons, Ch. 3., Section 3 of the Swedish Income Tax Act sets out three independent criteria for unlimited tax liability in Sweden. These criteria are: resident in Sweden, domiciled (resident) in Sweden and substantial connection to Sweden. Unlimited tax liability means that individuals are obliged to pay tax in Sweden for all income in Sweden and all income from abroad. However, there are exceptions to tax liability both in domestic law (e.g. the six-month rule) and in international tax agreements.

11 CRS stands for Common Reporting Standard and is the OECD's reporting standard for the exchange of information. DAC2 is the EU equivalent.

In the Swedish National Council for Crime Prevention's report on fraud, it is emphasized that the digital banking and payment market enables fraud. Digital banking transactions, which are usually not monitored by bank staff, can create favourable conditions for several types of fraud. In order to increase consumer protection, in October 2023, the Swedish Financial Supervisory Authority was directed by the government to review the measures payment service providers use to prevent fraud.[12] The Swedish Financial Supervisory Authority is particularly concerned about recent trends in the incidence of fraud in the payment market, where social manipulation is being used to deceive crime victims and large sums of money are entering the criminal economy.

While the emergence of a digital banking and payment market has contributed to convenient and fast payment solutions, it has also created new ways for criminals to commit fraud and quickly launder and conceal criminal proceeds. Fraud affects many people and has increased over time. In 2022, roughly 180,000 fraud cases were reported to the police, which can be compared to approximately 50,000 reports in 2000[13] with criminal proceeds of approximately SEK 5.8 billion in 2022 according to estimates. Fraud is considered to be one of the most profitable crimes for individuals and groups within organized criminal environments,[14] and criminal proceeds from fraud contribute to the financial strength of criminal networks and can be reinvested in other types of crime. Criminal proceeds are considered to be a strategic resource for the different criminal networks that participate in these crimes.

12 The Government's assignment to the Swedish Financial Supervisory Authority to counter fraud, FI2023:02625.

13 Report, Swedish National Council for Crime Prevention (2023) *Bedrägerier mot privatpersoner* (Fraud against private individuals).

14 Report, Swedish Police Authority (2021) *De dödliga bedrägerierna* (Deadly fraud).

4. Legal regulations

4.1 Businesses authorised by the Swedish Financial Supervisory Authority

In order to be allowed to operate a business that offers financial services, operators generally need to obtain authorisation from the Swedish Financial Supervisory Authority. Companies that receive authorisation fall under the supervision of the Swedish Financial Supervisory Authority. The Swedish Financial Supervisory Authority's supervision activities are based on an assessment of the risk profile in various businesses and how significant the negative consequences would be for society or consumers if the identified risks are realized. The specific requirements that are imposed on specific businesses and what the supervisory activities of the Swedish Financial Supervisory Authority entail are regulated in the various business laws, which are rules for specific types of business. In addition, in principle all companies that are granted authorisation are subject to the Swedish Financial Supervisory Authority's money laundering supervision activities in accordance with the Money Laundering and the Financing of Terrorism (Prevention) Act (2017:630). Below we provide an account of the authorisations issued by the Swedish Financial Supervisory Authority which are associated with neobanks.

4.1.1 Banking and financing activities

Any company that wishes to carry out banking or financing activities will have its application examined in accordance with the provisions of the Banking and Financing Business Act (2004:297) and the Banking and Financing Business Ordinance (2004:329). Banking refers to an activity that provides payment intermediation through payment systems and the receipt of funds that, after termination, are available to the creditor within a maximum of 30 days. The term financing activities refers to activities whose purpose is to receive repayable funds from the public and provide credit, provide a guarantee for credit or, for financing purposes, acquire receivables or make movable property available for use (leasing). In addition to the rules set out in the Anti-Money Laundering Act, banks and credit market companies also have a number of obligations, including requirements related to capital requirements, capital base requirements and consumer protection obligations.

4.1.2 Payment Services

Companies that provide payment services must, as a general rule, be authorised to offer these services in accordance with the Payment Services Directive (2010:751). Chapter 1, Section 2 of the act lists the eight different payment services that a financial company can be authorised to provide. A company can provide several different payment services simultaneously but must apply for separate authorisation for each of the activities. Similar to banks and credit market companies, payment institutions have a number of obligations they must fulfil, including capital requirements, capital base requirements and consumer protection obligations.

As noted above, there are a total of eight different payment services for which financial companies can apply for authorisation. Based on the definition of neobanks used in this document, the payment services relevant to the risk assessment of neobanks are listed here. These different payment services are defined in Chapter 1, Section 2 of the Payment Services Directive.

- Deposit and withdrawal of cash
- Execution of payment transactions
- Issuance of payment instruments
- Money transfer

