The Financial Intelligence Unit Annual Report 2021

Polisen
Swedish Police

Swedish Police Authority

May 2022

Contents

Foreword

In 2021, the Financial Intelligence Unit (FIU) continued to make progress in efforts to combat money laundering and terrorist financing. Thanks to increased resources and investments in analysis, systems development and improved routines that contributed to greater efficiency, the FIU was able to deal with more suspicious activity reports than ever before. The FIU also provided feedback to both industry entities and individual obliged entities in a more systematic way.

Serious and organised crime is largely motivated by financial gain. Measures to prevent criminals gaining access to money can have a major impact, and the FIU has a key role in the Swedish Police Authority's work to recover the proceeds of crime.

Stopping a front man from lending his account for a lot of small amounts from the sale of drugs in a vulnerable area can help to increase security in that area. Closing down a bureau de change that enables the profits from large-scale drugs sales to be reinvested in new drugs consignments to Sweden can have an even greater impact. Money laundering from systematic welfare fraud or VAT carousels can turn over even larger sums. Shutting this down can prevent major crime proceeds fuelling serious and organised crime or financing violent extremism.

Irrespective of the size of the amounts or the damage caused to society by criminal activity, measures need to be taken throughout the chain. The Swedish Police Authority cannot choose to focus just on the large and complex schemes; it has to be able to deal with a large amount of smaller intelligence matters in parallel.

Media reports in recent years have shown that money laundering is a widespread and global problem, and cross-border collaboration is essential to be able to tackle it. Through international cooperation, the Swedish Police has been able to obtain information contained in the encrypted chat platforms Encrochat, Sky ECC and Anom. This material provided unique insights and led to operational successes over the course of the year.

To keep pace with developments, law enforcement agencies need tools that are fit for purpose. The inquiry on strengthened measures to combat money laundering and terrorist financing presented its final report in 2021 and its proposals included greater possibilities for information exchange between government agencies and private partners in the financial sector. It is also proposed that more types of business should be involved in efforts to detect and identify suspicious financial flows. Strengthening capacity at all stages, from private companies to the FIU, will have a major impact on the prospects of effectively combating money laundering and terrorist financing.

Johan Olsson
Head of the National Operations Department

The tasks and activities of the Financial Intelligence Unit

The FIU is a part of the Intelligence Division at the National Operations Department of the Swedish Police Authority. The FIU is responsible for intelligence activities concerning money laundering and terrorist financing and must be independent in receiving, analysing and sharing information within its area of responsibility.

In 2021, approximately 45 people worked at the Unit. Employees have varying backgrounds in the Swedish Police Authority, other government agencies and the business sector.

The task of the FIU

The FIU gathers information about when money laundering is suspected to be part of an attempt to conceal proceeds of crime. The task also includes gathering of information on terrorist financing.

The FIU is part of the Swedish Police Authority. This means that the FIU adjusts its activities to guidelines from the police management and uses these when setting priorities among tip-offs, enquiries, requests for assistance and reports on suspicious transactions that it receives. As an intelligence service, a basic task is also to detect, at an early stage, trends in money laundering and terrorist financing that may influence other police activities or cause significant financial risks in general with regard to money laundering or terrorist financing.

The activities of the FIU are regulated by a number of acts and ordinances. Some of the information that forms the basis of the FIU's work comes from entities that are obliged to report in line with the Act on Measures against Money Laundering and Terrorist Financing[1], such as banks, gambling companies and payment service providers. Only employees at the FIU are able to access the database where this information is processed.

> Information is processed and analysed in different phases and can result in various types of measures, depending on their purpose.

From information to action

The FIU gathers and deals with information from various sources, for example reports from obliged entities, information from FIUs in other countries or other intelligence. The information is processed and analysed in different phases and can result in various types of measures, depending on their purpose. Examples of measures taken by the FIU may be to write an intelligence report, file a police report or initiate a strategic analysis case in a specific area.

Documents may be shared with other parts of the Swedish Police Authority or other law enforcement agencies for further action. For example, they can be added to a police report or result in the recipient filing a police report. However, the FIU is not automatically informed of the measures taken.

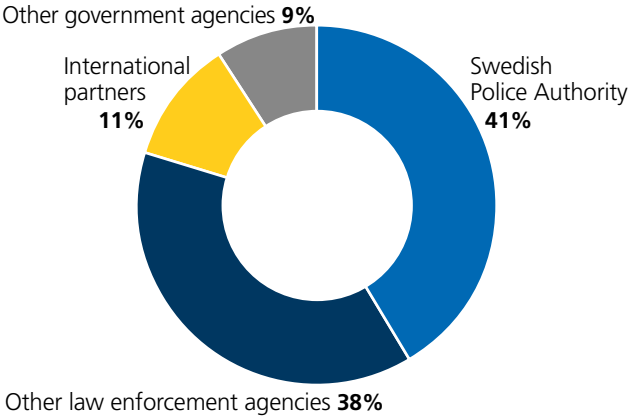
1 Act on Measures against Money Laundering and Terrorist Financing (2017:630).


500
SVERIGES RIKSBANK
FEM HUNDRA KRONOR

The illustration below shows a simplified model of how the FIU deals with the information it receives. In reality, a case may involve many more steps (see the example on page 14).

In 2021, the FIU shared a large amount of intelligence with other parts of the Swedish Police Authority as well as externally. The information was mainly received by law enforcement agencies in Sweden, but the FIU also handed over information to international partners, such as FIUs in other countries (see figure 1).

Figure 1. Recipients of information in 2021



From information to action

INFORMATION

The FIU receives intelligence from obliged entities, supervisory agencies, other FIUs and more.

REGISTRATION

The information is registered in the money laundering database. On the basis of certain criteria, an initial selection is made for further processing.

SETTING PRIORITIES

Information is assessed, given a priority level and supplemented with data from other sources.

Intelligence cases are set up.

PROCESSING

The information in each case is supplemented further by gathering and analysing data.

This work can result in new cases being initiated.

ACTION

Depending on the case, different measures are taken, such as sharing intelligence or issuing restraint orders.

STRATEGIC WORK

In parallel to operational efforts, the FIU also works strategically with the information contained in the money laundering database. The strategic work involves cooperating in various forums and analysing trends or methods.

The FIU is primarily an intelligence service, but if there is tangible information about an offence, the FIU is to file a report. A police report is also always filed when a restraint order is issued. In 2021, the FIU filed 609 police reports, which was the same number as the previous year (see table 1).

Analysis of information also results in other kinds of strategic analysis, guidance for industry organisations or information brochures, such as 'Information from the FIU'. These support obliged entities in their efforts to combat money laundering and terrorist financing. The information dealt with by the FIU may therefore be reused in various ways and for various purposes. This means that the information in a report from an obliged entity may form the basis of many different measures, taken for different purposes.

Table 1. Police reports by the FIU

Year	Number of police reports
2017	136
2018	165
2019	242
2020	609
2021	**609**

Restraint orders 2021

Restraint orders are a temporary prohibition to relocate or in other ways make use of assets that are suspected of being the object of money laundering or terrorist financing. Under the Act on Measures against Money Laundering and Terrorist Financing*, the FIU is authorised to take such decisions. An order applies for at most two working days, and must be examined by a public prosecutor during that time. Thus, a restraint order does not necessarily mean that money is seized or that a preliminary investigation is launched.

