The Financial Intelligence Unit Annual Report 2020

Polisen
Swedish Police

Swedish Police Authority

Table of Contents

Preface

As Sweden's Financial Intelligence Unit (FIU), the Swedish Police Authority has a central function in the fight against money laundering and terrorist financing. In 2020 many important steps were taken to streamline and improve the work. A new IT system was introduced, which has led to a new way of reporting suspected transactions to the FIU. Furthermore, an agreement was signed with the Swedish Financial Supervisory Authority on in-depth strategic and operational cooperation projects that aim to increase exchange of information and develop more efficient supervision. During the year, cooperation with private organisations was also developed, where the pilot project SAMLIT (Swedish Anti Money Laundering Intelligence Task Force) proved its potential for joint and targeted efforts against criminal activities by following the money.

The FIU's additional resources and reinforced organization also show clear results. During 2020 the FIU received a larger number of reports on suspicious behaviour, filed more police reports and issued more restraint orders than any previous year. A larger number of reports on suspicious activity was also forwarded to the authorities concerned. Further, the FIU ran a number of cases directed at influential criminal operators that resulted in criminal investigations related to e.g. gross fraud, gross money laundering and gross commercial money laundering offences.

Improved cooperation and clear efforts in 2020 proved to be the right way forward, but much work remains to be done. Turnover and laundering of proceeds of crime will remain a central part of criminal activities. For that reason, this part of the Swedish Police Authority's law enforcement activities will be further strengthened during 2021. Through new possibilities offered by legislation, cooperation with other parties, strong educational efforts and improved IT support, the FIU will continue to improve its capacity and represent the hub in the fight against money laundering and terrorist financing.

Johan Olsson
Head of the National Operations Department

The tasks and activities of the Financial Intelligence Unit

The Financial Intelligence Unit (FIU) is a part of the Swedish Police Authority's intelligence service and is assigned to the National Operations Department. This means that our activities focus on the early stages in cases of potential organised crime, specifically suspected money laundering or terrorist financing.

All the activities of the FIU comply with national legislation and international regulations. Guidelines from the police management form the basis for priorities when tips and requests or reports on suspicious transactions are brought to the FIU's attention. As an intelligence service, an important task is to detect trends that may influence other police activities or pose significant risks to society as concerns money laundering and terrorist financing. We provide early warnings within a well-defined but large area of operations.

The information that serves as the basis for our work comes from operators that are obliged to report transactions in accordance with the Act on Measures against Money Laundering and Terrorism Financing (2017:630). They include for instance banks and insurance businesses as well as various credit and payment services. Information may also derive from other intelligence sources.

Due to its assigned mission, the FIU can not prioritise either operational activities or overarching strategies, analyses and cooperation projects. We must do both. This means that reports on suspicious transactions that we receive need to be handled at the operational level, while at the same time strategic analyses on money laundering and terrorist financing need to be produced for a wider audience.

At the moment, the FIU employs around 45 people. The FIU consists of four groups with police officers and civilian employees. Employees have diverse educational backgrounds with experience from both government authorities and private businesses.

The FIU must adhere to a number of laws and regulations. The regulatory framework states that the FIU is a part of the Swedish Police Authority, but also that access to the money laundering register is restricted to employees at the FIU. The FIU must be independent in receiving, analysing and disseminating information in its area of responsibility.

However, being independent does not mean acting alone – legislative developments are rather about increased exchange of information, improved cooperation and more efficient routines.

The Financial Intelligence Unit in 2020

2020 was an intense year for the FIU. New functions were created and new competencies recruited for all functions; at the same time, a completely new IT system was launched for reporting by business operators and supervisory authorities. In addition, the Swedish Police Authority and five banks in Sweden initiated a project to improve operational coordination, and the Black Wallet project[1] broke new ground in the fintech sector.

Reporting on suspicious transactions show an increase of 13 percent compared to 2019, despite the difficulties associated with introducing new systems. In 2020 the FIU issued more restraint orders than any previous year, and the number of police reports filed more than doubled compared to the previous year.

Sector-specific analytical reports were written on money laundering through gambling, real estate and payment services agents. In addition, an in-depth analysis was made on how money is handled by serious organised crime related to drugs based on the contents of the Encrochat communication service. There are summaries of these analyses in the chapter on money laundering. The FIU also contributed to the national risk assessment for money laundering and terrorist financing, which was completed in the spring of 2021.

The FIU is tasked with performing independent reviews of the information that, by law, is exclusive to the FIU, but at the same time its operations are subject to review just like other parts of the Swedish Police Authority and its intelligence activities. The information processing of the FIU was reviewed in various ways in 2020. On the one hand, the Swedish Commission on Security and Integrity Protection reviewed the processing of personal data, and on the other hand the Council of Europe continued its review of operations that was launched in 2019.

> "The Financial Intelligence Unit ran a number of cases involving influential criminals and their inner networks, which resulted in the launch of several criminal investigations".