4.1.3 Electronic money

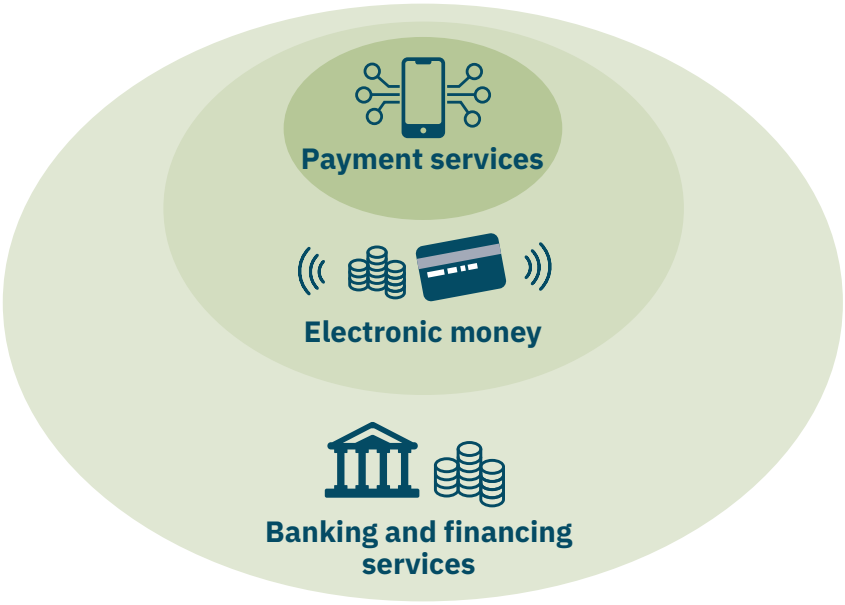
Financial companies that intend to issue electronic money need to obtain authorisation from the Swedish Financial Supervisory Authority in accordance with the Electronic Money Act (2011:755). The term electronic money refers to an electronic store of monetary value as represented by a claim on the issuer, which is issued in exchange for funds for the purpose of carrying out payment transactions in accordance with the Payment Services Directive (2010:751), and which is accepted as a means of payment by entities other than the issuer.

Banks, credit market companies, payment institutions and electronic money institutions must submit information to the Swedish Financial Supervisory Authority annually. This information is part of the supervisory activities that the authority performs in order to ensure that operators are fulfilling the conditions set out in business regulations and the Money Laundering and the Financing of Terrorism (Prevention) Act (PTL).

4.1.4 Hierarchy of authorisations

Authorisations to conduct banking or financing activities, issue electronic money and provide payment services overlap to a certain extent. The Banking and Financing Business Act (2004:297) encompasses both the Electronic Money Act and the Payment Services Directive. This means that a financial company that is authorised to conduct banking or financing activities may also issue electronic money and provide payment services without applying for an additional authorisation. However, the company is required to inform the Swedish Financial Supervisory Authority of its intention to engage in these activities in good time before the company begins offering the new service. The Electronic Money Act in turn encompasses the Payment Services Directive, which means that a company with authorisation to issue electronic money may also provide payment services provided that it informs the Swedish Financial Supervisory Authority before starting this activity. However, a company that is authorised to provide payment services cannot engage in banking or financing activities or issue electronic money.

Figure 2. Visualisation of authorisation hierarchy.



4.2 Companies with authorisation from foreign supervisory authorities within the EEA

Certain financial businesses with their registered offices in other countries within the EEA are allowed to operate in the Swedish market. This applies to banks, e-money institutions and payment institutions, among others. A basic requirement is that the company has an authorisation issued by the competent authority in the country in which the company has its registered office. The company can then notify the competent authority in the home country of the intention to provide services in Sweden. Foreign companies can conduct operations in Sweden either by offering their services through "passporting" to target the Swedish market, or by establishing a branch in Sweden. E-money institutions and payment institutions also have the option of hiring an agent in Sweden. The Swedish Financial Supervisory Authority is notified by the foreign supervisory authority. If the application concerns an e-money institution or a payment institution that wants to use an agent or establish a branch, the Swedish Financial Supervisory Authority must inform about all reasonable grounds for concern in connection with the intention to use an agent or the establishment of a branch with regard to money laundering or terrorist financing. The decision to approve operations in Sweden is made by the competent foreign authority, which also has the primary responsibility for the supervision of the company's work to combat money laundering and terrorist financing if operations will be carried out through direct passporting or through the use of agents. If operations will be carried out through a branch in Sweden, the Swedish Financial Supervisory Authority will be the supervisory authority for the branch's work to combat money laundering and terrorist financing.

4.3 Money laundering regulations and the Swedish Financial Supervisory Authority's money laundering supervision

A vast majority of the companies that are authorised by or registered with the Swedish Financial Supervisory Authority, including banks e-money institutions and payment institutions, are obliged to comply with money laundering regulations and are under the Swedish Financial Supervisory Authority's money laundering supervision. In addition to the Anti-Money Laundering Act, the regulations these companies are subject to and thus required to comply with are the Swedish Financial Supervisory Authority's regulations (FFFS 2017:11) regarding measures against money laundering and terrorist financing, as well as Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006). The various acts are usually collectively referred to as the administrative regulations for money laundering.

The administrative regulations for money laundering are risk-based regulations, which means that those who are obliged to comply with the regulations have knowledge of the risks of money laundering and terrorist financing. The regulations also require operators to take effective measures to counteract these risks in their operations by taking risk-based measures to prevent the business from being used for money laundering and terrorist financing. The measures that must be taken depend on the specific risks encountered in the business, but the basic principle is that the greatest amount of resources should be allocated to the part of the business where the risks are assessed to be the most significant.

In addition to the risk-based approach, the administrative regulations for money laundering impose a number of different requirements on operators to take certain actions. For example, operators are required to perform a general risk assessment; to establish routines and guidelines for customer due diligence, monitoring and reporting; and to perform the risk assessment of customers, all of which must be based on the general risk assessment and the requirements to implement customer due diligence measures.

The regulations also establish requirements for operators to continuously perform checks on customers and their transactions. Operators may not establish a business relationship with a customer if it is suspected that the services the operator provides will be used for the purposes of money laundering or terrorist financing. No transactions may be executed if it is reasonable to suspect that the transaction is part of money laundering or terrorist financing scheme, or if there is insufficient knowledge about the customer and there is no possibility to monitor and assess the customer's activities. Suspicious transactions and activities must always be reported to the Financial Intelligence Unit.