In addition, restraint orders may only be issued when it is imperative that action is taken without delay to keep the assets from being hidden. The reasons for the measure must also outweigh the intrusion or the detriment that the measure implies.

Both the FIU and obliged entities can detect circumstances that can lead to a restraint order being issued. Obliged entities can indicate a special risk indicator in a report or contact the FIU directly if they believe there are grounds for issuing a restraint order.

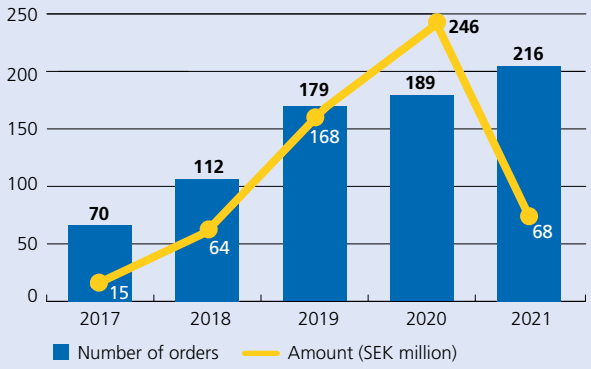
Restraint orders usually apply to assets in an account, but in 2021 the FIU also made decisions regarding assets in the form of cryptocurrencies.

In 2021, the FIU initiated more restraint orders than in previous years. In total, the FIU issued 216 restraint orders for assets worth just short of SEK 70 million, which is comparable to the level in 2018 (see graph).

Individual cases with unusually high amounts may cause deviations in the total amount, which happened in 2019 and 2020.

In addition, the FIU can forward information to ongoing investigations about the possibility to seize money, as happened in just under 70 investigations in 2021. The result of this measure may be the same as a restraint order, i.e. that proceeds of crime are no longer disposable for criminals.

Restraint orders from the FIU



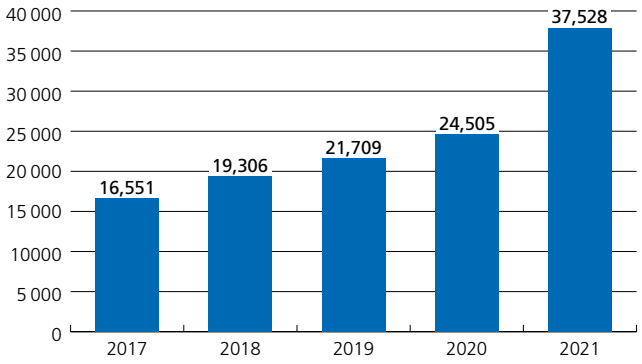
* Chapter 4, section 11, Act on Measures against Money Laundering and Terrorist Financing.

Reporting to the Financial Intelligence Unit

Under the Act on Measures against Money Laundering and Terrorist Financing, some types of entities are obliged to report activities that are suspected to be money laundering or terrorist financing to the FIU. This obligation does not only apply to financial entities, but also other types of businesses. The reporting obligation also applies to certain government agencies, including supervisory authorities responsible for the sectors covered by anti-money laundering legislation.

The number of suspicious activity reports submitted by entities covered by the reporting obligation (obliged entities) has grown gradually in recent years and amounted to 37,528 in 2021 (see figure 2).[2] This was over 50 per cent more than in 2020 and more than double since 2017. The reports were submitted by 278 unique reporting entities, which is slightly more than in the previous year.

Figure 2. Number of submitted suspicious activity reports



2 The graph shows the number of reports from entities covered by the obligation to report suspicions of money laundering and terrorist financing. In addition to these reports, the FIU receives intelligence information from other law enforcement-agencies and from FIUs in other countries. There may also be tips from the public.

The significant increase in the number of reports in 2021 does not necessarily mean that cases of money laundering have increased correspondingly. The larger number is likely due to new technical possibilities for automated reporting. Another explanation may also be that many banks have increased the number of employees working on these tasks, putting them in a better position to detect more instances of suspected money laundering and terrorist financing.

The increasing number of reports is positive, but the number does not tell the whole story about the information value of the reports. A report may contain thorough analyses and large amounts of material, while others contain a single transaction. In addition, there are large differences in quality between the reports. A prerequisite for the FIU to be able to deal with the information is that reports are structured in the right way.

In 2020, the Swedish Police Authority changed the IT system for reporting to the FIU. After the introduction of the new system goAML, there are still a number of obliged entities that struggle with data quality in these reports. These problems cause errors in the money laundering database, which impedes the work of the FIU. Moreover, the FIU has to spend time and resources on making corrections and providing obliged entities with feedback.

While these problems persist, the growing number of reports cannot fully contribute to efforts to counter money laundering and terrorist financing. In 2021, therefore, the FIU prioritised efforts to evaluate and provide information in order to improve report quality (see the section on 'Feedback').

Table 2 on page 11 shows how the number of suspicious activity reports is spread across different categories of businesses. As in previous years, approximately two thirds of all suspicious activity reports come from banks (see figure 3). The financial sector as a whole submits 90 per cent of all reports. The gambling sector also contributes a relatively large share of the reporting, and only about 0.5 per cent of the reports come from other sectors.

Among real estate brokers, lawyers and accountants, for example, only a few obliged entities per year report suspicions to the FIU. Here, the number of reporting entities and reports needs to grow. Among operators in the financial sector, there is potential to improve the information value of the reports that are submitted.

Reasons for suspicions in 2021

Obliged entities indicate whether the reports that are submitted concern suspicions of money laundering or terrorist financing. The reports are also tagged with one or more risk indicators that show the circumstances that caused the suspicion to arise.

The vast majority of reports submitted to the FIU concern suspected money laundering. In 2021, 98 per cent of reports were about suspected money laundering, 1 per cent about suspected terrorist financing and approximately 1 per cent about suspicions of both activities.

A common risk indicator when there are suspicions of money laundering is that the customer is believed to have provided incomplete or incorrect information. Approximately one third of the reports are tagged with this indicator (see figure 4).

Obliged entities also frequently notice high-speed transactions or large turnover on the account, compared to what is known about the customer. Almost a third of the reports are tagged with one of these indicators.