Operational work in the form of intelligence cases was successful in 2020. The FIU ran a number of cases involving influential criminals and their inner networks, which resulted in the launch of several criminal investigations. These investigations involved gross fraud, gross money laundering and gross commercial money laundering. The FIU played a central part in those investigations.

The work directed at influential criminals and their networks also contributed to the Swedish Tax Agency and the Swedish Social Insurance Agency, among others, taking administrative measures aimed at these operators and their businesses. These measures are assessed to result in a significant reduction of capacity for the networks.

1 Black Wallet is a two-year project financed by the EU that will end in February 2021. The project aims to assist law enforcement authorities and the private sector in preventing, detecting and investigating terrorist financing and money laundering in the fintech sector. The public reports that have been published for the sector are available for download at the website of the Financial Intelligence Unit.

In its operational work, the FIU initiated measures against organised crime facilitators. Some of these are "independent" criminal operators, i.e. individuals that do not belong to a particular network but that offer specialist skills and services to other criminals. They may be specialised in laundering money, providing fake pay slips or performing other services that simplify the handling of proceeds of crime. In addition, the FIU has run several operational cases directed at facilitators in the private sector who, in their professional capacity, participate in or are used for money laundering and other forms of economic crime.

Money laundering

The first part of this chapter comments on the effects of the COVID-19 pandemic on money laundering in Sweden. Then a summary is presented of the sector-specific analyses that the FIU initiated in 2020.

The effects of the COVID-19 pandemic on money laundering

The COVID-19 outbreak has had obvious effects on crime in Sweden. New forms of fraud have appeared in connection with for example government support measures, medical equipment and COVID-19 vaccines. As regards money laundering, it is difficult to draw general conclusions about the effects of the pandemic, as the differences are large between different sectors.

However, one likely effect is that the restrictions that have at times been introduced within and outside the country's borders have limited the possibilities for using and physically moving cash.

What is money laundering?

The opportunity to make money is a strong incentive for almost all kinds of crime, in particular organised crime. To be able to use proceeds of crimes such as fraud or drug deals, criminals need to turn them into apparently legal income, i.e. the money needs to be laundered.

The methods vary, but usually follow the steps described schematically below.

It is worth noting that all proceeds of crime are not laundered. Some are consumed without laundering and others are reinvested in criminal activities. There is also so-called reverse laundering where legitimate money is turned dirty, for example in order to avoid taxation.

Money laundering takes place through various steps:

1. Proceeds of crime are invested in the financial system, for example through cash deposits or the buying and selling goods.
2. The money is layered to hide its origin. In this step, several transactions are usually carried out to reduce the risk of detection, often using mobile transfers and fintech services.
3. The money is integrated into the legal economy. Integration may take the form of day-to-day expenses or investments in real estate and companies. Another factor is intelligence information that indicates that criminals show a growing interest for cryptocurrencies. This is not a new trend but the virus outbreak may have accelerated these developments.

This may have had the effect that some criminals were forced to change their methods and to a larger extent send cash in goods transports in order to move it across borders. Another sign that physical restrictions have had an effect on money laundering is that the number of reports on suspicious activity that concern online gambling has increased compared to other forms of gambling.

In addition, the pandemic has caused know-your-customer procedures among financial businesses to change due to difficulties in conducting physical meetings. These developments are assessed to have made it easier to use other people's identities and also lowered the threshold for people who act as front men.

Money laundering through payment service agents

Money transfers through various services are developing rapidly and are assessed to be an important channel in criminal circles, for handling and laundering proceeds of crime as well as terrorist financing. A large part of these transactions are made through local payment service agents who offer money transfers in addition to other business. They may be tobacconists, minimarts, hairdressers or other businesses. It is also common for bureaux de change to offer such services. Through these agents, it is possible to send cash payments from senders to receivers without a bank account.

They often involve cross-border transaction flows that may consist of complicated chains of intermediaries and receivers.

> "There are significant money laundering risks among payment service agents".

A closer analysis of reported suspicions and other intelligence information confirms that there are significant money laundering risks among payment service agents. Poor compliance of rules regarding identity checks, as well as other issues, leads to poor traceability of the origin of the money.

Despite clear legislation there is a risk that significant flows of transactions with criminal origins go undetected.

The FIU's analysis highlights several methods for this, for example when a large number of smaller transactions are sent to several different receivers in high risk countries.

The analysis also concludes that there are payment service agents who are involved in criminal activities, particularly in money laundering and other forms of financial crime.

It is therefore likely that these act as facilitators in money laundering schemes, and that transfer services are exploited for commercial money laundering.

Due to their appeal to money launderers, payment service agents are at risk of being subjected to various forms of undue influence, such as threats and blackmail. Criminal operators often target business operators that are active in a particular geographical area. This means that payment service agents that are active in areas where criminal groups have a large impact on the local community are particularly vulnerable.

In order to counter this type of money laundering, supervisory authorities and law enforcement agencies must target the payment service industry and its agents with joint measures. This work has already begun, and will develop further in 2021.