Operators who are under the Swedish Financial Supervisory Authority's money laundering supervision are obliged to comply with the administrative regulations on money laundering and to assist the authority in verifying compliance. The Swedish Financial Supervisory Authority has the power to carry out a number of different supervisory measures to verify compliance with the regulations. In the event that deficiencies are identified, it is ultimately the various business regulations that determine the type of intervention the authority is able to apply. Some of the measures that the Swedish Financial Supervisory Authority typically applies are orders to make corrections, sanction charges and ultimately – in the case of particularly serious violations – the revocation of the operator's authorisation or registration.

4.4 EBA guidelines

Credit institutions and financial institutions are also bound by guidelines covering the use of solutions to establish business relationships with new customers remotely[15], which are published by the European Banking Authority (EBA). The guidelines include measures that companies must take in connection with the adoption or review of solutions for establishing business relationships with new customers remotely. For example, companies should introduce and maintain risk-based policies and procedures for customer due diligence in situations where the customer relationship is established remotely. These should include, for example, a description of the situations when it is appropriate to use the solution for establishing business relationships with new customers remotely, while taking into account the risk factors that have been identified and assessed in, among other things, the general risk assessment. These policies should also include information about the checks the company carries out to ensure that the first transaction with a new customer is not completed until all initial customer due diligence measures have been carried out.

If a company introduces a new remote onboarding solution, the company should perform an assessment of, among other things, how the solution will affect the risk of money laundering or terrorist financing, as well as tests to assess risks of fraud and identity fraud. The company's risk-mitigation measures should also be assessed.

4.5 Reporting to the Financial Intelligence Unit of Sweden

An important obligation for neobanks that are authorised in Sweden is that they immediately report suspected cases of money laundering or terrorist financing in their operations to the Financial Intelligence Unit of Sweden. In 2023, operators in Sweden that fit into the category of neobanks in this report accounted for just under 7 percent of the total number of suspicious activity reports submitted to the Financial Intelligence Unit of Sweden[16]. Of the 30 neobanks, 11 had authorisation for banking activities, and these operators accounted for 77 percent of the suspicious activity reports from neobanks. Some neobanks submitted few or no reports. Some operators appear much more frequently in suspicious activity reports submitted by other parties than what they themselves report. Just like other financial institutions, neobanks only have a reporting obligation in the countries where they are registered. Within the EU, neobanks can often operate freely within the common market for goods and services. This means that neobanks must report suspected cases of money laundering or terrorist financing to the FIU in the country where the neobank is registered. If the persons or companies that appear in reports have a connection to Sweden, the relevant FIU in that country must forward the information to the Financial Intelligence Unit of Sweden. The reverse also applies if a foreign citizen or a company that is a customer of a neobank registered in Sweden appears in a report.

15 EBA/GL/2022/15 Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849.

16 For comparative statistics, see the Financial Intelligence Unit of Sweden's 2023 annual report. To provide some perspective, 7 percent is slightly lower than what the gambling industry reports (9 percent) and one tenth of the reporting from all banks (70 percent).

5. Risk assessment and impact assessment

5.1 Definitions of threats, vulnerabilities and consequences

According to the FATF, risk can be seen as a function of three factors: threats, vulnerabilities and consequences. A risk assessment for money laundering and terrorist financing is a product or process based on a methodology that is decided by the parties involved. The following definitions are based on the definitions used by the FATF.

The word threat refers to a person or group of people, object or activity with the potential to cause harm to, for example, the state, society or the economy. The threat can be criminals and their facilitators, as well as their funds and activities. Threats are often an important starting point for developing an understanding of the risk of money laundering and terrorist financing. In order to be able to perform the risk assessment, it is therefore important to have insight into the entire chain. In the case of money laundering, this means that we need to understand the criminal acts that generate criminal proceeds, as well as the actual money laundering process used to conceal the origin of criminal proceeds. In the case of terrorist financing, one needs to have insight into both of the origin of the funds and how the funds are used to finance terrorism.

The concept of vulnerabilities comprises the conditions that can be exploited by the organisation or individuals that constitute a threat or that may support or facilitate its activities. In this context, vulnerability refers to the weak points in various systems for combating or controlling money laundering and terrorist financing. Vulnerabilities may also include the features of a particular country, sector, a financial product or type of service that make them attractive for the purposes of money laundering or terrorist financing.

Consequence refers to the impact or damage that money laundering or terrorist financing may cause. This includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society as a whole. Money laundering and terrorist financing have both short- and long-term consequences for the general population, specific groups, the business climate, national interests and international interests, as well as the reputation and attractiveness of the financial sector in a country. A risk assessment in this area should thus include an assessment of threats, vulnerabilities and consequences.

Given that it can be difficult to determine or estimate the impact of money laundering and terrorist financing, it is generally accepted that an in-depth impact assessment does not necessarily need to be performed, and that countries may instead choose to focus on creating an overall picture of the various threats and vulnerabilities in the respective country. The most important thing when performing a risk assessment is to find a method to assess which risks are greater than others, which in turn makes it easier to determine which measures are needed most.

5.2 Starting points for assessments

As institutions, neobanks are associated with a number of threats and vulnerabilities which, taken together, create a risk that neobanks may be used for the purposes of money laundering and terrorist financing. In this chapter, we assess the exposure of neobanks to these risks based on the risk of both money laundering and terrorist financing. This is done based on the following starting points:

- The sector is exposed to threats from actors who seek to exploit neobanks for the purposes of money laundering and terrorist financing. These threats are rated on a scale of 1–4, with 4 being the highest level.
- Vulnerabilities refer to limitations in the sector's ability to prevent money laundering and terrorist financing at an aggregate level. These are also assessed on a scale of 1–4, with 4 being the highest level.

Taken together, threats and vulnerabilities determine the overall risk level for money laundering and terrorist financing through neobanks. The level is expressed as a numerical average of these two factors. First, a risk assessment is presented, which is based on assessments of the current risks and vulnerabilities for neobanks; then, an analysis of the potential consequences that money laundering and terrorist financing activities through neobanks can have for society is presented.

