Content

Preface ................................................................................................................. 3
The tasks and activities of the Financial Intelligence Unit .................. 4
The Financial Intelligence Unit in 2019 ...................................................... 5
Money laundering ......................................................................................... 6
  Characteristic modi operandi in 2019 .................................................... 8
  BEC ........................................................................................................ 9
  Vishing .............................................................................................. 10
  Money laundering via online gambling accounts ................................ 11
  Money laundering via real estate ......................................................... 11
  Commercial money laundering ......................................................... 12
  Cryptocurrency exchange agents ...................................................... 12
  Commercial money laundering using a real estate agent’s escrow account .................................................. 13
Terrorist financing ....................................................................................... 14
  What constitutes terrorist offences and terrorist financing? ............ 14
  What does terrorist financing look like? ........................................... 14
  Cooperation ....................................................................................... 15
The international work of the Financial Intelligence Unit ................. 16
goAML ......................................................................................................... 17
Black Wallet ............................................................................................... 18
  FinTech brings changes to financial markets ..................................... 18
  Project Black Wallet ........................................................................... 18
New legislation .......................................................................................... 20
  New legislation in 2020 ..................................................................... 20
  Request to the Government ............................................................... 21
  Provisions on reporting in goAML .................................................. 21
The Financial Intelligence Unit in numbers .......................................... 22
  Restraint orders ............................................................................... 24
  Filed reports ...................................................................................... 24
FAQ ........................................................................................................ 25
In 2019, money laundering and terrorist financing was frequently discussed in the media and among law enforcement agencies and business operators. The discussions centred on money laundering scandals and the resulting need for stronger measures to prevent money laundering and terrorist financing. The Financial Intelligence Unit functions as a hub for such countermeasures and constantly strives to be at the forefront. Extensive work is carried out to discover suspicious activities at an early stage and to give feedback to those parts of society where they may be taking place.

Reporting to the Financial Intelligence Unit on suspicious activities increased in 2019. Due to this reporting, we were able to issue restraint orders for more money than ever before – money that was being laundered but never reached the intended recipients. In many cases, the money was returned to the owners.

The Financial Intelligence Unit, by tracing financial activities among actors involved in serious crime and processing money laundering cases, made an important contribution to the Swedish Police Authority’s overall efforts to counter serious violent crime, such as shootings, explosions and international cases concerning trafficking in human beings and drugs. The Financial Intelligence Unit is active in all of the regional intelligence centres in Sweden, along with eleven other authorities. In 2019, the Financial Intelligence Unit worked on more than 20 cross-agency money laundering cases, which originated in for example frauds, drug offences and environmental offences.

In 2020, the recently implemented IT system goAML will start to produce results in the form of more numerous and more thorough analyses of received money laundering reports. This will improve our strategic ability to detect modi operandi and trends as well as our operational capability to detect various money laundering schemes. To a larger extent than before, we will respond to business operators’ growing need for feedback. In addition, we are currently cooperating with several business operators and supervisory bodies to increase our information exchange at the operational level. This higher level of ambition makes it necessary to recruit approximately 20 new employees before the beginning of 2021, mainly intelligence officers and analysts.

The Financial Intelligence Unit continues to improve its ability to stay at the forefront and function as the hub for combating money laundering and terrorist financing.

Mats Löfving
Head of the National Operations Department
The Financial Intelligence Unit is a part of the Swedish Police Authority’s intelligence service and is assigned to the National Operations Department. This means that we become active at an early stage in cases of potential organised crime, specifically suspected money laundering or terrorist financing. The Financial Intelligence Unit uses the guidelines issued by the police’s management to prioritise tip-offs, questions, requests for assistance and reports on suspicious transactions that are received by the Unit. As an intelligence service, a basic task is also to detect trends and developments in money laundering and terrorist financing that may influence other police activities or cause significant financial risks in general. We are supposed to provide early warnings within a well-defined but large area of operations.

The Financial Intelligence Unit must adhere to a number of laws, regulations and EU legal acts. The regulatory framework states that the Financial Intelligence Unit is a part of the Swedish Police Authority and organised as a section (the Police Authority functions as the financial intelligence unit), but also that access to the money laundering register is restricted to employees at the Unit. The regulatory framework stipulates that the Financial Intelligence Unit must be independent in receiving, analysing and disseminating information in its area of responsibility. This means that we express ourselves clearly and that our assessments of current information and intelligence are based on our specific role as financial intelligence unit. However, independent does not mean alone – legislative developments usually leads to more exchange of information, increased levels of cooperation and more efficient routines, and this is outside the control of the Financial Intelligence Unit. Demands for independent assessments and compliance with security and privacy provisions have to be balanced with national and international cooperation. At the same time, we need to form a part of the legal system, from crime prevention to investigations support.