Money laundering on the gambling market

Since 2019 there is a license-based regulation of the gambling market in Sweden, which replaces the former monopoly. Swedish and international companies may apply for a license to operate on the Swedish market. In accordance with the Anti-Money Laundering Act, licensed gambling companies have an obligation to report to the FIU.

The gambling sector is at risk for being exploited for money laundering since for example payments from gambling accounts may provide an apparently legitimate explanation to the origin of the money. The Swedish Gambling Authority assesses that the risk for money laundering is highest for gambling at state-run casinos, commercial online gambling and betting. In commercial online gambling, large amounts may be turned over fast. As regards state-run casinos and betting (through gambling agents), it is rather the possibility to turn over cash that makes these forms of gambling appealing for money laundering.

The FIU has analysed money laundering through these three forms of gambling, based on aggregated data on the individuals that have been reported for suspicious gambling behaviour. The analysis confirms that the sector is exploited for money laundering.

Some of the operators who use the gambling market to launder money can be linked to criminal groups in vulnerable areas[2] that are mainly active in drug-related and violent crime. The number of reported suspicions related to online gambling increased in 2020, while the number of reports decreased in other categories. This is likely the result of increased online gambling due to the COVID-19 pandemic.

The modus operandi vary between different forms of gambling. In online gambling, there are examples of fixed poker games where criminals transfer money to gambling accounts and intentionally lose money to a third party who is an accomplice in the scheme. The winner then transfers the money to his bank account where it is classified as gambling winnings. In betting

2 A vulnerable area is characterised by a low socioeconomic status where criminals have influence on local society.

there is sometimes match fixing, i.e. match results are manipulated. Through match fixing, it is possible to launder proceeds of crime and at the same time make them grow, as winnings are guaranteed.

More examples of modus operandi and a more thorough description of the analysis is presented in the report *Money laundering on the gambling market through online gambling, betting and state-run casinos*.[3] The report also includes proposals for ways to mitigate the risks.

Money laundering through real estate

The real estate market is likewise an appealing sector for criminals who want to launder money. For example, rental incomes can be used to explain money with an illegal origin, and loans can be paid using dirty money. Real estate deals make large-scale money laundering possible, as transactions may involve significant amounts.

In 2020 the FIU analysed how real estate agents can function or be exploited as enablers of money laundering. The analysis is based on intelligence information on real estate deals, including reports on suspicious activity in the money laundering register.

A review of the material confirms that money laundering exists on the Swedish real estate market. Despite this, reporting by real estate agents to the FIU is very limited. However, in those cases where banks report suspicious transactions involving real estate, they usually concern large amounts. This means that real estate agents sometimes either don't notice suspicious transactions or neglect to report them.

Suspicions often concern doubts about how the purchase is financed or who is really behind the deal. These things should be investigated in the know-your-customer process. Real estate agents could thus be seen as facilitators, even if they are not aware of it.

There are also suspicions that real estate agents sometimes act as active facilitators, for example by letting their escrow account be used for other things than the down payment. Another example is a sale where the amount indicated on the purchase contract is lower than the market value and the buyer instead pays a part of the price under the table.

Real estate agents are also exploited for other forms of crime. During the last year, the FIU discovered several mortgage schemes in which applications were based on false documents. These are on the one hand cases of pure fraud where there was never any intention of repaying the debt, and on the other hand cases in which criminals want to borrow money from the bank to finance purchases of houses. An example of fraud is that a front man buys a property which is then given a highly exaggerated evaluation by a real estate agent. A mortgage is then taken on the property and the individuals involved share the borrowed amount.

Available information indicates that individuals who launder money through real estate are over-represented in other forms of financial crime, which means that the economic capacity of these individuals is comparatively high. Compared to other sectors that have been analysed, it is less common that operators have suspected links to criminal networks. Also, comparatively fewer have registered addresses in vulnerable areas.

The analysis of money laundering on the Swedish real estate market is presented in its entirety in the report *Penningtvätt via fastigheter, fastighetsmäklare som möjliggörare (Money laundering through real estate, real estate agents as facilitators)*.[4]

3 See https://polisen.se/om-polisen/polisens-arbete/finanspolisen/.
4 The report is available at the website of the Financial Intelligence Unit https://polisen.se/om-polisen/polisens-arbete/finanspolisen/.

Encrochat

In the spring of 2020, French authorities and Europol managed to gain access to the contents of the encrypted communication service EncroChat. The service was used by serious organised crime to organise and distribute drugs. The Swedish police were given access to parts of the material and were able to follow influential criminal operators' crime schemes in real time, which has resulted in a large number of arrests and a number of convictions.

In addition to the operational successes, the material is an excellent source of knowledge from a strategic point of view. For the FIU, this has been a unique opportunity to study the extent of the proceeds of crime generated by drug trafficking in Sweden, as well as how these are laundered and turned over and what roles are essential in managing such proceeds of crime.

The material confirms that proceeds of crime are handled via different financial methods, which involve loans and companies to launder money and also to gain more money through deception. In addition, proceeds of crime in the form of cash are used on a parallel market where the money is turned over without obstacles, up to a relatively high level. For example, buying expensive watches to use as a means of payment for drugs, as collateral or as tradeable goods seems to be a common way of using money from crime.