These assessments have been done based on data reported to the Financial Intelligence Unit of Sweden and the Swedish Financial Supervisory Authority, as well as information from the Swedish Economic Crime Authority and the Swedish Tax Agency. At the time of the publication of this risk assessment, the Swedish Financial Supervisory Authority's survey regarding neobanks' compliance with money laundering regulations[17] had not been completed. The assessments have therefore primarily been based on previous experience from the supervision of institutions which, like neobanks, are characterised by technological development and are associated with similar risks. Furthermore, the Swedish Financial Supervisory Authority has been able to estimate the risks to a certain degree from a sector-wide perspective based on reported data and other information gathered from authorities.

5.3 Threat and risk assessment for the banking sector from NRA 2020/2021

The national risk assessment for 2020/2021 looked at the financial sector, and banking and financing activities are part of this sector. It is mainly commercial banks that were covered, that is, limited companies that have been granted authorisation from the Swedish Financial Supervisory Authority to conduct deposit operations. The banking sector is the sector where money laundering and terrorist financing has the potential to have the most severe consequences at a national level. Traditional banks have taken comprehensive measures to reduce the risks, but the threat level remains high as almost all transactions go through the banking system at some stage.

The threat to banking or financing activities was assessed as high (4), and for payment institutions and e-money institutions, it was assessed as significant (3). The vulnerability for banking or financing activities was assessed as moderate (2), and for payment institutions and e-money institutions, it was assessed as significant (3). The risk in the banking sector was therefore assessed as significant (3). For the payment institutions and e-money institutions sectors, the risk of money laundering and terrorist financing

17 The Swedish Financial Supervisory Authority's survey of three neobanks began in November 2023.

was classified as significant (3). Neobanks operate both as banks, with banking authorisations, and as payment institutions and e-money institutions, which is why the risk assessment is based on the risk assessment for these sectors.

5.4 Threats linked to neobanks

5.4.1 High-risk customers

Traditional banks have taken comprehensive measures to reduce the risks of money laundering and terrorist financing, for example, by expanding monitoring systems and refusing to onboard or continue to serve high-risk customers. According to several authorities, extensive efforts to combat money laundering and terrorist financing have likely caused high-risk customers to look to other actors, because they have a continued need to carry out transactions for the purpose of money laundering. Neobanks are considered to be attractive to criminal actors who need to launder money, in part due to the speed of transactions, the fact that the onboarding process is relatively simple (both in the actor's own name and through straw men) and the possibility to hide the identities of the real senders and recipients.

There have been several cases where criminal actors who, after being turned down or terminated as customers of traditional banks, have opened accounts in neobanks. In some cases, criminal actors have multiple accounts in several different neobanks. This is done both in the actor's own name and using the name of straw men. The vulnerability that is most frequently exploited is the ability to bypass the verification process that is done of the customer's information, thereby hiding the identity of the real account holder.

5.4.2 Companies as tools in criminal activities

Several investigations have noted that companies are used as tools in criminal activities, and the problem with gatekeepers is significant today.[18] Many of the risks associated with corporate transactions are the same for both big banks and neobanks. It is not uncommon for companies to carry out large transactions, but neobanks, as mentioned, provide the opportunity for the actors completing the transactions to remain anonymous due to the reliance on less stringent checks. There is therefore a risk that the companies that are used in money laundering and terrorist financing will use accounts in neobanks instead of traditional banks, primarily due to the simplicity and speed of transactions and the fact that it is easier to conceal the true identity of the person who is representing the company and managing the account. In the Swedish Economic Crime Authority's preliminary investigations, it can already be seen that companies used in criminal activities use accounts in neobanks.

One concrete example is a Swedish limited company where, leading up to bankruptcy, the board members are replaced by individuals who are gatekeepers. The company is subsequently declared bankrupt, but the company continues to trade in vehicles abroad and receives payments for these, with the proceeds deposited into a neobank account. The company has also held an account in another neobank, where millions of krona have been deposited and then transferred. Another concrete example is where criminal proceeds from fraud are transferred from Swedish corporate accounts in traditional banks to foreign corporate accounts, and from there to neobank accounts where the perpetrators can access these funds, for example, by using debit cards. In other cases, criminal proceeds from tax crimes are laundered through transactions using neobank accounts. Proceeds are then moved further to other accounts or to various payment cards.

18 SOU 2023:34 *Bolag och brott – några åtgärder mot oseriösa företag* (Companies and crime – measures to prevent rogue companies).

The Financial Intelligence Unit of Sweden assesses that there is a substantial dark figure in the ability to detect, report and respond to the use of companies for money laundering and that this presents a serious vulnerability in society's ability to combat money laundering.[19] The fact that information about suspicious transactions is not reported to the Financial Intelligence Unit of Sweden increases this dark figure, as it becomes more difficult for the authority to survey the extent of money laundering. If companies that are exploited in criminal activities use neobanks to a greater extent, this dark figure will likely only increase further.

5.4.3 Transactions to high-risk countries

Many neobanks operate on the world market, which means that they are also attractive targets for terrorist financing due to the ability to carry out transactions that go to high-risk countries that traditional banks will not perform. Groups and individuals who finance terrorist activities also seek anonymity and limited traceability, which makes neobanks an attractive target for terrorist financing.

5.5 The vulnerabilities of neobanks

5.5.1 General overview of the vulnerabilities of neobanks

For criminal activities that generate money, some form of money laundering is needed to hide the origin of the criminal proceeds. These actors strive to make it difficult to trace the origin of this money and ultimately find a way to integrate the funds back into the economic system or to reinvest the funds in criminal activities. Cash is still commonly used in criminal activities, for example, in connection with payment for illicit drugs or to pay for "black labour", but the use of digital funds is increasing in line with the ongoing digital transformation in society at large.