Figure 3. Percentage of suspicious activity reports 2021

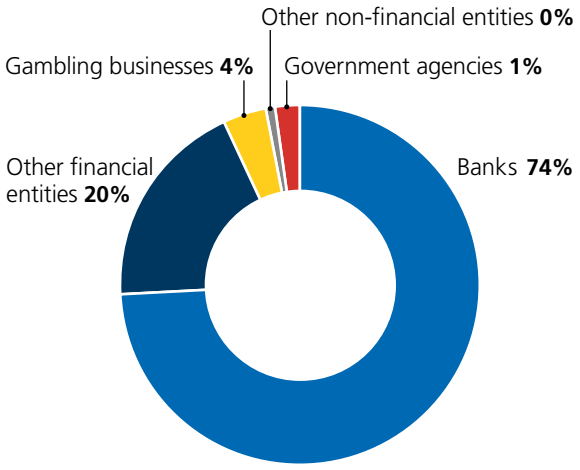
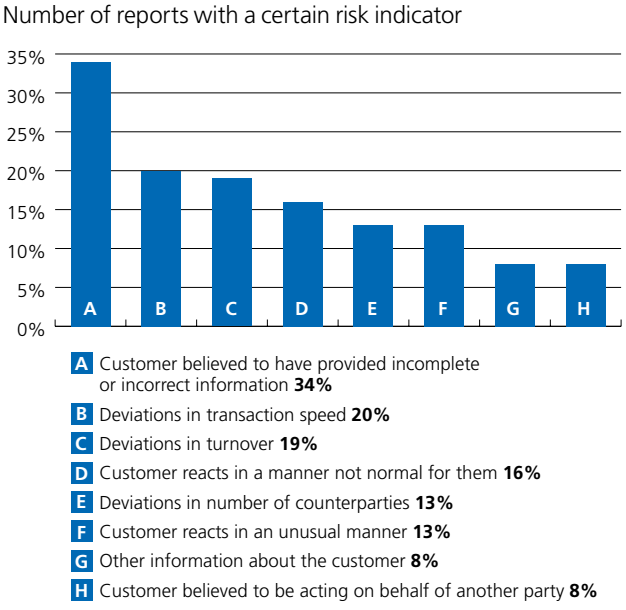


Figure 4. Most common indicators – money laundering



Suspicions of terrorist financing are usually tagged with the indicator geographic area (see figure 5). It could be an area where terrorist activities are taking place or where there is corruption, or a country that does not have efficient systems in place for countering money laundering and terrorist financing. Indicators showing insufficient 'know your customer' information are also relatively common, sometimes due to the fact that the customer is far away, making it difficult to verify the customer's identity.

Figure 5. Most common indicators – terrorist financing

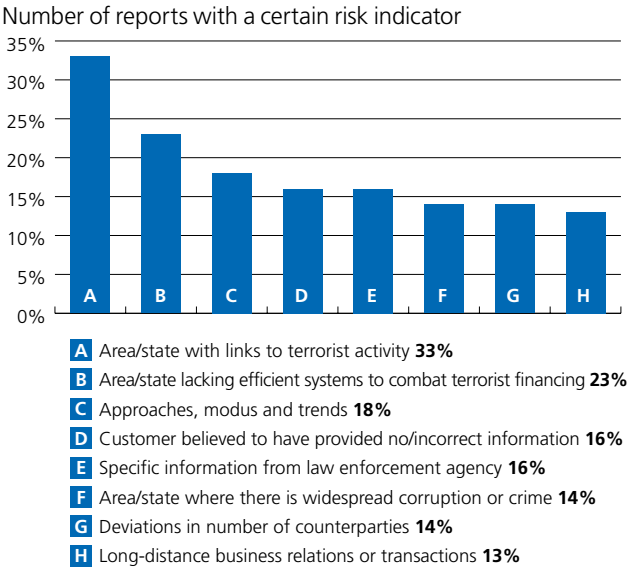


Table 2. Number of reports received per sector 2017–2021

	2017	2018	2019	2020	2021
Banking and financing institutions including credit market companies	12,169	14,421	16,831	18,342	27,801
Life insurance businesses	32	32	42	17	33
Securities businesses	..	10	19	6	4
Financial businesses with compulsory registration	27	166	493	163	383
Insurance intermediaries	..	..	..	0	1
Electronic money institutions (including reports by representatives)	35	50	39	13	4
Fund businesses including alternative investment funds	..	..	..	2	2
Payment services*	3,674	3,764	3,045	4,032	6,743
Currency exchange and deposit businesses				270	325
Consumer credit businesses	68	149	185	87	138
Mortgage credit businesses	..	..	..	12	8
Real estate agents	6	..	23	5	6
Gambling services**	381	474	481	907	1,444
Professional trade in goods***	55	37	83	122	116
Pawn shops	7	6	6	12	17
Auditing (approved or authorised public accountant or registered accounting firms)	8	7	20	8	20
Accounting or auditing services (excluding approved or authorised public accountants and registered accounting firms)	9	16	19	6	9
Tax advisers	..	..	..	4	0
Lawyer or junior lawyer at law firm	..	..	6	1	1
Other independent lawyers	..	..	..	0	3
Company formation, trustees etc.	..	..	..	0	0
Supervisory authorities	24	23	19	8	7
Other authority	47	133	239	488	463
TOTAL	**16,551**	**19,306**	**21,709**	**24,505**	**37,528**

.. indicates that the sector submitted five or fewer reports during the year. 2020 actual numbers are given.

* From 2015 to 2019, the category Payment services included payment institutions and registered payment service providers, including currency exchange. Starting in 2020, currency exchange and deposit businesses were lifted out to form a separate category.

** Gambling services were included in the Act on Measures against Money Laundering and Terrorist Financing on 1 August 2017.

*** The category professional trade in goods includes auction centres and companies trading in vehicles, scrap metals, precious stones, antiquities and art with a value that exceeds EUR 5,000. Until 1 August 2017 the limit was EUR 15,000.

Money laundering 2021

In 2021, currency exchange was a prioritised area for the FIU's efforts to counter money laundering. One reason for this is the content of decrypted chats (Encrochat, Sky ECC and Anom), which gave new insights into money laundering and the handling of proceeds from organised crime. This material showed that currency exchange has a key function in the smuggling of drugs into Sweden.

This chapter describes some of the FIU's anti-money laundering activities during 2021. In addition to currency exchange, the FIU handled many other types of cases, such as money laundering using cryptocurrency, money mules, insiders and other enablers, as well as companies that are controlled by criminal networks.

The FIU also produced in-depth analyses of various phenomena and modi operandi. One area for analysis was the use of cryptocurrencies, with intelligence indicating increased interest among criminals. Another area of analysis was money laundering connected to fraud. Approximately one fifth of all money laundering reports concern suspicions that the money derives from fraud.

Money laundering through 'neobanks' was another area of in-depth analysis, due to the fact that such entities are becoming increasingly common. The areas of analysis are described in detail in the sections below.

The FIU also contributed to a national risk assessment of money laundering and terrorist financing, which was published during the year.

This is money laundering

The opportunity to make money is the major incentive behind organised crime. In order to use their proceeds from crime in the legal economy, criminals need to launder them. Normally, money laundering is performed through a series of transactions where the proceeds of crime pass through various owners and change form. They may also be divided into smaller portions. Money launderers sometimes use what are called 'enablers'. These enablers may have expert skills or offer services that are needed in the money laundering schemes. The methods vary, but usually follow the steps described here.

It is worth noting that all proceeds of crime are not laundered. Some are consumed without being laundered and others are reinvested in criminal activities. There is also 'reverse laundering' where legitimate money is turned dirty, for example in order to pay undeclared wages.

PLACEMENT

The aim of placement is to make the proceeds of crime enter the financial system, for example through cash deposits or the buying and selling of goods.

LAYERING

Layering takes place through various transactions intended to hide the traces between the origin and final destination of the money. Often, the money is moved in several stages in order to reduce the risk of detection.