At the moment, the Financial Intelligence Unit has approximately 35 employees, but extensive recruiting was initiated in 2019 to strengthen our operational and strategic capabilities. The unit is composed of four groups, with an even distribution of men and women. Approximately one third of the employees are police officers and two thirds are civilian employees with educational and professional experience from various kinds of investigative and analytical work.
For the first time, the number of reports on suspicious transactions exceeded 20,000. The Financial Intelligence Unit cooperated with other Swedish law enforcement actors in more than 600 cases.

During 2019, the Financial Intelligence Unit deployed a new IT system for filing and managing reports on money laundering. The deployment was performed in close cooperation with business operators. In the beginning of the year, we initiated a two-year project financed by the EU in which we, along with the Finnish financial intelligence service, will map terrorist financing and money laundering risks in the FinTech sector.

During the year, the coordination function for prevention of money laundering and terrorist financing published a national risk assessment of money laundering and terrorist financing. Along with other actors, the Financial Intelligence Unit worked on the risk assessment.

Feedback, guidance and information to business operators were also central themes during 2019. During the autumn, the Financial Intelligence Unit arranged a workshop aimed at all business operators. The level of interest was high, and in 2020 we will consider arranging the workshop at a larger venue to make it possible for more business operators to participate.

---

1 A type of fraud using social manipulation; a fuller description is provided in the chapter on money laundering under the heading Characteristic modi operandi 2019.

2 Financial Technology: companies developing or using innovative financial solutions and services, such as applications for mobile payment services.

3 The Swedish Police Authority heads a national coordination function for prevention of money laundering and terrorist financing, which consists of representatives from 17 organisations.
Money laundering

The opportunity to make money is a strong incentive in almost all kinds of crime, in particular in organised crime. To be able to use their proceeds from crime in the legal economy, criminals need to launder them. Money deriving from crimes such as fraud, drug trafficking or robberies have to be transformed into what looks like legal income and assets.

Crimes resulting in financial gain are potential predicate offences to money laundering, including evasion offences (such as reporting false information in order to evade taxes or other fees).

Money laundering is often described as consisting of three stages:
1. Introducing proceeds of crime into the financial system
“Integration of proceeds of crime varies depending on such things as the amounts involved and the capacity of criminals. They may be spent on for example day-to-day expenses...”
2. Layering of the proceeds of crime in order to hide their illegal origin
3. Integration of the money into the legal economy

The process may differ depending on the predicate offence, the amount of money involved and in what sector of the economy the money laundering takes place. Proceeds of crime which have passed through these stages may usually be used by the criminal with little risk of detection.

Proceeds of crime may take different forms: property, money in the form of cash or account balances, cryptocurrencies or other assets. This means that the introduction of the proceeds of crime into the financial system also takes different forms. Common methods are cash deposits or purchases and sales of goods that were bought using proceeds of crime.

In the deceptive layering stage, a number of transactions are carried out in order to make tracing more difficult. In general, transfers that are executed immediately or that make tracing more difficult are attractive. This means that mobile transfers and financial technology (FinTech) services are frequently used.

“Not all proceeds of crime are laundered. Some of them are consumed without laundering; others are reinvested in criminal activities.”

The next chapter describes a number of different money laundering schemes encountered in 2019. These descriptions are examples, representing various modi operandi. One of the procedures most frequently reported to the Financial Intelligence Unit is BEC4. The new law on gambling resulted in a higher number of reporting entities, which most likely will lead to a larger number of reported transactions.

The mortgage example is a more typical example of money laundering. Cryptocurrencies is a modus operandi where the possibilities for anonymity have become a challenge for law-enforcement authorities, and an example of how a parallel financial infrastructure has emerged. Commercial money laundering (i.e. conducted on a habitual basis or on a sizeable scale) is an important aspect of anti-money laundering, as actors with low quality customer due diligence and monitoring are often exploited by criminals. It should be added that the use of various FinTech services is a modus operandi which is developing fast, as are the potential risks (see section on Black Wallet).