This means that there is a risk that neobanks will become a more commonly used tool in criminal activity in the future, primarily due to the simplicity and speed of digital transactions and the ability to remain anonymous, which can make it easier for criminal actors to move and conceal criminal proceeds. When the opportunity to use financial services digitally without a physical meeting increases, where verification processes are carried out completely digitally, there is a higher degree of anonymity, which leads, for example, to a higher risk that account gatekeepers will be used.

The national risk assessment for 2020/2021 found that the use of digital banking and money transfer services facilitates the collection and transfer of money. The simplicity, speed and greater degree of anonymity offered by neobanks are some of the built-in vulnerabilities that also make them appealing to individuals looking to carry out transactions for the purpose of terrorist financing. The Swedish Economic Crime Authority has also observed this trend, as neobanks are often used in the first step of a money laundering process.

From a criminal law perspective, the origin of the funds does not matter when it comes to terrorist financing, but groups and individuals who finance terrorism also strive to remain anonymous and reduce traceability as much as possible. In this way, most of the vulnerabilities associated with money laundering are also relevant to terrorist financing. For some criminal actors, what is particularly attractive is the ability to transfer money to high-risk countries quickly with less stringent checks than in a traditional bank. Reduced traceability makes it more difficult to detect and investigate criminal activity. It is not uncommon for a neobank to be registered in

19 Report, Financial Intelligence Unit of Sweden (2022) Financial Intelligence Unit of Sweden's 2022 annual report.

one country, but to offer its services in multiple countries (in some cases, the global market), which complicates the reporting of suspicious transactions and the ability of law enforcement authorities to work closely with operators in the sector.

5.5.2 Many different parties

Many of the neobanks that are active on the Swedish market are foreign financial institutions that are authorised for these activities in other countries. This means that people in Sweden can be customers of neobanks registered in other countries. If these neobanks do not have a physical branch in Sweden, the Swedish Financial Supervisory Authority does not perform supervision for them, and they are exempt from the reporting obligation to the authority. This means that the quality of the supervision of these neobanks is dependent on supervisory authorities in other countries. Furthermore, foreign neobanks may have less knowledge of the financial behaviour of customers in the Swedish market compared to the market in which they usually operate. As a result, high-risk customers may seek out neobanks that have no knowledge of conditions in the Swedish market and what is considered risky behaviour in a Swedish context. Access to and understanding of Swedish registers, which operators use to perform customer due diligence measures, may also be lacking among foreign neobanks.

The process of requesting information from other countries and receiving answers to these requests in connection with preliminary investigations and tax investigations is a lengthy process. Responses from other countries can provide important information, for example, whether transfers have taken place to accounts in other countries, which is why new requests are often needed to seek international legal assistance from other countries. Preliminary investigations and tax investigations have shown some examples where requests have been made at several levels in an attempt to trace transactions. The fact that external parties often handle some of the functions and products offered by neobanks (e.g. issuance of payment cards) can also make it difficult to trace transactions. And the fact that responsibility for different functions is distributed among different actors also means that transactions can be more difficult to trace. The Swedish Economic Crime Authority has also noted this issue, as it often receives inquiries from other countries regarding Swedish citizens who are account holders in neobanks and who appear in these countries' preliminary investigations.

One concrete example that highlights these difficulties concerns an inquiry regarding an individual who is a customer of a neobank in a country other than Sweden. In this case, the neobank in question replied that the customer is an e-money institution and that the law enforcement authority needs to contact them. When contact was made with the e-money institution in yet another country, the answer received is that the e-money institution uses a subcontractor and that the requested end customer is a customer of yet another operator in a third country.

Digital banking transactions, which are usually not monitored by bank staff, can create favourable conditions for several types of fraud. The increasingly fragmented process for individual transactions, which can be divided among a number of different actors who only have control over the step in the chain they manage themselves, and the fact that no individual actor has the whole picture, makes it difficult to identify fraudulent transactions.

5.5.3 Cross-border operations – different inspection bodies or inadequate checks

As described above, Neobanks are obliged to report suspicious transactions to the FIU (equivalent to the Financial Intelligence Unit of Sweden) in the country in which they are registered. This means, for example, that a suspicious transaction from an account in a neobank that is registered in a country other than Sweden, but which is held by a Swedish citizen, must be reported to the FIU in that country. The same applies to foreign nationals who are customers of Swedish neobanks.

Foreign actors operating in Sweden have a limited reporting obligation, which in principle is completely dependent on self-reporting. In its taxation activities, the Swedish Tax Agency has a limited ability to collect information from foreign actors. It can also be difficult for law enforcement agencies and the Swedish Tax Agency to get responses to inquiries sent to certain jurisdictions. Furthermore, the fact that many different jurisdictions can be involved in a case can also mean that statements of earnings are not provided to the Swedish Tax Agency for transactions to and from other countries. In addition, information reported to the FIU in the country where the neobank is registered may not be shared with the Financial Intelligence Unit of Sweden. Due to deficiencies in reporting, Swedish authorities are not provided with important information.

A statement of earnings for foreign payments going to and from Sweden is part of the Swedish Tax Agency's control process and increases the ability of the agency to trace money and identify unreported income. There are indications that there are deficiencies in the statements of earnings for transfers from Swedish banks and financial institutions to foreign neobanks. There are examples where a Swedish neobank has provided a statement of earnings for foreign payments, which concerned significant amounts of money, to a neobank in another EU country, without specifying the final recipients of the payments. These cases indicate a lack of transparency, which means that there is a high risk that authorities will be unable to detect money laundering through neobanks and cases where recipients are connected to criminal activities. There are also indications that financial institutions underreport foreign statements of earnings to the Swedish Tax Agency.