INTEGRATION

The last stage is to integrate the money in the legal economy. This may take the form of day-to-day expenses or investments in real estate and companies.

Operations

As mentioned above, currency exchange and currency transfers from Sweden were one of the focus areas for operational efforts during 2021. The FIU cooperated with other law enforcement agencies and also conducted operations of its own that led to police reports. In addition, the FIU sent background material to the Swedish Financial Supervisory Authority to assist in its supervision of bureaux de change.

> In 2021, currency exchange was a prioritised area for the FIU's efforts to counter money laundering.

The operational intelligence work of the FIU covers many different areas. The list below shows some examples of cases during 2021. It should be noted that this work was performed at the intelligence stage, and the cases did not necessarily result in the launch of a preliminary investigation or a prosecution.

- Gathering of financial intelligence on a travel agency in a Vulnerable Area resulted in the filing of a police report on a gross money laundering offence. Large amounts of cash were seized during the search of the travel agency's premises.
- Money mules linked to an international criminal network with roots in Central Asia were arrested at Arlanda Airport carrying large sums of cash. The FIU went on to identify the companies that these individuals could be linked to, in order to build the money laundering case.
- A Swedish individual living in another European country was suspected of enabling money laundering of proceeds of crime through cryptocurrency transactions. The FIU cooperated with the police in another country in the case.
- The FIU gathered financial intelligence due to suspicions of corruption during a public procurement process.
- An audit of suspicious transactions linked to fund-raising made it possible for the FIU to identify individuals who may be linked to terrorist financing.
- A lawyer was suspected of acting as an enabler of money laundering by letting criminals use his escrow account to process the proceeds of crime.
- The FIU closely studied a wholesale drug dealer who was identified in decrypted chats and found that proceeds of crime had been invested in real estate.
- Indications of money laundering at a sports club turned into suspicions directed at individuals close to the club who are linked to a criminal family network.
- The FIU noted an increase in the number of reports on credit fraud, with some companies featuring recurrently as instruments of fraud. A preliminary investigation was launched, resulting in a conviction.

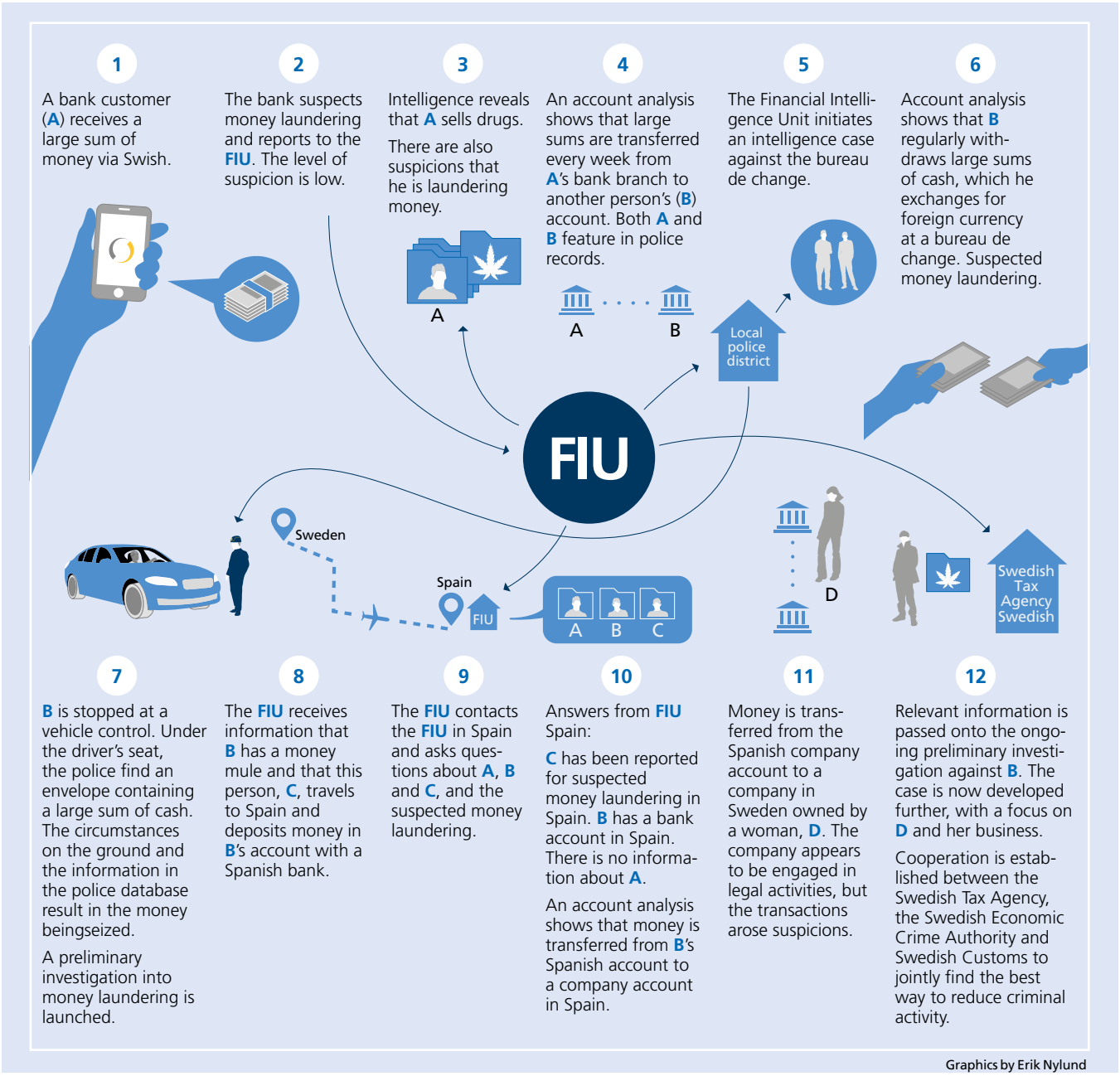
Example of an operational case in 2021

Some cases are of a simple nature, while more complicated cases may run over a long period of time and involve many different cooperation partners in several countries. The illustration on the next page shows examples of the steps that may have to be taken in more complex cases, and how the operations of the FIU may be of use.

The case was initiated when a bank was contacted by a real estate agent during the purchase of an apartment. The bank reacted to the fact that the client had significantly more money in their account than previously. The bank investigated the reasons for this, but was unable to ascertain the origins of the money and submitted a money laundering report to the FIU.

The data was processed and information exchanged between various parts of the Swedish Police Authority as well as a foreign FIU, which revealed new information about another operator and a company that was suspected of money laundering.

Illustration of an example of an operational case



As the example shows, the path from information to action is not always as straight as in the schematic on page 6. The case also highlights the fact that a single report may turn into an important piece of the puzzle, contributing to more than just the initial suspicion.

Currency exchangers as enablers

Currency exchange businesses provide an important channel for criminals' money laundering and illegal handling of proceeds of crime. In 2021, the FIU analysed how illegal currency exchange was exploited to launder money and how targeted efforts can have an impact.

The analysis shows that currency exchangers engaging in criminal activity often function as important links in serious and organised crime. Drug trafficking is frequently the primary source of the proceeds of crime, but other types of crime also occur in this context, such as human smuggling, terrorist activities and the exploitation of undeclared labour.