Cash is the main means of payment in the drug trade. This requires access to various types of facilitators who, knowingly or unknowingly, offer illegal processing of money as a service. For example, criminals depend on currency exchange for their drug trade in other countries. The material shows a strong link between money laundering and other organised crime.


"The methods for terrorist financing change continuously."
POLIS
4,0 bar

Terrorist financing

Within the Swedish Police Authority, the FIU is responsible for ensuring that exploitation of financial businesses and other businesses for terrorist financing purposes is prevented and detected. This includes collecting, providing or receiving money that will be used to plan or perform terrorist attacks. This mission includes hindering the financing of recruitment efforts to an organisation classified as a terrorist organisation and financing of training for terrorist attacks. The Financial Intelligence Unit works closely with the Swedish Security Service on intelligence concerning terrorist financing in Sweden, but does not conduct preliminary investigations about suspected terrorist financing.

Like in previous years, terrorist financing is assessed to mainly be performed by individuals. The recipients are individuals, groups or organisations that can be linked to terrorist activities. Terrorist financing also takes place in organised form through criminal activities, running of companies, donations and fundraising. Sometimes non-profit organisations are misled by the receiver and exploited for terrorist financing. However, suspicions in such cases are not necessarily reported to the FIU, as non-profit activities are not subject to the reporting obligation.

The FIU makes the assessment that the number of platforms for financing of recruitment and radicalisation in violent Islamist circles has increased and will continue to do so as more payment services enter the market. However, the extent of terrorist financing is still at a lower level than money laundering in general.

During the year, the FIU has seen how organisations such as IS and Al-Qaida use cryptocurrencies to fund their activities to a larger extent than before. It has been revealed that Swedish operators have sent money to terrorist organisations using cryptocurrencies. The FIU believes that this method will continue to be important for terrorist financing capabilities. Exports of large amounts of cash using money mules also occur.

What does a typical case of terrorist financing look like?

The methods for terrorist financing change continuously as a consequence of new technologies or the work of law enforcement agencies. One example highlighted by the FIU in 2020 is how money flows from Sweden to the border regions between Turkey and Syria again increased. In many cases, these were small-scale transfers of cash made through an online money remittance service, or at a physical agency, to individuals who are suspected money mules or representatives for a terrorist organisation. It is likely that a part of this method is to hide the receiver's identity and the intended end-use of the money.

These money flows may be connected to the fact that people in Sweden have tried to support individuals in prison camps in Syria. Whether the money ended up in the hands of the prisoners or was used in other ways by a terrorist organisation is difficult to ascertain. For the FIU, the important part is to find out whether the initial receivers of the money from Sweden are suspected of belonging to a terrorist organisation. When reports on suspicious activities are assessed to be relevant for concerns terrorist financing, the FIU continues to process the information in various ways, on its own and in close cooperation with the Swedish Security Service.

The international work of the Financial Intelligence Unit

Money laundering and terrorist financing are offences that take place all over the world. The criminal schemes often involve transactions between various countries, inside and outside the EU, and cross-border cooperation in this area is thus a necessity.

Thanks to continuous and direct exchange of information with financial intelligence units in other countries, the FIU is able to rapidly and securely gather intelligence information about cross-border transactions and criminals. In the same way, the FIU is able to check whether criminals who are active in other countries are also present in the Swedish money laundering register to gain a complete picture.

Operational forms of cooperation includes the restraint order, which is a possibility to freeze assets that was transferred abroad in cases of suspected money laundering or terrorist financing. The FIUs is able to issue restraint orders for assets in Sweden on request from another country, and also to issue such requests to another country (see also the section on legislation on page 18). The most frequent reason for restraint orders in an international context is suspected BEC fraud (Business Email Compromise), where email conversations are hacked so that international payments are redirected to Swedish accounts.

Strategic-level cooperation aims to exchange expert knowledge on risks for money laundering or terrorist financing, as well as on effective methods for detecting, preventing and hindering these activities. In this way, the FIU is able to get early warning signals when new trends are detected in other countries. Through this cooperation, Sweden is able to influence new international regulations.

New forms of cooperation during the pandemic

The FIU is usually present at international meetings of the global organisation Financial Action Task Force (FATF)[5], but these were held with around 90 delegates in smaller, virtual versions in 2020. One focus area for the organisation in 2020 was sanctions directed at the proliferation of weapons of mass destruction. Recommendations have changed so that this is now something to be considered in risk management. The organisation also published reports on how COVID-19 has affected these types of crime, such as money laundering based on handling of goods. In addition, several projects were initiated that concern terrorist financing and a new project about the links between environmental crime and money laundering.

At the European level, the EU commission presented an extensive action plan directed at money laundering and terrorist financing. The FIU took part in a working group in a forum with other financial intelligence units of the EU called FIU Platform. The group analysed the structure and

5 FATF is an association that gathers around 40 countries and regional organisations. It is based in Paris and issues recommendations on how to counter money laundering and terrorist financing, and it also evaluates countries based on these recommendations.

the tasks for a new FIU support and coordination mechanism at the EU level. Thanks to digital meeting fora, the working group has been able to hold meetings weekly without having to travel. In other international fora, such as the Egmont Group[6], not much work has been performed due to the current situation.

