



REPORT IN BRIEF

Prioritised risks in anti-money laundering and combating the financing of terrorism

22 March 2024

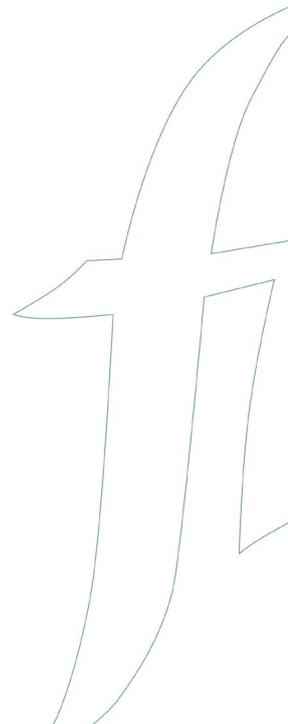
Summary

There is a high risk that the financial system is being used by criminals to launder money. This is serious and drives organised crime. At the same time, there is still a risk that the financial system is being used to finance terrorism or to circumvent international sanctions decided by the EU Council. Given these risks, one of FI's supervision priorities for 2024 is to review that financial firms are doing what they should to protect themselves from being used for criminal purposes.

A well-functioning financial system should be stable and characterised by a high degree of confidence. This is a prerequisite for a functional economy.

In order for FI's supervision to be as efficient as possible, we need to direct our resources to areas where the risks are the greatest and we can achieve the most benefit. Within anti-money laundering supervision, the risks are currently assessed to be located in specific categories of firms, such as digital banks, small and mid-size banks, and cash-intensive businesses. The risks are also sector-wide, such as the use of companies as instruments for crime, the increasing risk of terrorist financing, and deficiencies in compliance with international sanctions.

In this report, we present the areas where we right now assess the risks of being used for money laundering to be greatest for financial firms and to which we will devote special attention in our supervision during the year.



Introduction

Money laundering is a global problem that makes it possible for criminals to transfer their illicit gains without revealing their illegal activities. As noted in the 2021 national risk assessment of money laundering and terrorist financing¹, there are no reliable estimates of how much money is being laundered in Sweden every year, but it most likely is in the billions. Terrorist financing, on the other hand, constitutes a serious threat to general safety. In August 2023, the Swedish Security Service raised the terrorist threat level in Sweden to High (a 4 on a scale of 5) due to the deteriorated security situation.

Money laundering and terrorist financing are thus difficult challenges for society at large. These criminal activities also represent serious challenges for both the Swedish and the global economies. For this reason, the work to reduce illicit financial flows is one of the global targets (Target 16.4) in the UN's action plan, Agenda 2030. The work to combat money laundering and terrorist financing is therefore also part of Finansinspektionen's (FI) work to promote sustainable development in the financial sector.

The financial sector as a whole is particularly exposed to the risk of being used for money laundering and terrorist financing. Part of our assignment is to apply a risk-based approach to the supervision of more than 2,200 firms. These firms range from sole-proprietorship foreign currency exchange offices to large global banks, and the threats and vulnerabilities can vary significantly. In order for our supervision to be as effective and appropriate as possible, we identify every year the risks (for example, trends and current phenomena) that should be prioritised within the supervision of the coming year.

For our risk identification, we use information obtained from firms via the annual anti-money laundering reporting. We also draw on the experiences from our ongoing supervision and previous investigations as well as our collaborations with other supervisory or law enforcement authorities in Sweden and abroad. In the past few years, these collaborations have increased not only in scope but also in significance and thus have contributed to our understanding of risk. Nationally, we can mention our collaborations with the Financial Intelligence Unit of the Swedish Police and the Swedish Gambling Authority as well as the work of the Coordinating Function to Combat Money Laundering and Terrorist Financing. Internationally, we worked in particular during the year with the Nordic-Baltic

¹ The Coordinating Function to Combat Money Laundering and Terrorist Financing issues a regular report on the overall risk assessment for Sweden related to money laundering and terrorist financing. The assessment is supported by 16 authorities and the Swedish Bar Association.

AML/CFT Working Group, the IMF, and the 70 anti-money laundering colleges established in accordance with the guidelines from the EBA.

Prioritised risk areas for 2024

One of FI's prioritised supervision areas for 2024 will be to review that financial institutions are doing what they should to protect themselves from being used for criminal purposes. We account here for the risks related to anti-money laundering that we assess to be most relevant in the financial sector for the year.