Currency exchangers can be criminal individuals acting without a formal business, criminal bureaux de change with a legitimate façade, informal payment systems or representatives for money transfers. In addition to commercial money laundering, these businesses are often involved in other types of financial crime such as accounting offences and tax offences.

Today, it is relatively simple to start and register a seemingly legitimate currency exchange business. This fact may be exploited by criminals and other enablers, who are able to launder millions of SEK through such businesses.

> It is obvious that access to illegal currency exchange is vital for large-scale drug trafficking in Sweden.

In its analysis, the FIU considers these businesses to be central enablers of money laundering. The operators are important platforms for criminals' currency exchanges but also for the export of cash originating from crime, i.e. courier activities. These usually concern transports of cash originating from serious crime.

A previous analysis of the decrypted Encrochat platform estimated that the annual turnover from drug trafficking in Sweden at the wholesale level is approximately SEK 12 billion. Large amounts are thought to be exported from Sweden to be reinvested in new drugs consignments abroad. It is obvious that access to illegal currency exchange is vital for large-scale drug trafficking in Sweden.

In 2021, law enforcement agencies conducted successful operations. Close cooperation between government agencies has resulted in the shutting down of criminal currency exchange businesses. This is thought to have temporarily reduced the ability of criminals to launder and handle proceeds of crime.

Money laundering through cryptocurrencies

In 2021, the FIU improved its capabilities to counter money laundering and terrorist financing via cryptocurrencies, for example through training, analysis and cooperation.

Reports of suspicious transactions in cryptocurrencies continued to increase in 2021. Suspicious activity reports were submitted from banks as well as obliged entities in the cryptocurrency sector, with the latter submitting approximately a quarter of the reports.

Common reasons for suspicions are that the customer has a level of turnover that deviates from the norm and that the customer is assumed to be acting on behalf of someone else. In the reports from banks, the single most common suspicion is that the money originates from fraud. Suspicions of cryptocurrencies being used to pay for illegal goods and services are also common.

Illegal crypto-exchangers are a challenge in the fight against organised crime as they function as enablers of money laundering for criminals and networks. There is a link between serious organised crime and individuals reported for cryptocurrency transactions. Almost one third of these individuals feature in other intelligence concerning serious organised crime – primarily involving drugs, weapons and violence, money laundering, systematic profit-driven crime and fraud.

> There is a link between serious organised crime and individuals reported for cryptocurrency transactions.

The use of cryptocurrencies and crypto-assets is on the rise and the market is constantly evolving. This, combined with a keen interest in cryptocurrencies on the part of criminals, means that it is extremely important for both government agencies and obliged entities to have a good level of knowledge and to cooperate. As the trade in cryptocurrencies takes place at international level, cross-border cooperation is a prerequisite for combating money laundering using cryptocurrencies.

Crime proceeds from fraud

Approximately one in every five money laundering reports sent to the FIU is about suspicions of money originating from fraud. Fraud is also by far the most frequent type of criminal activity recorded in convictions related to money laundering. This is partly because in simpler fraud schemes it is often relatively straightforward to verify that the money comes from a crime as it is possible to see which

accounts and account holders have been involved in a transaction.

In 2021, the FIU conducted an analysis of what the reports say about how crime proceeds are handled.[3] The analysis reveals that the individuals involved are often engaged in multiple criminal activity and that there is a major risk of proceeds from fraud being reinvested in other serious crime involving drugs, weapons and violence, for example.

The analysis also shows that there are structural differences between criminals committing various types of fraud, in terms of financial capacity, organisational capabilities and capacity for violence. The size of crime proceeds also varies, as does the extent to which money laundering is detected and reported.

The dark numbers and the actual scale are both thought to be particularly large when it comes to VAT and welfare fraud. Despite the fact that few such suspicious activity reports were received, the transactions that were reported amounted to hundreds of millions of SEK in the space of one year.

> The analysis reveals that there are often multicriminals involved and that there is a major risk of proceeds from fraud being reinvested in other crime.

The FIU has compared different types of fraud based on an estimate of the size of crime proceeds, the criminals' capacity and the risk of the money being reinvested in organised crime. On the basis of this, VAT and welfare fraud are considered to pose the biggest threat. They generate billions each year – money that can be reinvested in other crime. The criminals involved have high financial and organisational capacity and clear links to serious organised crime.

BEC fraud[4], loan fraud and vishing fraud[5] also pose a serious threat from a crime proceeds perspective, but for slightly different reasons. BEC fraud is behind a considerable proportion of the reports received by the FIU. Money laundering is thought to be widespread and the organisers can in many cases be linked to international criminal networks.

Loan fraud also amounts to quite a large sum. This fraud enables individuals involved in serious crime to access crime proceeds by owning property and also creating incentives for the recruitment of enablers, such as insiders at banks.

Vishing fraud generates relatively smaller sums, but it is the type of fraud for which the largest proportion of individuals reported for suspicious activity have links to other crime and criminal networks. Vishing is believed to be an important source of income for organised crime in Sweden.

There are a number of vulnerabilities that need to be addressed in order to make it more difficult to obtain and launder crime proceeds from fraud. This includes strengthening the capacity of banks and other obliged entities to detect and prevent fraud before it happens, and – with regard to VAT and welfare fraud – increasing checks on the part of government agencies that pay money.

Some possible measures to reduce vulnerabilities include:

- Systematic monitoring of transactions on tax accounts, with a focus on the risk of money laundering, on the part of the Swedish Tax Agency and obliged entities.
- A higher level of customer adaptation in the monitoring of transactions on company accounts.
- Technical solutions enabling banks to detect and stop transactions from BEC fraud before they are carried out.
- Stronger controls of identity and salary documents in connection with the granting of credits in order to reduce the risk of loan fraud.

3 See the report (in Swedish) by the FIU https://polisen.se/contentassets/ecf-43d8a5243446abae- 6aa441dbd574e/bedragerier-och-penningtvatt.pdf

4 BEC (business email compromise) is when the fraudster sends an email claiming to be from someone else in order to induce an employee of a company to carry out transactions.

5 Vishing is when a perpetrator contacts someone by telephone and claims to be an employee at the victim's bank for example. They then induce the victim to perform an action that provides the fraudster with financial gain.

Neobanks exploited for money laundering

The growth of 'neobanks' has increased in recent years.[6] Neobanks enable fast cross-border transactions, making them attractive to criminals wanting to launder dirty money or finance serious crime, such as terrorism. Criminals can also exploit accounts with neobanks to act anonymously and make purchases or payments using cryptocurrencies.

For this reason, the FIU decided in 2021 to initiate an analysis of the risks and methods of money laundering and terrorist financing via neobanks. This analysis confirms the suspicion that neobanks are used for money laundering, for example in the form of layering so as to conceal the fact that money originates from criminal activity.

Intelligence indicates that criminals are frequent users of neobanks. Almost 40 per cent of the people reported for suspicious transactions to or from accounts with neobanks also feature in other intelligence about serious organised crime.

> Intelligence indicates that criminals are frequent users of neobanks.