6 Egmont is an organisation for 166 Financial Intelligence Units that enable secure exchange of information, experience and training to combat money laundering and terrorist financing.

goAML

After several years of preparation, the new reporting system goAML was launched on 13 January 2020. The former system was closed in mid-March 2020 and since then the FIU only accepts suspicious activity reports and responses to request through goAML. So far, more than 500 business operators have registered in the system, which is used in around 50 other countries all over the world. The system is operated by the UN and was developed especially for the purpose of reporting of suspected money laundering and terrorist financing.

One of the reasons for the change of systems is that the previous solution did not meet the standards set by FATF. A new system was necessary to provide the statistical and anaytical platform required by the FIU. The major difference is that virtually all information is now reported in a uniform manner, which gives the FIU access to more structured data and thus a far better basis for analysis and follow-up.

There have been challenges for the FIU and business operators in connection with the launch of goAML. At first, the main task was to provide assistance to business operators about the new reporting method and give feedback on reporting errors. The next step is to provide feedback about the quality of the information in the reports. goAML is designed to process structured data. Because of this, it is crucial that business operators report in a correct manner so that the FIU is able to forward the information to law enforcement agencies and other cooperation partners for further measures.

> "More than 500 business operators have registered in the system so far."

Business operators who make frequent reports have the possibility to automatise the process using XML files, while those who make infrequent reports of a small number of transactions generally submit reports manually. Some business operators considered the manual reporting process complicated, and for that reason the FIU has simplified the reporting process for certain business operators. The efforts to make reporting more efficient and easier continue during 2021.

SAMLIT – the Swedish Anti Money Laundering Intelligence Taskforce

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 to further strengthen 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. At the end of 2020, a decision was taken to enhance and formalise this cooperation project in 2021.

The legal basis for the exchange of information is the obligation of the banks to provide, on request from the Swedish Police Authority, all information necessary to investigate money laundering or terrorist financing. Due to its responsibility to combat money laundering and terrorist financing, the FIU played a central part in contacts and cooperation with the banks.

The methods used are the same as for ordinary reporting, but in SAMLIT the Swedish Police Authority and the banks have cooperated in a more operational manner, and banks have been able to perform more in-depth and broader analyses than before. These forms of cooperation were developed taking into consideration that bank secrecy prevents banks from sharing information included in the secrecy obligation with each other. Based on a number of questions concerning suspected criminal individuals and companies, suspicions of money laundering could be investigated by working together. SAMLIT has also resulted in banks taking measures directed at the individuals in question and improving their monitoring of modus operandi.

Early on, it was apparent that the project produced results and the investigations have grown. Money was seized, preliminary investigations were initiated and parallel cases opened. One challenge has been to limit the number of cases in order to channel all information to those instances that are able to take measures to prevent or investigate criminal activities.

One part of the project is to develop the exchange of information, to provide feedback where relevant and to further improve the exchange of information in accordance with the rules on money laundering. This question is also included in the instructions for the Government Commission on enhanced measures against money laundering and terrorist financing, which will present its conclusions in May 2021.[7]

The efficiency of the project has been confirmed by all participants and in 2021, more cases will be opened. There are also ideas to open up the project to more business operators.

7 Commission Directive 2019:80 and Supplemental Directive 2020:122.

New legislation in 2020

Legislation on money laundering has been amended and grown more extensive during a long period of time. 2020 was no exception. Several changes were made during the year, which means that the fifth Anti-Money Laundering Directive[8] has now been implemented in Sweden. Among other things, more categories of business operators now have reporting obligations to the FIU, including persons who manage and trade in virtual currencies. In addition, further protections for whistle-blowers and improvements of international cooperation were introduced. The Swedish Security Service now has the right to request financial data directly from business operators without needing assistance from the FIU.

The definition of a politically exposed person (PEP)[9] was expanded, and the information exchange and forms of cooperation at the national level between the FIU and supervisory authorities were strengthened. In addition, international cooperation between financial intelligence units in different countries was improved. A clarification was also made that the FIU should provide feedback, to the extent possible, to business operators that have reported suspected money laundering and terrorist financing.

In addition to the amendments to the Anti-Money Laundering Act, a new act entered into force during the year. The act[10] makes it possible for the FIU and other law enforcement agencies to quickly establish the identity of physical and legal persons who have accounts and safe deposit boxes at financial companies.

At present, the FIU makes requests directly to financial companies. The new system (the "Mechanism") makes information on owners directly and immediately available through a search on a technical platform that is provided by the Swedish Tax Agency. The Mechanism is a way to provide several government agencies, including the Swedish Police Authority, with a more efficient tool to rapidly find out where individuals and companies hold bank accounts and safe deposit boxes. This will improve efforts to combat money laundering and terrorist financing.