Companies as instruments of crime

The 2021 national risk assessment highlighted the risk that firms and other legal persons are used as instruments in the criminal act. This is partly because, for a financial institution it can be more difficult to follow a firm's business activities and transactions compared to private individuals. There is also the challenge of understanding the true ownership and control structure for a company. There is therefore a considerable risk that firms and other legal persons are being used in more complex and systematic money-laundering structures. This overview has been confirmed by the Financial Intelligence Unit of the Swedish Police and other anti-crime authorities.

Increased risk of terrorist financing

Terrorist financing represents a direct and concrete threat to the general safety of both Sweden and other countries. According to the most recent status report from the Swedish Security Service, the level of threat towards Sweden has increased. Sweden has gone from being a legitimate target to a prioritised target for terror attacks. The requirements on businesses' work to combat terrorist financing have thus increased correspondingly.

Unlike for money laundering, terrorist financing can utilise both legally and illegally obtained funds. Only small amounts are usually needed to enable an attack both in Sweden and abroad. The collection and transfer of assets can occur quickly, using simple means and without major costs. The financier does not need to have special skills, but international contacts are an important factor in the money reaching the intended destination.

Banks and other types of payment service providers are assessed to be the sectors where the risks of terrorist financing are the greatest. This is largely due to the size of the sectors and the ease with which they can be accessed, but their services are also well-suited for the purpose. The market for cryptoassets is also assessed to be a sector where there is a risk of transfers related to terrorist financing.

Digital banking services and cryptocurrency exchangers

FinTech-sector firms, which help firms and private individuals with different types of new and innovative payment services, are continuing to increase in terms of both number and turnover. Digital banks (neobanks), which have popped up on the Swedish market in recent years, are offering a larger product range than traditional payment service providers. Because the industry is marked by a rapid rate of development and innovation, it is important that the firms adapt and develop their method of managing the risks associated with their products and services at the same rate. In recently conducted investigations of payment service providers, we have seen several examples of how firms have not adapted their ability to combat the risk of money laundering and terrorist financing to their growing operations.

The trade in cryptoassets is increasing and is often a prerequisite for trade in narcotics on the Darknet. It is also an attractive way for criminals to transfer their illicit gains. Trade in cryptoassets also entail tangible risks from consumer protection and climate perspectives. The risks associated with trading in cryptoassets is highlighted both in the 2021 national risk assessment and the EU's most recent supranational risk assessment.

The riskiest actors among those that engage in the trading of cryptoassets are those that provide services subject to registration without having applied to FI for registration. These actors are increasing in number and have large turnovers according to analyses from law enforcement authorities. Among these traders, there is a risk of both low risk awareness and limited ability to counteract use in criminal acts while the risk of being used for criminal purposes is correspondingly high.

Increased risk of money laundering among small and mid-sized banks

As the major banks have improved their preventive work, there are indications that criminal actors are instead shifting to small and mid-sized banks. These smaller banks often offer a range of services that is similar to that of the major banks, which entails similar risks. There is therefore a risk that some of the risks that previously were centred around the major banks have now shifted to smaller actors.

Increased risk for money laundering in cash-intensive business activities

We have seen in our supervision a risk of smaller firms, particularly foreign currency exchangers, not having sufficient knowledge about the risk of money laundering and terrorist financing and the regulations in the area. As a result, this

leads to a greater risk that they will be used by criminal actors for money laundering.

The same applies to firms that provide informal value transfer services, such as *hawala*, where traceability and transparency are often very low. The risks associated with *hawala* are highlighted in particular in the 2022 national risk assessment, which states that the system is often used as a channel to make payments to countries associated with high or extremely high risk of money laundering or terrorist financing.

These firms' business activities are also cash intensive. There is a risk that this will make the firms particularly attractive for criminals who need to transfer their illicit gains; this has also been noted in the EU's most recent supranational risk assessment. These activities are also assessed to be interesting tools for terrorist financing.

Risk of non-compliance with international sanctions

Due to Russia's invasion of Ukraine, the number and scope of the EU's restrictive measures have increased. In order for the sanctions to have the desired impact, it is crucial that businesses follow the rapid development and comply with the sanction provisions. The sanctioned firms and persons may not have access to assets and financial means to a greater extent than specified in the sanction regimes.