The analysis indicates that criminal operators who launder money via neobanks to a large extent encounter the same criminal groups that pose a threat in Vulnerable Areas and Particularly Vulnerable Areas with strong links to drug-related and violent crime.

National risk assessment 2020/2021

In April 2021, the coordination function for the prevention of money laundering and terrorist financing[7] published a new national risk assessment. The report was based on extensive efforts that were initiated more than a year earlier. The FIU dedicated various resources to the project and contributed in the form of methods development, analysis and composing the report.

The risk assessment was based on the 22 different sectors governed by Swedish anti-money laundering legislation. Based on a survey of threats and vulnerabilities, an assessment was made of the risk that a certain sector would be exploited for money laundering or terrorist financing.

The risks were then compared in a national context from the perspective of the possible impact on society. For money laundering, a quantitative assessment was made using a four-level scale, while the assessment of risks for terrorist financing was only made qualitatively.

For the financial sector, the risk of money laundering was considered highest for banks and financial institutions. Banks represent the basic financial infrastructure and more or less all money that is laundered needs to pass through the banking system at some stage. Financial institutions are also exposed to major risks, in particular bureaux de change and the unregulated trade in virtual currencies.

Outside the financial sector, threats and vulnerabilities were considered to be highest in the goods retail sector. Cash purchases of luxury goods are anonymous up to certain amounts, and criminals do not need any special skills to launder money.

Gambling companies and real estate agents are other examples of sectors that are at risk of being exploited for money laundering that goes unnoticed by the businesses as well as the banks involved. The gambling market was considered to have the highest threat level due to its high accessibility and the possibilities to turn over relatively large amounts in a short period of time.

A more detailed description of the threat and vulnerability analysis and impact assessment, as well as proposals for risk reduction measures, can be found in the report *National risk assessment of money laundering and terrorist financing in Sweden 2020/2021*.[8]

6 The term 'neobank' is not a legal term. The meaning is a 'new bank', with 'neo' meaning new or modified in Latin. A neobank can most simply be described as a digital bank where the user can perform all services using a mobile app or a web interface. Neobanks can offer many of the products and services that traditional banks offer, but they do not have to be banks in the formal sense, with a banking licence; instead they can be a financial institution or an e-money service provider.

7 The Swedish Police Authority heads a national coordination function for the prevention of money laundering and terrorist financing. The function consists of representatives from 17 organisations, including law enforcement agencies and supervisory authorities.

8 https://polisen.se/contentassets/a7aeda235652476b829488438e4aed8f/national-risk-assessment-of-money-laundering-and-terrorist-financing-in-sweden_.pdf

Terrorist financing

Over the course of the year, the FIU ran several intelligence operations concerning terrorist financing. These operations concerned phenomena ranging from suspected terrorist financing with cryptocurrencies to cash transfers using money mules.

Unlike money laundering, where the objective is to hide the criminal origin of the money, terrorist financing is about hiding the purpose and thus the destination of the money. No other offence need precede the financing therefore. Many terrorist attacks have been financed with relatively small, sometimes legitimate, amounts of money.

These operations concerned phenomena ranging from suspected terrorist financing with cryptocurrencies to cash transfers using money mules.

Though some terrorist attacks during the last few years did not require specialist skills or large amounts of money, terrorist organisations do have a need for money for infrastructure, recruitment, propaganda and operations.

The following are some of the conclusions from the FIU's intelligence work against terrorist financing:

- Terrorist financing has taken place in Sweden for decades but it increased markedly from 2015, likely due to the refugee crisis caused by the civil war in Syria.
- Sweden is mainly a sending country, i.e. money is collected in Sweden and moved abroad for direct or indirect financing of terrorist activities. However, money is sometimes also imported to Sweden to finance radicalisation efforts.
- Terrorist financing is thought to be more common in violent Islamic extremist circles than in other violent extremist circles.
- All violent extremist movements have the ability to use cryptocurrencies to raise funds from members or individuals. In some cases, such fundraising takes place under false pretences, for example charity donations.
- When IS in Syria and Iraq had become a less significant actor, the FIU instead focused on trying to find money flows to other countries where terrorist organisations are active.
- Sectors with a particularly high risk of terrorist financing are registered payment service providers and money transfer agents. Unregistered Hawala agents[9], generally unknown to the authorities, are also considered a high-risk sector.

9 Agents who act as middlemen for transactions through informal payment systems. The system works by middlemen all over the world guaranteeing specific amounts for their clients. These amounts may then be transferred to another individual at a completely different location by means of cash deposits and withdrawals with local middlemen. The middlemen then settle their accounts at an aggregate level.

Feedback

Providing feedback to obliged entities is a part of the FIU's task. This can be done in various ways and in a number of forums. A main focus during 2021 was to provide feedback on the data quality in reports from obliged entities. It is vital for the FIU's work that the information in the reports is entered correctly.

Seemingly simple errors, such as an account number being entered in the wrong format, make it much more difficult to link the information in the money laundering database. This directly affects the further analysis of the information and the chances of taking operational measures, such as restraint orders, and also sharing the information. Due to this, it is necessary to ensure the data quality of the reports.

Focus on data quality in reports

A report that does not meet basic requirements is rejected and the reporting entity needs to correct or supplement the report and submit it again. When necessary, a discussion is held with the reporting entity to clarify the report.

Reports from obliged entities considered to have a good basic level in their reporting are automatically approved. These reporting entities are provided with general feedback on their reports, if needed. In 2021, a large initiative was carried out in which approximately 40 obliged entities' reports were reviewed and compared with a basic standard during a set period of time. Material containing the overall feedback was then sent to the obliged entities. In several cases, meetings were held to clarify certain points and issues.

Ensuring data quality and providing overall feedback is time-consuming work for the FIU and obliged entities, but it is essential for making the information useful. The FIU needs higher-quality reporting to be able to analyse clusters, see links between networks and detect when proceeds of crime are layered. In this way, it is possible to turn more information into operational reports that can be shared with other parts of the Swedish Police Authority or other law enforcement agencies, such as the Swedish Economic Crime Authority or the Swedish Security Service. This can later result in a conviction or an administrative measure that helps to counter money laundering and terrorist financing.

Seemingly simple errors, such as an account number being entered in the wrong format, make it much more difficult to link the information in the money laundering database.

Feedback on risks and methods

Another way of providing feedback is to give information about current methods and trends, as well as the risks that may exist for a certain payment method or in a particular sector. The aim of this type of feedback is to help obliged entities detect suspected money laundering or terrorist financing in a systematic way, and stop suspicious transactions at an early stage. This kind of more general feedback is given in various forms, such as in mail-outs or industry- or subject-specific reports.

The FIU also provides training and takes part in seminars, information meetings and trade fairs. In 2021, the FIU participated in:

- Lectures on the risk of money laundering in the gambling sector held in various forums arranged by the Swedish Gambling Authority and trade associations.
- Training initiatives on money laundering together with other government agencies, including the Swedish Financial Supervisory Authority.
- Training for the banking sector and real estate sector through their trade associations.
- Seminars for obliged entities under the supervision of the county administrative boards.
- Lectures held for a number of government agencies that participate in the coordination function for the prevention of money laundering and terrorist financing, including the Swedish Inspectorate of Auditors.