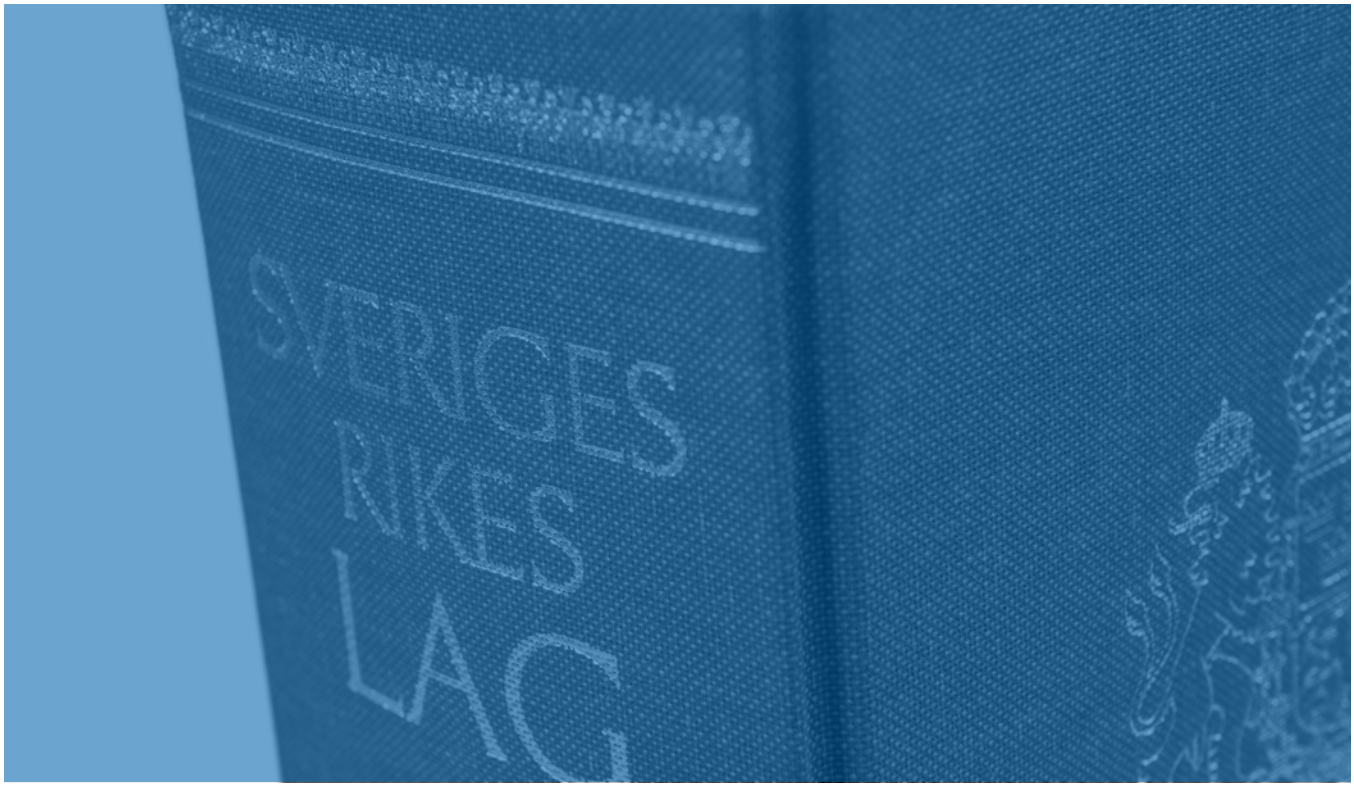
Suggested further measures

Through *Kommittédirektiv 2019:80 Stärkta åtgärder mot penningtvätt och finansiering av terrorism* ("Commission Directive 2019:80 Strengthened measures against money laundering and terrorist financing"), the Government appointed a commission to analyse which measures should be taken to further strengthen efforts to combat money laundering and terrorist financing. The commission's task includes analysing

8 The fifth Anti-Money Laundering Directive was implemented mainly through Government Bill 2018/19:150 and Government Bill 2019/20:53 which amended the Act on Measures against Money Laundering and Terrorism Financing (2017:630) (the Anti-Money Laundering Act).

9 Politically exposed persons (PEP) are individuals with important public functions in a country. Examples in Sweden include the heads of state and government, ministers, members of the Riksdag, Supreme Court judges, other higher officials and their family members.

10 The Act on Systems for Accounts and Safe Deposit Boxes (2020:272) introduces the requirements of the fourth Anti-Money Laundering Directive in Swedish legislation (article 32(a)).



the conditions for information exchange mainly between banks and law enforcement agencies, as well as proposing more efficient forms for such exchanges. This part of the commission's task is of particular importance for the FIU, as the intelligence service started cooperating with a number of large banks. The cooperation project focuses on exchange of information on prioritised operators in order to combat money laundering in accordance with current legislation (see section on SAMLIT). One current obstacle for efficient work is bank secrecy, which makes it impossible to share relevant information with other business operators.

Another important task of the commission is to analyse whether the system with obligations to report and provide information to the FIU is adequate and appropriate. In 2019, the FIU sent a request[11] to the Ministry of Justice. The request addresses the problems that arise when business operators offer services or distribution channels through a third party vendor which is not subject to the reporting obligation.

The proposals of the commission remain to be seen, but the FIU believes that there are a number of important operators in the payment services market who possess valuable information about transactions and who should be obliged to report and/or provide data to the FIU. The commission will present its conclusions no later than 31 May 2021.

Provisions for reporting in goAML

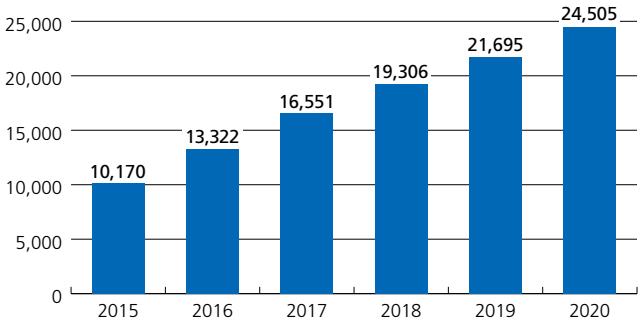
The Swedish Police Authority's provisions for reporting and providing information based on the Anti-Money Laundering Act entered into force on 16 March 2020. The provisions state that business operators as defined in the Anti-Money Laundering Act are obliged to submit their reports to the Swedish Police Authority's web portal goAML (see section on goAML).

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

The Financial Intelligence Unit in numbers

The number of suspicions of money laundering or terrorist financing that were reported to the FIU continued to increase and reached a total of more than 24,500 in 2020, see Figure 1. This was 13 percent more than the previous year and more than twice as high as 2015. The total value of the transactions that were reported during the year amounted to more than SEK 15 billion. In this context, it is important to note that the required level of suspicion is low, and that transactions are sometimes reported just because they somehow deviate from normal patterns. The amount thus includes transactions that on further examination turn out not to be relevant.

Figure 1. The number of suspicious activity reports in 2015–2020



In 2020, the FIU received reports from 241 business operators. That is somewhat less than the 285 reporting business operators in 2019, which may be due to a certain threshold to start reporting in the new system. The FIU prioritises its work to simplify reporting for business operators that only rarely submit reports and that do not have an automated technical solution.

Table 1 shows how suspicious activity reports are distributed between different types of reporting entities. Most reporting comes from the financial sector where banks submit approximately 75% of all reports. Gambling companies also submit a comparatively large number of reports. As concerns smaller operators with more infrequent reporting, there is a noticeable increase in the categories cash trade in goods and pawn shop businesses. However, reporting from these sectors are still at a low level. Businesses outside the gambling and finance sectors submitted less than 1% of the reports to the FIU in 2020, see Figure 2.

Figure 2. Entities reporting to the Financial Intelligence Unit in 2020

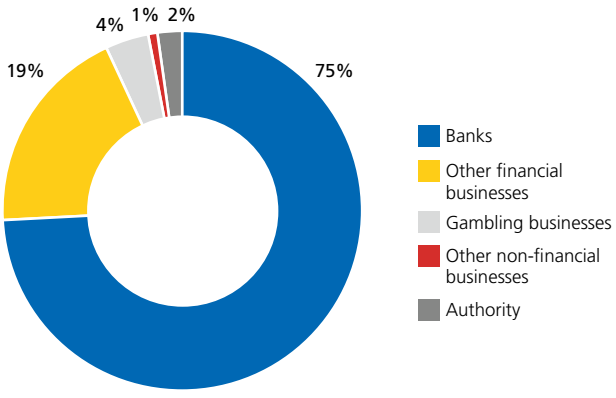


Table 1. Number of reports received per sector 2015–2020

	2015	2016	2017	2018	2019	2020
Banking and financing institutions including credit market companies	5,700	9,271	12,169	14,421	16,831	18,342
Life insurance businesses	42	17	32	32	42	17
Securities businesses	7	..	..	10	19	6
Financial businesses with compulsory registration	473	31	27	166	493	163
Insurance intermediaries	4	..	..	..	..	0
Electronic money institutions (including reports by representatives)	148	392	35	50	39	13
Fund businesses including alternative investment funds	3	..	..	..	..	2
Payment services*	3,415	3,124	3,674	3,764	3,045	4,032
Currency exchange and deposit businesses						270
Consumer credit businesses	6	46	68	149	185	87
Mortgage credit businesses			..	..	..	12
Real estate agents	3	..	6	..	23	5
Gambling services**	313	325	381	474	614	907
Professional trade in goods***	36	41	55	37	83	122
Pawn shops			7	6	6	12
Auditing (approved or authorised public accountant or registered accounting firm)	3	10	8	7	20	8
Book-keeping or auditing services (excluding approved or authorised public accountants and registered accounting firms)	10	18	9	16	19	6
Tax advisers	0	..	..	..	..	4
Lawyer or junior lawyer at law firm	4	..	..	..	6	1
Other independent lawyers	0	..	..	..	..	0
Company formation, trustees etc.	0	..	..	..	..	0
Supervisory authorities	3	37	24	23	19	8
Other authority			47	133	239	488
TOTAL**	**10,170**	**13,322**	**16,551**	**19,306**	**21,695**	**24,505**

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

* In 2015–2019 the category Payment services included payment institutions and registered vendors of payment services including currency exchange. For 2020 currency exchange and deposit businesses were lifted out and form a category of their own.