5.5.4 Verification of customers and the customer due diligence process

In the national risk assessment for 2020/2021, it was found that the financial system depends on a high level of trust in the primary verification of a person's identity. This means that the use of gatekeepers and misuse of identities are particularly problematic for the Swedish money laundering regime. Neobanks are obliged to implement customer due diligence measures for their customers. The customer due diligence processes and the requirements for documentation may differ between different neobanks, but due to the fact that the onboarding process for a new customer is simpler and faster, the quality of customer due diligence measures can also be affected.

One notable vulnerability in the verification and customer due diligence processes in neobanks is that the customer is not identified in a physical meeting. When the verification process is instead based on digital meetings, the customer typically sends certified copies of an ID document and a photo. However, this creates opportunities for actors to misuse other people's identity documents. It is relatively easy to use fake identity documents, and there are even online services that openly state in their advertising that they will help customers bypass the verification process for a fee.

Even if e-identification is used, there are documented cases where e-identification is bypassed in connection with verification processes. One particularly important aspect, which presents a serious vulnerability and opens the door to several types of

fraud, is the login and digital signature process (approvals of transactions). Another vulnerability, which is exploited by actors who commit fraud, is the possibility for the bank to issue a new mobile e-identification to a new device, which can then be used in connection with login and document signing.[20] One concrete example is a ruling issued by the National Board for Consumer Complaints, which describes how a perpetrator in a fraud case convinced an individual to install an e-identification in his name on the perpetrator's device. He was then able to use the e-identification to open an account in a neobank and transfer money there from the other person's account.

Within the EU, there is eIDAS[21], but it does not address the fundamental vulnerabilities of e-identification: the inability to verify the identity of the person who has been issued an e-identification and to verify that the person using it is indeed the person to whom the e-identification was issued.

5.5.5 Customer relationships and the division of responsibilities

When a cooperation agreement between operators includes a "white labelling" scheme, which enables certain operators to offer products and services that otherwise fall outside of the operator's own authorisations (see Section 2.5), it often leads to questions about risk ownership and the division of responsibilities in the customer due diligence processes and transaction monitoring. This in turn leads to fuzzy boundaries regarding which party owns the customer relationship and thus is responsible for the risk of, for example, money laundering or terrorist financing. These cooperation agreements are not currently specifically regulated under Swedish law, which can create problems when drawing boundaries regarding customer relationships and the division of responsibilities.

5.5.6 Lack of transparency

In the national risk assessment for 2020/2021, it was noted that technological developments give rise to new challenges. New payment solutions are emerging, and the way they are designed can create opportunities to conceal transactions and assets, making detection and controls more difficult. These new solutions also make transactions faster.

Some neobanks use accounts known as virtual bank accounts. These accounts can be compared to client funds accounts, meaning the neobank has an account with a bank with balances for several of its customers. The neobank keeps the balances for each individual customer in order by using various ledgers. For example: the neobank looks like a traditional bank to the end customer, but when customer X deposits money into the neobank account, which is usually linked to a payment card, the funds are actually deposited to bank B where the neobank is the account holder (where the same account includes holdings for other customers). This type of account set-up complicates the ability of banks to trace funds and perform monitoring activities. It can also lead to incorrect counterparty information in the anti-money laundering register when submitting a suspicious activity report.

The Account and Deposit Box systems Act (unofficial translation, Swedish title lagen om konto- och värdefackssystem) covers credit institutions, foreign credit institutions with branches in Sweden, securities companies and foreign securities companies with branches in Sweden. The term credit institution refers to banks and credit market companies, which are authorised to provide deposit accounts, among other activities.

20 Report, National Board for Consumer Complaints (2023) *Bedrägerier mot privatpersoner* (Fraud against private individuals).

21 eIDAS: Regulation on electronic identification and trust services, Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Therefore, most Swedish neobanks are not covered by the law and are not included in the Swedish Tax Agency's Mekanismen platform[22]. Mekanismen is a technical platform developed by the Swedish Tax Agency so that law enforcement agencies, the Swedish Tax Agency's taxation operations and the Swedish Enforcement Authority can quickly access information about which accounts a person or company holds, or acts as proxy for, with the above-mentioned institutions. Mekanismen also makes it possible to determine which persons or company/companies hold a particular bank account or deposit box. Currently, around 120 institutions are connected to Mekanismen. Due to the fact that neobanks that are not considered banking and credit market companies are not included in Mekanismen, a search in Mekanismen for a person, a company's corporate identity number or personal identity number (for representatives) does not return hits for accounts held in many Swedish neobanks. As a result, these assets are often not detected and remain hidden from authorities, which creates a significant risk.

Operators with authorisation to conduct banking activities in Sweden are included in Mekanismen, which means that authorities can find specific account holders with the operator when they perform a search. However, operators without authorisation to conduct banking activities in Sweden, such as foreign neobanks or Swedish neobanks without authorisation to provide deposit accounts, are not included in Mekanismen. If a neobank that is not authorised to conduct banking activities in Sweden holds client funds accounts with an operator that does have authorisation, only information about the neobank's client funds account can be found on Mekanismen; however, information about which customers have account holdings with the neobank in question will not be searchable. Customers' holdings in the neobank's client funds accounts may refer to funds that are to be made available at a later date on a payment card, a business account or savings account through another operator with whom the neobank has a cooperation agreement.

One example: Person A has an account with a Swedish bank with authorisation to conduct banking activities and an account with a neobank that does not have authorisation. When searching for the person in Mekanismen, only the first account will be found, not the second. This is because the neobank where person A has an account in turn has a client funds account in the Swedish bank, and the Swedish bank does not have information on which customers the funds in the client funds account belong to. Person A's holdings in the neobank are thus one step removed from the accounts that can be searched in Mekanismen.