Characteristic modi operandi in 2019
Various types of fraud were the offences most frequently reported to the Financial Intelligence Unit. These frauds ranged from merchandise that were never delivered after payment, with initial contacts made through

4 Business e-mail compromise: fraud with the purpose of acquiring money through erroneous payments; a thorough description of the procedure is found under the heading Characteristic modi operandi in 2019.
ads at online marketplaces or through social media (where also romance scams are becoming increasingly common), to more advanced schemes such as BEC fraud and vishing.

Fraud might be an end in itself, but also a way for criminals to fund other criminal activities. Regardless of the modus operandi, the proceeds of these crimes are often fed into serious organised crime.

**BEC**

The purpose of BEC (business e-mail compromise) fraud is to become the recipient of erroneous payments. The most common method is that a fraudster, who claims to be a senior executive of a company, sends an e-mail to the company’s financial manager requesting that a payment be made to a specific account in a foreign country. This is made possible through an earlier data security breach or through manipulating the sender’s e-mail address (spoofing).

The common denominator is that the money is transferred to another country, to make recovery more difficult and to launder the money. It is possible for the receiving bank to detect the fraudulent transaction, as there is frequently a mismatch between the name of the recipient of the transaction and the holder of the bank account.

---

5 Using a false identity online, for example a fake e-mail address.
However, if this is not detected and the transaction is approved, the money is quickly layered away from the primary money mule’s bank account to make it impossible to recover the proceeds of crime.

A substantial part of all the reports made to the Financial Intelligence Unit concerns BEC frauds and in the past year considerable resources were dedicated to it. There are strong indications that the majority of these activities are organised by international organised crime groups.

Vishing

Vishing takes place when a fraudster calls someone and tries to manipulate that person into handing over information that makes it possible to access his or her bank account. Usually, the fraudster claims to be calling from the security department of a bank, or sometimes from an authority, a telecom operator or a retail store. During the call, the fraudster may state, for example, that the receiver of the call has been the victim of a fraud. The caller (i.e. the fraudster) is, however, able to stop the fraud, but only if the victim verifies his or her identity using Bank ID (a Swedish
The fraudster usually deceives the victim into believing that all their money will disappear unless they verify their identity. Instead, the verification gives the fraudster access to the victim’s bank account or the possibility to issue a new Bank ID that is controlled by the fraudster. The victim’s account is then emptied and the money transferred to front men. The money is later withdrawn in cash or converted to cryptocurrency.

“Usually, the fraudster claims to be calling from the security department of a bank, or sometimes from an authority, a telecom operator or a retail store.”

Money laundering via online gambling accounts

In the beginning of 2019, a new law on gambling entered into force. Among other things, this led to an increase in the number of operators for which anti-money laundering legislation is applicable. The gambling industry has historically been used for money laundering, but new legislation and increased awareness has led to better reporting. Reports show that online gambling accounts, in combination with other financial services, are frequently used in money laundering schemes.

“Reports show that online gambling accounts, in combination with other financial services, are frequently used in money laundering schemes.”

A common modus operandi is that money from various sources is transferred to online gambling accounts, frequently using FinTech services. A private individual then gambles at the online gambling company, spending the required minimum amount, and then withdraws the rest of the deposited balance to his or her bank account. Usually, this is not the same account as the one from which the money derived. The money that was returned to the private individual’s bank account can then be referred to as “gambling winnings”, as they derive from an online gambling account, at least technically speaking. However, the purpose of the deposit in the online gambling account was not to gamble, but to have a plausible explanation for the origin of the money.

Money laundering via real estate

Trading in real estate is a well-known method for money laundering. Various methods are used. If the purchase is mostly financed through mortgages, there are only limited possibilities to launder money directly through the real estate purchase. In these cases, it is generally the down payment that may consist of proceeds of crime. Instalment payments may also consist
of proceeds of crime, which is a form of money laundering. The property turns into a legal asset whose origin is not called into question, and when the property is eventually sold the owner is able to claim that the money from the sale is legal.

Another way to use real estate for money laundering is to pay for repairs of buildings using proceeds of crime, thus increasing the value of the property. When the property is sold, the increase in value constitutes laundered money. At times, a part of the purchase price is paid under the table using proceeds of crime; when the buyer later resells the property, this money has turned into laundered money. It is also possible to inflate the purchase price and the buyer is compensated with proceeds of crime under the table to the seller. The buyer gets to launder proceeds of crime and the seller gets access to dirty money.

"Another way to use real estate for money laundering is to pay for repairs of buildings using proceeds of crime, thus increasing the value of the property."