Strategic and operational cooperation

In 2021, the FIU developed its cooperation with national and international partners in a way that yielded positive results for law enforcement. The FIU was able to continue analysing information from encrypted chats, such as Sky ECC, Anom and Encrochat, that was collected by the Intelligence Division in cooperation with other EU countries and the United States. This resulted in continued success in efforts to combat organised crime, as a large number of individuals from criminal networks were sentenced in Swedish courts and key individuals could be identified.

The coordination function for the prevention of money laundering and terrorist financing published a national risk assessment based on the sectors covered by money laundering legislation.[10] The FIU played a leading role in the production of the risk assessment and took part in training to increase knowledge and risk awareness among obliged entities in the sectors that are considered to have the greatest risks.

In 2020, new forms of cooperation were initiated with the five largest banks in Sweden. This cooperation is now of a more permanent character and has been expanded to form a new group with a more strategic focus (see the section on SAMLIT below).

The ongoing dialogue that was initiated last year with the Swedish Financial Supervisory Authority was also strengthened. By way of special agreement[11], the FIU has been able to share more tangible data to help the Swedish Financial Supervisory Authority improve its efforts vis-à-vis sectors where risks have been found.

Internationally, the FIU continued its work in various strategic forums, including the global organisation Financial Action Task Force (FATF)[12]. Meetings were held virtually this year as well due to the pandemic. The FATF's work has resulted in the adoption of a document on best practices for freezing of assets and a new guide on cryptocurrencies and 'Crypto Asset Service Providers'. The organisation has also decided to strengthen its recommendation to member states on available information in databases of individuals or companies that are the real owners of companies, known as beneficial owners.

In summer 2021, the European Commission presented a major legislation package against money laundering and terrorist financing. The FIU participated actively in a working group in the EU forum FIU Platform, working with other FIUs from the EU. Efforts were made to monitor and try to influence the EU legal acts that were negotiated between the EU institutions. The FIU also supported the Government Offices with expert knowledge in the same field. In other international forums, such as the Egmont Group[13], activities have been limited due to the pandemic.

10 See also 'National risk assessment 2020/2021' in the section on money laundering.
11 Agreement based on the Act on the Obligation to Provide Information in the Context of Cooperation against Certain Types of Organised Crime (2016:774).
12 The Financial Action Task Force is an association of approximately 40 countries and regional sub-organisations. The FATF issues recommendations on how to counter money laundering and terrorist financing and also evaluates countries on the basis of these recommendations.
13 Egmont is an organisation for 166 FIUs that enables the secure exchange of information, experience and training to counter money laundering and terrorist financing.

In the course of the year, the FIU strengthened its general cooperation with Europol through information dissemination in the area of money laundering. During the second half of 2021, cooperation with Europol focused on links to cash exports and a new Europol working group for economic and financial crime from a wider perspective.

The FIU in SAMLIT 2021

SAMLIT, the Swedish Anti-Money Laundering Intelligence Taskforce, is an initiative that was launched in 2020 in which the Swedish Police Authority and the five largest banks in Sweden cooperate. The aim is to improve efforts to combat money laundering and terrorist financing. The Swedish Police Authority is represented by the Intelligence Division at the National Operations Department, and the five participating banks are Danske Bank, Handelsbanken, Nordea, SEB and Swedbank.

> During the year, the group worked on twelve cases and more will be initiated in 2022.

The legal basis for the exchange of information is the banks' obligation to provide, at the request of the Swedish Police Authority, all information necessary to investigate money laundering or terrorist financing. Given its task to combat money laundering and terrorist financing, the FIU played a central role in contact and cooperation with the banks.

In 2021, SAMLIT consisted of two groups, one operational group (the Operative Intelligence Group, OIG) and a pilot group with a strategic focus (the Strategic Intelligence Group, SIG).

Within the OIG, the Swedish Police Authority and the banks cooperate on cases concerning suspected criminal individuals and companies. During the year, the group worked on twelve cases and more will be initiated in 2022.

In 2021, the strategic group (SIG) was launched. SIG initiated various pilot projects that will continue during the course of 2022. Among these was a forum for exchanging knowledge and sharing information on risks, modi operandi and trends etc. The group also developed methods to implement common analysis projects of a strategic character. The purpose of such analyses is to improve knowledge of certain phenomena or identify new methods. The aim is to share the knowledge that the group generates with a target group outside the forum itself.

SAMLIT produced good results in both of the groups during 2021 and the forum is appreciated by both the banks and the Swedish Police Authority.

New legislation in 2021

In recent years, legislation on money laundering has developed rapidly. An important reason is the need to counter the risks that follow from new types of businesses.

In 2021, the Act on Measures against Money Laundering and Terrorist Financing was expanded to include real estate agents' companies, instead of just individual real estate agents. This change means that Swedish legislation corresponds better to the requirements in the fourth Anti-Money Laundering Directive[14]. Another amendment was that real estate agents and real estate agents' companies with a special registration for brokering rental properties are now included as obliged entities in the Act on Measures against Money Laundering and Terrorist Financing.[15]

Crowdfunding service providers[16] were also included as obliged entities in a legal sense through an amendment in 2021. The amendment concerns legal persons established in Sweden that conduct businesses in accordance with the EU regulation on crowdfunding.[17]

Suggested further measures

During the year, the results of a number of inquiries were presented, with the aim of further strengthening the legislative framework.

In February 2021, a memorandum[18] was presented that contains proposals for implementing the EU directive on financial information[19]. The memorandum includes proposals on additional government agencies that are to be given access to information on holders of accounts and safe deposit boxes at institutions through the 'Mechanism' (see fact box).

In addition, there are proposals on how to bring about an increased exchange of financial information to enable certain government agencies to request and access financial information and analyses from the FIU to a greater extent. It is proposed that these legislative amendments enter into force on 1 July 2022.

> The Mechanism can provide considerable efficiency gains and help to prevent the financial system from being exploited for money laundering or terrorist financing.

In May 2021, the Inquiry on strengthened measures against money laundering and terrorist financing[20] presented its final report to the Government. One issue that the Inquiry looked into was the possibility of greater information exchange between government agencies and obliged entities. This is an area of particular importance for the work of the FIU (see the section about SAMLIT).

The Inquiry noted that provisions on secrecy and other confidentiality are a hindrance to the information exchange that is needed. The Inquiry therefore proposes that it be possible to make separate decisions on cooperation for the purpose of taking measures against money laundering and terrorism financing. Within this kind of cooperation, information that is subject to secrecy or other confidentiality could be exchanged using an obligation to provide information. The Swedish Police Authority takes a positive view of the Inquiry's proposals.

14 Directive (EU) 2015/849 of the European Parliament and of the Council.
15 The various forms of registration are explained in the Real Estate Agent Act (2015:516).
16 Crowdfunding is a financing method where small amounts are raised from a large number of individuals or companies.
17 Regulation (EU) 2020/1503 of the European Parliament and of the Council.
18 Ds 2021:5
19 Directive (EU) 2019/1153 of the European Parliament and of the Council.
20 SOU 2021:42

The Inquiry also proposes, in line with a request by the Swedish Police Authority[21], the introduction of a reporting obligation and an obligation to provide information for certain entities that are not obliged entities within the meaning of the Act on Measures against Money Laundering and Terrorist Financing.