Each EU member state must have an asset recovery office (ARO) for criminal proceeds in order to be able to quickly trace the proceeds of criminal activity outside the borders of the respective member state without having to request legal assistance. AROs have access to Mekanismen, which simplifies and speeds up the process of detecting where criminal proceeds are located within the EU. The fact that not all neobanks are connected to Mekanismen therefore makes it difficult to quickly trace criminal proceeds.

For companies that have bankgiro via neobanks, there are deficiencies in the way data and account details are registered and managed. The neobank is often indicated as the primary organisation linked to corporate accounts or bankgiro numbers, instead of the actual holder. When using Bankgirot's search service for bankgiro numbers, this is evident when, for example, a search for a company's corporate identity number does not generate any results. This problem has several negative consequences, such as inaccuracies in the data held by banks and in the anti-money laundering register, which affects the ability to monitor suspicious transactions.

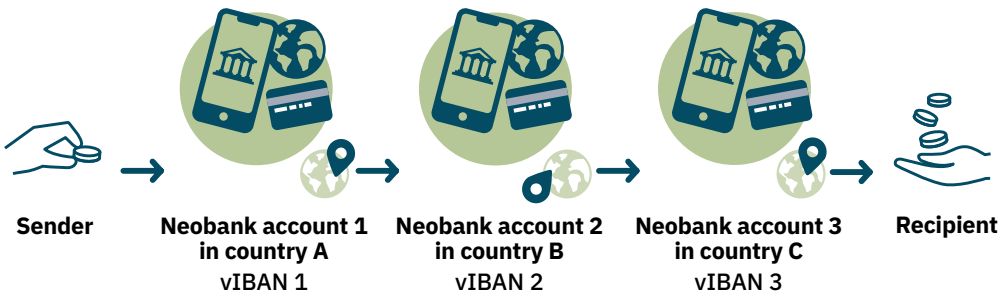
22 Account and Deposit Box systems (Mekanismen); more information about Mekanismen can be found on the Swedish Tax Agency's website.

There is also a vulnerability associated with information sharing for transactions between different operators in the transaction chain, which is addressed in the Financial Intelligence Unit of Sweden's report on neobanks.[23]

This applies in particular to deposits to an account with a neobank where both the sending and receiving bank and the neobank in question have limited information about the receiving and sending parties. In the case of a card deposit, the transaction usually takes place through an interface via the neobank. When the funds go to a neobank's client funds account at a receiving bank, the sending bank does not see the identity of the account holder at the neobank. The neobank, in turn, may have limited information about who the payment card belongs to and thus the identity of the sender. Several neobanks also allow individuals other than the account owner to make card payments to another person's account.

In its threat assessment of financial and economic crime for 2023[24], Europol reported that vIBANs are being exploited by criminals, as they enable fast international payments that mask the identity of the main account, the issuing operator and the country of origin. Due to the structure of vIBAN, there is virtually no limit to the number of intermediaries that can be used between the bank and the end customer (Figure 3). This vulnerability is exploited in the criminal economy to launder money and maintain a parallel economy. For example, criminal actors can carry out transactions using a large number of virtual bank accounts with payments going to different countries. In this way, they can easily spread out their assets over many virtual bank accounts and make it difficult to trace the flow of funds. This makes it more difficult to detect and trace suspicious transactions and creates extra steps in financial investigations. Due to the ability to conceal transactions and the lack of transparency, efforts to combat money laundering become more complicated, and it is more difficult for law enforcement authorities to do their work.

Figure 3. Different vIBANs in a series of transactions.



23 Report, Financial Intelligence Unit (2022) Neobanker (Neobanks).
24 Report, Europol (2023) The Other Side of the Coin – Analysis of Financial and Economic Crime.

5.6 Risk assessment and impact assessment

The risk of money laundering and terrorist financing is assessed by weighing threats and vulnerabilities.

In the national risk assessment for 2020/2021, the threat of money laundering and terrorist financing in the banking sector was assessed as high (4). Almost all money laundering schemes use the banking sector in some way, and neobanks are part of the banking sector, which means that the threat of money laundering for neobanks is assessed to be the same as for the banking sector as a whole, high (4).

This assessment is based on the fact that there is a continued need for transactions in money laundering and terrorist financing schemes, but when high-risk customers are rejected by traditional banks, they are likely to look for other solutions to meet this need. Based on the ability to conceal the identities of account holders, senders and recipients and trace transactions, neobanks are attractive to high-risk customers. These vulnerabilities mean that the threat that companies will be used in money laundering schemes is also factored into the assessment, as there is a risk that it will be more difficult to detect money laundering and terrorist financing when the funds go through companies. The fact that many different parties are involved means that there is a risk that the number of suspicious transactions that come to the attention of the Financial Intelligence Unit of Sweden will decrease further. This not only leads to an even greater increase in the dark figure, but it also makes the Swedish Tax Agency's activities more difficult. The ability to carry out transactions that go to high-risk countries has also been factored into the assessment.

In the national risk assessment for 2020/2021, the vulnerability of the banking sector to money laundering and terrorist financing as a whole was assessed as moderate (2), and for payment institutions, payment service providers and electronic money issuers, it was assessed as significant (3).

The vulnerability of neobanks to money laundering and terrorist financing is assessed as significant (3), that is, the second highest level. This assessment is based on the fact that neobanks share many similarities with payment institutions, payment service providers and electronic money issuers, as not all neobanks are authorised to conduct banking activities. But the identified vulnerabilities for neobanks are also similar to the above sectors, namely, the large number of parties and jurisdictions involved in transactions, difficulties regarding the traceability of transactions, the lack of physical meetings in connection with verification and customer due diligence processes, and the ability to hide the identity of the true account holder, sender and recipient.