Commercial money laundering
Commercial money laundering is included in the Act on Penalties for Money Laundering Offences (2014:307), but there are few convictions for this offence. In 2019, the Financial Intelligence Unit decided to take a closer look at this offence in order to better understand what is needed for a conviction.

For commercial money laundering, the crucial point is not whether the money derives from criminal activities (which is the case for normal money laundering). Instead, the circumstances surrounding the transactions are central, as are the way these were performed and how the risks for money laundering were managed. If the entity neglected to take measures to prevent money laundering and thereby took reprehensible risks, that would constitute commercial money laundering. Intent to take part in a money laundering scheme and knowledge that the money derived from crime or criminal activities is thus not necessary. The provisions on commercial money laundering are applicable to business activities or other activities conducted habitually or on a large scale. Commercial money laundering may take place in businesses handling money or other assets, when these businesses are obliged to take measures according to the regulatory framework on money laundering.

"If the entity neglected to take measures to prevent money laundering and thereby took reprehensible risks, that would constitute commercial money laundering."

Cryptocurrency exchange agents
Cryptocurrencies received more attention from the media a few years ago, but trade is still going on in a relatively large scale. There are legal uses for these currencies, but they are also used for purposes such as drug trade, in particular on the darknet – an encrypted part of the internet. Cryptocurrencies are kept in virtual wallets whose owners are often anonymous; this makes them useful for money laundering purposes.

"Cryptocurrencies are kept in virtual wallets whose owners are often anonymous; this makes them useful for money laundering purposes."

Trading in cryptocurrencies must be registered with the Swedish Financial Supervisory Authority. Anyone performing such trades to an extent that cannot be considered a hobby is subject to the regulatory framework on money laundering. This includes
requirements on customer due diligence of the individuals with whom the person trades.

Normally, these exchange agents have one or several accounts at companies trading in cryptocurrencies. Through various platforms, the exchange agent makes contact with people that are interested in buying or selling virtual currency. The buyer and the seller agree on the procedure for the exchange. A money transaction takes place between them, usually using mobile transfers but account transfers and cash payments also occur. In this way, the exchange agent’s customers are able to evade the customer due diligence and the anti-money laundering measures that would have been performed if the exchange had taken place at a company registered with the supervisory authority.

At present, a substantial part of this trade is performed by private individuals who have not registered their business with the Swedish Financial Supervisory Authority. They may have a considerable turnover without being subject to any supervision or having to perform the controls stipulated in money laundering legislation. Payments for the cryptocurrencies are frequently made to regular personal bank accounts, and it is not uncommon for an exchange agent’s bank account to turn over amounts that are several times larger than that person’s annual income as declared to the Swedish Tax Agency. In these cases, the business operator that provides a bank account and other financial services to the exchange agent has the obligation to perform adequate customer due diligence so as to be able to act on this kind of abuse.

Commercial money laundering using a real estate agent’s escrow account

When homes and real estate are bought, payments and transfers are normally made through the escrow account of the real estate agent that manages the deal. As the real estate agent is conducting a business operation, customer due diligence must be performed and the agent is supposed to investigate the origin of funds deposited in his or her escrow account. If, for example, the real estate agent accepts a down payment where the origin of the money is questionable, he or she might be committing commercial money laundering. Examples include a down payment that is transferred from someone else than the buyer, that is paid into the agent’s account in cash, that is transferred from several different accounts or whose origin cannot be reasonably explained.

"Trading in cryptocurrencies must be registered with the Swedish Financial Supervisory Authority. Anyone performing such trades to an extent that cannot be considered a hobby is subject to the regulatory framework on money laundering."
Terrorist financing

Just like suspected money laundering, business operators have to report suspected terrorist financing to the Financial Intelligence Unit. This might be suspicious transactions or deviating procedures with possible links to terrorist financing.

In terrorist financing, the crucial point is the destination of the assets. This differs from money laundering, where the origin of the assets is in focus. This means that no predicate offence is necessary for terrorist financing, and in fact many terrorist offences were funded using relatively small amounts of money with a legal origin. Discovering suspected terrorist financing is a major challenge for law enforcement authorities and business operators.

What does terrorist financing look like?

Terrorist financing may be done with limited funds, and these funds may have a legal or illegal origin. Due to this, it is often harder to detect than money laundering. In other cases, terrorism is funded with proceeds of crime; in these cases, it may be detected in the same way as money laundering. Proceeds of crime that are used to fund terrorism may also derive from various kinds of volume crime, such as fraud and theft. It is important to note that violent extremists are also found in regular criminal groups without obvious religious or ideological affiliations.