An obligation to provide information means that a business operator must, *at the request* of the Swedish Police Authority or the Swedish Security Service, provide without delay the information needed for an investigation into money laundering or terrorist financing.

The Inquiry proposes that the obligation to provide information be expanded to cover credit check companies, those with a permit to conduct clearing activities[22] and those that provide obliged entities with electronic ID services or a service for the mobile transfer of money where the transfer takes place immediately.

The reporting obligation means that an actor who has *detected a circumstance* that can be assumed to have a link to or actually be money laundering or terrorist financing must inform the FIU of this without delay.

It has been proposed that the reporting obligation, which will become a new provision in the Act on Measures against Money Laundering and Terrorist Financing, should cover those with a permit to conduct clearing activities.

What is the Mechanism?

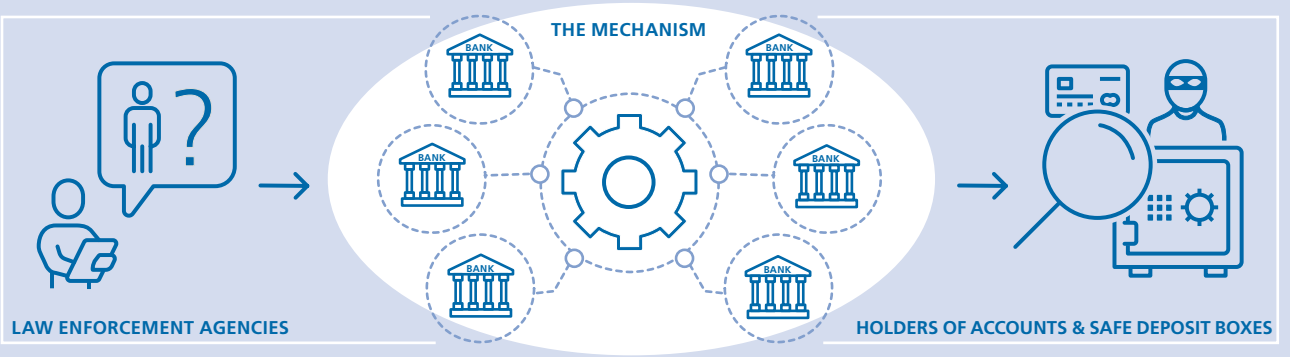
In 2021, the Mechanism was launched as a new system for information about holders of accounts and safe deposit boxes. The background to this is an act that entered into force in 2020. Under the Act on Account and Safe Deposit Box Systems (2020:272), information about holders of accounts and safe deposit boxes must be directly and immediately searchable on a technical platform administered by the Swedish Tax Agency.

The Mechanism enables the Swedish Police Authority and other law enforcement agencies to quickly find out where people and companies have accounts and safe deposit boxes. Previously, this information had to be obtained by sending specific requests to individual financial companies.

The Mechanism can provide considerable efficiency gains and help to prevent the financial system from being exploited for money laundering or terrorist financing.

However, to harness this level of efficiency, all of the institutes covered by the regulatory framework have to join the Mechanism. At the end of 2021, the technical platform had been launched but only a few institutes were linked up to it and the Swedish Police Authority had not yet had the opportunity to join the system.

The operational use of this tool will therefore not become apparent until this year, as more institutes join the platform and the Swedish Police Authority is able to conduct searches.



21 Request for legal review, ref. no. A540.680/2018.

22 Those who have a permit under section 3 of the Credit Information Act (1973:1173) and Chapter 19 of the Securities Market Act (2007:528).

Questions and answers

What happens when a report is submitted to the FIU?

When the FIU receives a report, the report is assessed along with other information that is available to the FIU. The information may be processed and shared with entities outside the FIU to aid them in their work.

It may also be investigated further within the FIU. Further information is obtained from various sources, which may result in the information being shared with partners or the filing of a police report. Many reports are not used at first, but they are saved in the money laundering database to be used again if important new information is received.

When do we report to the FIU, and what does "reasonable grounds for suspicion" really mean?

The assessment of whether to report to the FIU must be based on the business operator's 'know your customer' information and risk assessments. The level of suspicion required for reporting to the FIU is low. The legislation refers to transactions and behaviour that deviate from what the business operator may reasonably expect, considering its 'know your customer' information and the products and services it provides. Activities and transactions that do not deviate from the norm, but that may be presumed to be part of money laundering or terrorist financing activities should also be reported.

Are we allowed to tell anyone that we have submitted a report to the FIU?

No. Chapter 4, section 9 of the Act on Measures against Money Laundering and Terrorist Financing (2017:630) states that obliged entities that submit reports are bound by professional secrecy and are not allowed to disclose, to the customer or any third party, that a report has been submitted to the FIU. However, this information may be shared with supervisory authorities and law enforcement agencies, among others, and in certain circumstances within the group and with other obliged entities that are involved in the same transaction with the same customer.

Do we report everything that deviates or that we do not understand?

The starting point is that the business operator is supposed to have enough 'know your customer' information to understand transactions and behaviour. In cases of transactions or behaviour that are not understood, the first thing to do is to enhance 'know your customer' measures. That may lead to the suspicions being dismissed, in which case they should not be reported. At other times, enhanced 'know your customer' measures result in stronger suspicions, in which case they must be reported. If the assessment is made that the risk of money laundering or terrorist financing cannot be managed, the business relationship with the customer should be discontinued or, at the very least, the customer should be denied access to the services that were abused.

Another basic rule is that the reporting should be done promptly. This means that there are cases where enhanced 'know your customer' measures cannot be taken before the report has been submitted. This should then be done after the report has been submitted and should be the starting point for further measures.

Is a report to the FIU a police report?

No. A report on money laundering and a police report are not the same. The level of suspicion required for a money laundering report is lower than for a police report. Due to the low level of suspicion, the information is subject to strict confidentiality. The FIU is the only operator that has access to the information. A police report may be filed by the FIU when a report on money laundering has been processed, if there are sufficient reasons to do so.

A police report should be filed for fraud that has been completed. It is recommended that the defrauded customer does this on the police website (polisen.se/utsatt-for-brott/polisanmalan/) or alternatively by calling the police phone number 114 14. Then, the business operator submits a report on suspected money laundering as a possible consequence of the fraud. When doing so, please refer to the K number of the police report. In this way, important information from the money laundering database can be added to the preliminary investigation.

Are we supposed to report when we decide to not perform a transaction?

Yes. Chapter 4, section 3, second paragraph of the Act on Measures against Money Laundering and Terrorist Financing (2017:630) states that a report must be submitted even if the transaction was not performed. The same applies if a business relationship with a customer has been discontinued due to the risk of money laundering or terrorist financing.

Publisher
Swedish Police Authority
Production
Communications Department,
National Communications

Orders
Swedish Police Authority
Customer Service, telephone 114
Ref. no
A155.051/2022

Issue
100 copies
Printed by
Polisens Tryckeri, Stockholm,
May 2022

Graphic design
Blomquist Communication
Photos
Swedish Police Authority, Most photos,
Getty