** Gambling services were introduced in the Anti-Money Laundering Act on 1 August 2017. For 2019 the number of reports was adjusted from 481 to 614.

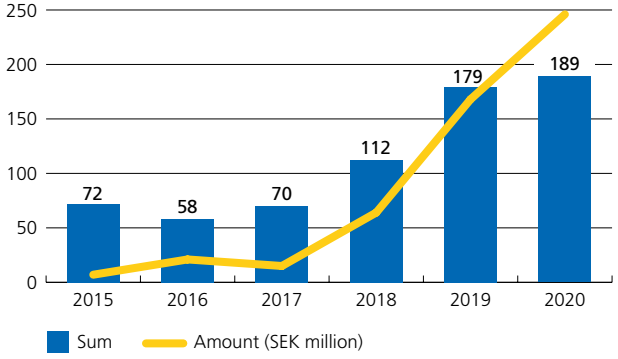
*** The category professional trade in goods includes auction centres and companies trading in vehicles, scrap metals, precious stones, antiquities and art with a value that exceeds EUR 5,000. Until 1 August 2017 the limit was EUR 15,000.

**** Two errors were detected in the statistics for 2019; the first is the sum of the total number of reports and the second the number of reports in the gambling sector. The total number of reports for 2019 was adjusted from 21,709 to 21,695. For the gambling sector the number of reports was adjusted from 481 to 614. Other sectors are not affected.

The number of restraint orders continued to increase in 2020

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. In 2020 the FIU decided on 189 restraint orders for assets with a total value of nearly SEK 250 million, see Figure 3. This amount was an increase of 46% compared to 2019 and the highest ever.

Figure 3. Restraint orders



Filed police reports more than doubled compared to 2019

The level of suspicion required for reporting to the FIU is low. For example, the customer may act in a way that deviates from what is expected taking into account the business operator's know-ledge on the customer. The low level of suspicion makes it possible for the FIU to discover things that, taken together with other information, may turn out to be an important part of the puzzle and lead to other measures being taken. All reports are assessed and a large part processed. In certain cases, the FIU makes the assessment that there is a sufficient level of suspicion to initiate a preliminary investigation, normally concerning money laundering. In these cases, the FIU files a police report.

In 2020 the FIU filed 609 police reports, more than twice as many as the previous year, see Table 2. In addition to these, the FIU took other measures that at a later stage resulted in police reports or support to ongoing preliminary investigations.

Table 2. Police reports by the Financial Intelligence Unit

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

The significant increase compared to 2019 is mainly the result of an increased focus on operational work and higher capacity for the FIU to process incoming reports. The increasing trend during the last few years is also due to a large flow of reports that are linked to fraud.


juni
juli
augusti
september
oktober

FAQ

What happens when a report is submitted to the FIU?

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 register to be used again if further 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 normal, but that may be presumed to form a part of money laundering or terrorist financing should also be reported.

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 behaviours. In cases of transactions or behaviours that are not understood, the first thing to do is to enhance customer due diligence measures. That may lead to the suspicions being dismissed, in which case they should not be reported. At other times, enhanced customer due diligence measures result in stronger suspicions, in which case they must be reported. If it is assessed that the risks for money laundering or terrorist financing cannot be managed, the business relationship with the client should be discontinued or, at the very least, the client 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 customer due diligence measures cannot be performed before the reporting. Enhanced customer due diligence should then be performed after reporting and 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.

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

No. Chapter 4, Section 9 of the Anti-Money Laundering Act (2017:630) states that business operators that submit reports are bound by professional secrecy and are not allowed to disclose, to the client or any third party, that a report was submitted to the FIU. However, this information may be shared with supervisory authorities and law enforcement authorities, among others, and in certain circumstances within the group and with other business operators that are involved in the same transaction with the same client.

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

Yes. Chapter 4, Section 3, second paragraph of the Anti-Money Laundering Act (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 client was discontinued due to the risk for money laundering or terrorist financing.

A police report should be filed for frauds that have been completed.

It is recommended that the defrauded client does this at the police's website (polisen.se/utsatt-for-brott/polisanmalan/) or alternatively at the police's 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 register can be added to the preliminary investigation.

Publisher
Swedish Police Authority
Production
Communications Department

Diarienr.
A076.210/2021

Edition
200 copies
Printed by
Polisens Tryckeri, March 2021

Graphic design
Blomquist Communication
Photo
Swedish Police Authority page 1, 6, 9, 11, 12, 15, 19.
Mostphotos page 23.