What constitutes terrorist offences and terrorist financing?

Definitions of what is considered terrorist offences are given in the Act on Criminal Responsibility for Terrorist Offences (2003:148). In summary, they are acts committed with the intent to

- seriously intimidate a population or a group of population,
- unduly compel a public authority or an inter-governmental organisation to perform an act or abstain from acting, or
- seriously destabilise or destroy fundamental political, constitutional, economic or social structures in a state or in an intergovernmental organisation.

The Act on Criminal Responsibility for the Financing of Particularly Serious Crime in some cases (2002:444) provides that it is illegal to collect, provide or receive funds or other property with the intention that it should be used or in the knowledge that it is to be used for terrorism.

This means that an individual who transfers money or other property to individuals or groups that plan or commit terrorist offences is guilty of terrorist financing. The assets do not have to be used specifically in terrorist attacks. The stipulations also concern financing of for example recruitment and training for terrorist offences and other particularly serious crime.

"In terrorist financing, the crucial point is the destination of the assets. This differs from money laundering, where the origin of the assets is in focus."

"Terrorist financing may be done with limited funds, and these funds may have a legal or illegal origin."
To make it possible for the business operator to detect terrorist financing, good customer due diligence is important. Who is the customer? Is the turnover on the account reasonable? Is the transaction reasonable? Is there an explanation for the customer’s counterparties? Are the procedures deviating? How can these procedures be understood when taking into account available strategic analyses or other developments?

It is difficult to predict or prove terrorist financing using only financial information. Due to this, cooperation between the Swedish Security Service and other intelligence services, in Sweden and in other countries, is vital.

The Financial Intelligence Unit processes and analyses the information provided by the business operator. If there are suspicions of terrorist financing, the Financial Intelligence Unit forwards intelligence information to the Swedish Security Service and other relevant authorities. In some cases, the information is shared with FIUs in other countries. Following further processing and analysis, some reports received by the Financial Intelligence Unit are considered to concern suspected terrorist financing.

“Following further processing and analysis, some reports received by the Financial Intelligence Unit are considered to concern suspected terrorist financing.”

Cooperation
The Financial Intelligence Unit cooperates continuously with the Swedish Security Service on matters such as terrorist financing, modi operandi, trends and other current issues. In some cases, the Financial Intelligence Unit participates in the work of regional intelligence centres on suspected terrorist financing.

The Financial Intelligence Unit also takes part in international training courses and international platforms on terrorist financing. In addition, there is a yearly Nordic Forum on Terrorism Financing held together with our counterparts in the Nordic countries. The purpose of these meetings is to share information on trends and modi operandi that were detected during the past year in order to discover and prevent terrorist financing.

Example of a case
The Financial Intelligence Unit receives a report concerning a non-profit organisation that raises funds for people in need in a war zone. The report includes information on the four officials of the non-profit organisation. The Financial Intelligence Unit searches in police databases and finds matches for two of them, with links to violent extremism. Another business operator had already reported one of them to the Financial Intelligence Unit concerning suspicious transactions to Turkey.

The Financial Intelligence Unit gathers more financial information about this individual and finds transaction lists with other links to violent extremist circles.

Considering the information received and these individuals’ links to violent extremist circles, it is suspected that the transfers made by the organisation to the war zone may be an indication of terrorist financing. The Financial Intelligence Unit notifies the Swedish Security Service and others for further assessment.

---

6 Financial Intelligence Units. These may be independent authorities or form part of another authority, and may be either civilian or police authorities. In Sweden, the Financial Intelligence Unit is a part of the Swedish Police Authority.
The international work of the Financial Intelligence Unit

International cooperation is an important part of a financial intelligence unit’s work. International cooperation takes place at the operational level, with exchange of information on people, companies and organisations between financial intelligence units across the world, but also at the strategic level, with exchange of information on modi operandi and trends. Important venues for international cooperation on financial intelligence are the global organisation FATF, the EU FIU platform for cooperation between financial intelligence units in the EU and Egmont, which is an important forum for cooperation with financial intelligence units outside the EU.

In addition to the Black Wallet project with Finland, EMMA (European Money Mule Action) was an important form of international cooperation during the past year. This is a recurring cooperation project aimed at money mules and coordinated by Europol and Eurojust together with the European Banking Federation. In Sweden, this project is closely connected to the Financial Intelligence Unit’s work to prevent BEC and vishing fraud, in which money mules play an important part in laundering the money.

The Financial Intelligence Unit has also provided information to various FATF working groups. The most important of these is the Financial Intelligence Unit’s participation in a FATF expert group which is tasked with developing a guide on digital identities. As Sweden is a leader in the field, our experiences will play a major part in future recommendations from FATF. The Financial Intelligence Unit has already called attention to these risks in material that was sent to business operators.

Member states’ anti-money laundering efforts are also under evaluation at the EU level. The Financial Intelligence Unit provided assistance in the form of experience, statistics and examples of national and international cooperation. An important part of our work during the past year was the ongoing Council of Europe assessment of the implementation of the fourth anti-money laundering directive. The results are expected in 2020.

---

8 A project funded by the EU and executed by the Finnish and Swedish police. The aim of the project is to map new financial services and products, and to identify risks for money laundering and terrorist financing in the FinTech sector.
Member states’ anti-money laundering efforts are also under evaluation at the EU level. The Financial Intelligence Unit provided assistance in the form of experience, statistics and examples of national and international cooperation. An important part of our work during the past year was the ongoing Council of Europe assessment of the implementation of the fourth anti-money laundering directive. The results are expected in 2020.

"The new method for reporting makes it possible for the Financial Intelligence Unit to improve its analyses of information found in money laundering reports."

The change of IT systems was due to the Swedish membership in FATF, which makes detailed demands that we have to follow. The change was necessary so as to be able to deliver the analyses and statistics that are included in the Financial Intelligence Unit’s mission.

The move to goAML introduces some changes for the Financial Intelligence Unit and for business operators. To a larger extent than before, the reporting will follow a pre-determined structure. Reporting may be manual or automated, but the structure is the same in both cases. The new method for reporting makes it possible for the Financial Intelligence Unit to improve its analyses of information found in money laundering reports. Due to this, the feedback to business operators and supervisory authorities will improve, as will the supporting documents shared with other law enforcement authorities.

During the year, the Financial Intelligence Unit continued its cooperation in the implementation project goTogether that started at the end of 2017. Around 30 business operators took part in the project. They assessed the reporting in a test portal and gave valuable feedback on reporting structures and documentation. At the end of the year, the portal opened for testing by other business operators than those who took part in the project. The testing portal will remain open for now, for the benefit of new business operators and new staff, and also to be able to test updates.

The police’s provisions on goAML can be found in the section New legislation.
FinTech brings changes to financial markets

Financial technology is a rapidly growing market that provides innovative financial solutions and services such as mobile payments. As a consequence, the number of actors in payment flows has increased. The larger number of actors in transaction chains may lead to segmentation of information. This, in turn, changes conditions for monitoring and customer due diligence. At the same time, other actors gain more insight in the flows and an improved ability to detect suspicious transactions. Several of these actors are at the moment not obliged to file reports in accordance with the Anti-Money Laundering Act (2017:630), which means that important information never reaches the Financial Intelligence Unit.

Project Black Wallet

Black Wallet is a two-year project funded by the EU that was launched in the beginning of 2019. The name of the project is based on the fact that the management of our personal finances is to an ever increasing degree moving from our wallets to our mobile phones, which we are able to use to quickly perform banking activities that used to require a visit to the bank and then several days of processing time. In the project, the Swedish and the Finnish police are cooperating along with other authorities in Sweden and Finland.

In Finland, the project is led by the Finnish Financial Intelligence Unit. In Sweden, Black Wallet is led by the Swedish Financial Intelligence Unit. The project will contribute to the Swedish Police Authority’s long-term goal – success in fighting and solving crime – and its strategic initiative to improve and future-proof its activities.

The project aims to map new financial services and products, and to identify risks for money laundering and terrorist financing in the FinTech sector. The project will focus on:

- How products and services may be exploited for money laundering and terrorist financing purposes.
- What information is available to operators, and how that information may be used for intelligence and investigative purposes.

The project strives to create a fuller picture of the FinTech sector in the EU, in particular as regards payment and money transfer services, in order to assist law enforcement authorities in their efforts to prevent, detect and investigate money laundering and terrorist financing. The Black Wallet project group held a number of presentations in 2019 to inform law enforcement authorities about risks and possibilities in the FinTech sector. The project is characterised by international cooperation with, among others, financial intelligence units in Europe.

Cooperation with the private sector is a prerequi-
site for the project’s success. One of the objects is to create a platform where the private and public sectors are able to cooperate on identifying risks and developing risk-mitigating measures. In 2019, the project group invited a large number of business operators to take part in the project, and a dialogue was held on:

- How to improve authorities understanding of the sector.
- How the sector works to prevent money laundering and terrorist financing.
- How the Financial Intelligence Unit and companies can work together.