In the national risk assessment for 2020/2021, the risk of money laundering and terrorist financing in the banking sector and the payment institution, payment service provider and electronic money sectors was assessed as significant (3).

There are currently neobanks that function as banks with banking authorisations, as payment institutions and payment service providers and as e-money institutions. The risk for neobanks is therefore also assessed as significant (3). This assessment is based on the threats and vulnerabilities that have been identified, above all the threat posed by high-risk customers; the difficulty tracing transactions; the ability to conceal the identity of the true account holder, sender and recipient; and the ability to carry out transactions to high-risk countries. This assessment may change over time due to, for example, changes in customer due diligence processes, changes that make verification processes more reliable or improved information exchange. But the assessment can also change as the use of neobanks and other electronic payment solutions increases over time.

Banking is the sector where money laundering has the potential to have the most severe consequences at a national level[25]. Traditional banks have taken comprehensive measures to reduce the risks, but the threat level remains high as almost all money laundering schemes go through the banking system at some stage. The exploitation of the banking sector for money laundering can potentially have a negative impact on confidence in the financial system and damage Sweden's reputation internationally. Terrorist financing has the same negative effect, but it also leads to the ability of actors to successfully carry out terrorist acts.

Neobanks are part of the banking sector, but the characteristics, vulnerabilities and threats identified in this report (i.e. the simplicity and speed of transactions, involvement of many parties and jurisdictions and the ability to conceal the true account holders, senders and recipients) can have other consequences. If neobanks are used for money laundering and terrorist financing, there is a risk that trust in the financial system will be eroded, particularly trust in neobanks, but Sweden's international reputation would be damaged to a lesser degree. In terms of the consequences for Sweden, the threats and vulnerabilities associated with neobanks create the risk that it will be more difficult to detect and prosecute money laundering and terrorist financing. This can lead to lower rates of prosecutions and obstacles to tax investigations, which can ultimately lead to reduced tax revenues if taxation cannot be carried out correctly.

25 Report, The coordination function (2021). "National risk assessment of money laundering and terrorist financing in Sweden 2020/2021".

6. Recommendations

Competence building

There is a general need to increase the knowledge of the risks associated with neobanks among Swedish operators and authorities who come into contact with these operations in their work. Competence building should focus on increased awareness of, among other things, the customer due diligence processes used by neobanks and the use of e-identification in these processes. The need for competence-building initiatives should be analysed based on the tasks performed by each individual operation.

Foreign neobanks

In order to facilitate the work of Swedish authorities, Sweden should work to improve the exchange of information about Swedish customers who hold accounts in foreign neobanks. This effort should also include measures to improve the traceability of transactions and counteract deficiencies in counterparty information.

Products and services

Products and services that cannot be obtained from certain neobanks, because they fall outside the scope of the operator's own authorisations, can instead be offered through white labelling schemes in cooperation agreements with other suppliers, usually traditional banks. However, there should be a review of Swedish legislation regarding the ability to offer products and services that fall outside the scope of an operator's own authorisations due to problems associated with drawing boundaries in customer relationships and the division of responsibilities, which is often an undesirable result of such cooperation agreements.

Verification

Remote verification processes should, as far as possible, be designed to reduce the risk of account gatekeepers and the use of stolen and false identities, for example, through increased use of e-identification. Sweden should therefore work to ensure that e-identification is used within the EU to the greatest extent possible when verifying customer identities and approving transactions.

International cooperation

Stronger international cooperation is a basic prerequisite for successfully combating money laundering and terrorist financing through the exploitation of neobanks. As there are currently deficiencies in the sharing and handling of suspicious activity reports between the FIUs in EU member states, the Financial Intelligence Unit of Sweden should take proactive measures to improve this situation. Through increased interaction and information exchange, the Financial Intelligence Unit of Sweden can also play an active role in improving both the quality and quantity of reporting from neobanks.

The reporting obligation

Different countries interpret the regulations within CRS and DAC2 differently. This leads to ambiguities regarding whether neobanks in other countries are covered by the obligation to report information about financial accounts. Currently, this creates a discrepancy between countries, and there is a risk that criminal actors who wish to evade taxation or commit money laundering will open accounts in neobanks registered in countries where neobanks are not considered to be covered by CRS and DAC2 reporting. Sweden should therefore investigate the possibility of harmonising the reporting obligation for financial institutions within the OECD and the EU.

The Swedish Tax Agency

There are indications of under-reporting of foreign statements of earnings to the Swedish Tax Agency, but at the moment, no sanctions are imposed in connection with deficiencies or omissions in this information. The Swedish Tax Agency should examine whether it is possible to impose late fees/sanctions on financial institutions in the event of late, incomplete or missing statements of earnings (KU80/81). The information should also be submitted on a form established by the Swedish Tax Agency.

The Swedish Tax Agency's Mekanismen platform

Swedish neobanks that are not authorised to offer deposit accounts are not covered by the requirement to report accounts to Mekanismen. However, these operators take funds from their customers, which are placed in client funds accounts with traditional banks. The fact that holdings belonging to customers of neobanks in these client funds accounts cannot be searched in Mekanismen makes it more difficult to trace transactions and to identify and recover criminal proceeds. It should be explored whether there are conditions to expand the reporting requirement regarding account holders so that neobank customers with accounts in a neobank, or in other banks where the neobanks have client funds accounts or similar, are also covered by the requirement. Such an investigation should also include vIBAN and identification of virtual bank accounts with neobanks.

THE COORDINATING BODY FOR ANTI-MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM