REPORT

Prioritised risks related to money laundering and terrorist financing

10 March 2025

Summary

There are many actors who have an interest in using the financial system for criminal purposes, such as for money laundering, financing of terrorism or to circumvent the EU's international sanctions. This is a serious matter and financial firms are obliged to prevent being exploited in this way. Given these risks, one of the FI´s priorities for 2025 is to review that firms comply with regulation aimed to prevent money laundering and other crime.

A well-functioning financial system should be stable and characterised by a high degree of trust. This is a prerequisite for a functional economy. Finansinspektionen (FI) exercises supervision of the financial firms that are subject to the Anti-Money Laundering Act to ensure they comply with the rules set out there to prevent them from being used for money laundering. In order for FI's supervision to be as efficient as possible, we need to direct our resources to areas where we assess the risks to be greatest and we can achieve the most benefit.

In this report, we present the areas where we right now assess the risks of being used for money laundering or terrorist financing to be greatest in the financial sector and to which we will devote special attention in our supervision during the year. The risks are currently assessed to be located in firms that offer digital banking services, crypto actors, and small and mid-size banks. We also observe risks in special areas, such as in correspondent relationships and in the provision of client funds accounts. Some of the risks are also sector-wide, such as the use of companies as instruments for crime, use of cash, the continued elevated risk of terrorist financing, and deficiencies in compliance with international sanctions.

Introduction

Money laundering, terrorist financing, and circumvention of sanctions are all global problems. As noted in the 2021 national risk assessment of money laundering and terrorist financing, money laundering most likely amounts every year to billions of kronor. [1] At the same time, terrorist financing constitutes a serious threat to general safety. Since August 2023, the Swedish Security Service has considered the terrorist threat level in Sweden to be high, a 4 on a scale of 5.

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 prevent money laundering and terrorist financing is therefore also part of FI's work to promote sustainable development in the financial sector.

Our assignment to supervise the financial sector is extensive and encompasses approximately 2,200 firms ranging from small currency exchangers to global banks, the threats and vulnerabilities of which can vary significantly. In order for our supervision to be as effective and appropriate as possible, we identify every year the risks that should be prioritised within the supervision of the coming year. For our risk identification, we draw on experiences from our ongoing supervision and previous investigations and use, among other things, information obtained from the firms via the annual regular reporting.

FI also works closely 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, the Swedish Economic Crime Authority, and the Swedish Gambling Authority as well as the work of the Coordinating Function to Combat Money Laundering and Terrorist Financing. Internationally, we are working in particular with the European Banking Authority, the Nordic-Baltic AML/CFT Working Group and the International Monetary Fund and are participating in around 70 anti-money laundering colleges for financial institutions that are active in several jurisdictions within the EU.

[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. This assessment is supported by 16 authorities and the Swedish Bar Association.

Prioritised risk areas for 2025

Reviewing the prevention of money laundering and other crime is one of FI's prioritised areas for its supervision in 2025. We make the assessment that several of the risks we identified in previous years continue to apply this year as well. We account here for the areas we consider to be most relevant for the year.

Client funds accounts

For a person with criminal intent, it can be beneficial to conduct transactions through a client funds account, as it provides increased opportunities for anonymity. The reports from both the Financial Action Task Force (FATF) and the Financial Intelligence Unit conclude that client funds accounts can be misused for money laundering purposes. The accounts can be used to both hide criminal proceeds and integrate them into the financial system, for example through investments in properties or securities.

Correspondent relationships

Correspondent relationships are an important component in the global payment system, particularly for cross-border transactions. Through correspondent relationships, financial institutions gain access to financial services in jurisdictions around the world and are able to provide cross-border payment services to their customers. Also, the innovative technological development in this area has created new opportunities. However, there are also risks since the financial firms provide services to actors with whom they do not have a direct business relationship with and they need to rely on that other financial firms have effective and suitable procedures and controls to prevent money laundering.

Companies as instruments of crime

As in previous years, FI makes the assessment that the risk is prominent that companies and other legal persons are being used as instruments of crime. This is partly because, for a financial institution, it can be more difficult to follow a corporate customers' business activities and transactions than those of private individuals. There is also the challenge of understanding a legal persons' true ownership and control structure. A company can also conduct larger and more complex transactions than a private individual, and for example enter cash into the banking system via daily cash deposits. There is therefore a considerable risk that companies and other legal persons are being used in more complex and systematic

money-laundering structures. This overview has been confirmed by the 2021 national risk assessment.

Digital banking services and crypto actors

The national risk assessment of money laundering and terrorist financing in Sweden for 2023/2024 discusses in particular the risks associated with fast, digital financial services that are offered by some actors on the financial market. The industry is characterised by a high rate of development and innovation that contributes to new financial solutions for both consumers and business clients but also to new opportunities for criminals to act in the new digital environment. It is therefore important that firms adapt and develop their method of managing the risks associated with their products and services.

The trade in crypto assets is continuing to increase, and the police describe it as a prerequisite for trade in narcotics on the Darknet. It is also an attractive way for criminals to transfer their illicit gains. Trade in crypto assets also entail tangible risks from consumer protection and climate perspectives. The risks associated with trading in crypto assets 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 crypto assets are those that provide services subject to registration without having applied to FI for registration. Among these traders, there is a risk of both low risk-awareness and a limited ability to counteract being used by criminal acts. Hence the risk of being used for criminal purposes is correspondingly high.

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 similar to that of the major banks and thus 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.

Terrorist financing

The threat towards Sweden is still high, and, according to the Swedish Security Service, Sweden is a legitimate target for terror attacks. This places high demands on businesses' work to prevent terrorist financing.

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. The market for crypto assets is also assessed to be a sector where there is a risk of transfers related to terrorist financing.

International sanctions

The Russian full-scale invasion of Ukraine has been ongoing since 2022, which has increased both the number and scope of the EU's international sanctions.

In order for the sanctions to have the desired impact, it is crucial that firms follow the rapid development and comply with the sanction provisions. So that the sanctioned businesses and persons may not have access to assets and financial means to a greater extent than that is specified in the sanction regimes.

FI's in-depth analysis into sanctions shows that the effectiveness of the automated systems that banks use for their sanctions screening could be higher in general and that there is room for some banks to improve their work in this area.