An analysis was made to identify sector specific properties that, separately or in combination, may lead to increased risks for terrorist financing and money laundering.

The project group also held presentations at several FinTech events and invited and visited business operators in the FinTech sector. The project plan for 2020 includes more visits to and training courses for business operators and law enforcement authorities in Europe.

“Cooperation with the private sector is a prerequisite for the project’s success.”

“Financial technology is a rapidly growing market that provides innovative financial solutions and services such as mobile payments.”
The legislation on money laundering and terrorist financing consists of:

- The administrative law framework, which is based on the fourth anti-money laundering directive and implemented in Sweden through the Anti-Money Laundering Act and the Anti-Money Laundering Regulation.
- The criminal law framework, based mainly on the Act on Penalties for Money Laundering Offences and the Act on Criminal Responsibility for the Financing of Particularly Serious Crime in some cases.

Both of these legislative frameworks have an impact on the Financial Intelligence Unit, which is tasked with preventing, detecting and stopping money laundering and terrorist financing.

The legislation on money laundering has been amended and grown more extensive during a long period of time. 2019 was no exception. During the past year, the Government sent several bills concerning this legislation to the Riksdag (parliament).

New legislation in 2020

The Government Bill Skärpta åtgärder mot penningtvätt och finansiering av terrorism (prop. 2018/19:150) (“More stringent measures for prevention of money laundering and terrorist financing”) introduces new categories of business operators that are obliged to report to the Financial Intelligence Unit, including persons managing and trading in virtual currencies.

In addition, further protections for whistleblowers and improvement measures for international cooperation were introduced. During the year, the Financial Supervisory Authority was given a wider mandate to intervene in cases of violations of the Anti-Money Laundering Act that were committed by foreign credit institutions. The regulatory framework on beneficial owners was also made clearer (prop. 2019/20:14 Ingripanden mot utländska kreditinstitut och vissa andra penningtvättfrågor) (“Interventions against foreign credit institutions and certain other money laundering matters”).

Furthermore, the definition of politically exposed person (PEP) was expanded, and the information exchange and forms of cooperation at the national level between the Financial Intelligence Unit 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 Financial Intelligence Unit should provide feedback, to the extent possible, to business operators that have reported suspected money laundering and terrorist financing (see the memo Vissa förtydliganden i regelverket om åtgärder mot penningtvätt och finansiering av terrorism) (“Certain clarifications of the regulatory framework on prevention of money laundering and terrorist financing”).

All of these changes entered into force during the year, or will enter into force in 2020 at the latest.

In the proposal Ett nytt konto- och värdefackssystem9 (“A new system for accounts and bank safe deposit boxes”), which was referred to the Council on Legislation, the Government proposes the introduction of a new national data search system that enables the Financial Intelligence Unit and other law enforcement authorities to quickly identify physical or legal persons that keep safe deposit boxes or accounts at

---

9 The proposal incorporates the corresponding requirement from the fourth anti-money laundering directive (Article 32(a) into Swedish law..
financial companies. At present, the Financial Intelligence Unit makes requests directly to financial companies.

The new system makes information on owners directly and immediately available through a search on a technical platform that is provided by the Swedish Tax Agency. The proposal provides the Financial Intelligence Unit with a better tool to quickly find out where individuals and companies keep bank accounts, and will make efforts to counter money laundering and terrorist financing more effective.

The system will not give the Financial Intelligence Unit access to more information or other data than what the Unit already is entitled to request from financial companies. For example, information on account balances and transactions will not be included in the system. The system for accounts and bank safe deposit boxes will be regulated in a new law proposed to enter into force on 10 September 2020.

Request to the Government
In a request to the Government\textsuperscript{10}, the Swedish Police Authority asked for a review of the provisions in the regulatory framework on money laundering with the aim of introducing either reporting obligations for providers of third-party services or an obligation for business operators using such third-party providers to report the transaction information that those services generates.

Provisions on reporting in goAML
The Anti-Money Laundering Act establishes that business operators are obliged to hand over all the information needed for conducting investigations on money laundering or terrorist financing to the Swedish Police Authority. As concerns the Act on Prevention of Money Laundering and Terrorist Financing, the Swedish Police Authority has been authorised to issue provisions on how business operators’ reporting to the police is to be done, as well as on how information requested by the police is to be provided.\textsuperscript{11}

The Swedish Police Authority’s provisions on 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 \textit{goAML}).

\textsuperscript{10} Request for law review, ref. no. A540.680/2018.

\textsuperscript{11} Regulation on Prevention of Money Laundering and Terrorist Financing (2009:92), Section 19, second paragraph.
In 2019, the Financial Intelligence Unit received a total of 21,709 money laundering reports from 285 different business operators. This is a 12 percent increase compared to the number of reports the previous year, and an increase of more than 110 percent during the last five years.

One possible reason for the increase is that the number of business operators with compulsory registration has increased during this time, partly due to the introduction of the Act on Prevention of Money Laundering and Terrorist Financing (2017:630), which entered into force in August 2017, and partly due to later amendments of this act.

The largest increase, however, took place in the category banking and financing institutions, continuing a several years long trend. One important explanation is that the sector is growing, and various new operators have been granted banking licenses. However, these operators generally already had some other form of license with a reporting obligation. Consequently, the larger number of operators in the banking sector cannot fully explain the larger number of reports. It is difficult to determine whether the rest of the increase is due to business operators redefining what they choose to report, in accordance with the more explicit legal definition, or due to an actual increase in money laundering.

In addition to banking and financing institutions, the increase is most obvious in the categories financial entities subject to compulsory registration and reporting from other authorities. Reporting from the category professional trading in goods remains at low levels.
Table 1. Number of reports received per sector 2015–2019\(^{12}\)

<table>
<thead>
<tr>
<th>Category</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
<th>2018</th>
<th>2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking and financing institutions including credit market companies</td>
<td>5,700</td>
<td>9,271</td>
<td>12,169</td>
<td>14,421</td>
<td>16,831</td>
</tr>
<tr>
<td>Life insurance businesses</td>
<td>42</td>
<td>17</td>
<td>32</td>
<td>32</td>
<td>42</td>
</tr>
<tr>
<td>Securities businesses</td>
<td>7</td>
<td>..</td>
<td>..</td>
<td>10</td>
<td>19</td>
</tr>
<tr>
<td>Financial entities subject to compulsory registration(^{14})</td>
<td>473</td>
<td>31</td>
<td>27</td>
<td>166</td>
<td>493</td>
</tr>
<tr>
<td>Insurance intermediaries</td>
<td>4</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>Electronic money institutions (including reports by representatives)</td>
<td>148</td>
<td>392</td>
<td>35</td>
<td>50</td>
<td>39</td>
</tr>
<tr>
<td>Investment funds businesses</td>
<td>3</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>Payment services(^{15})</td>
<td>3,415</td>
<td>3,124</td>
<td>3,674</td>
<td>3,764</td>
<td>3,045</td>
</tr>
<tr>
<td>Alternative investment funds</td>
<td>0</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>Consumer credit businesses</td>
<td>6</td>
<td>46</td>
<td>68</td>
<td>149</td>
<td>185</td>
</tr>
<tr>
<td>Mortgage credit businesses(^{16})</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>Real estate agents</td>
<td>3</td>
<td>..</td>
<td>6</td>
<td>..</td>
<td>23</td>
</tr>
<tr>
<td>Gambling services</td>
<td>313</td>
<td>325</td>
<td>381</td>
<td>474</td>
<td>481</td>
</tr>
<tr>
<td>Professional trading in goods(^{17})</td>
<td>36</td>
<td>41</td>
<td>55</td>
<td>37</td>
<td>83</td>
</tr>
<tr>
<td>Pawn shops(^{16})</td>
<td>7</td>
<td>6</td>
<td>8</td>
<td>7</td>
<td>20</td>
</tr>
<tr>
<td>Auditing (approved or authorised public accountant or registered accounting firm)</td>
<td>3</td>
<td>10</td>
<td>8</td>
<td>7</td>
<td>20</td>
</tr>
<tr>
<td>Book-keeping or auditing services (excluding approved or authorised public accountants and registered accounting firms)</td>
<td>10</td>
<td>18</td>
<td>9</td>
<td>16</td>
<td>19</td>
</tr>
<tr>
<td>Tax advisers</td>
<td>0</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>Lawyer or junior lawyer at law firm</td>
<td>4</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>6</td>
</tr>
<tr>
<td>Other independent lawyers</td>
<td>0</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>Company formation, trustees etc.</td>
<td>0</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>Supervisory authorities</td>
<td>3</td>
<td>37</td>
<td>24</td>
<td>23</td>
<td>19</td>
</tr>
<tr>
<td>Other authorities (handling cash) according to the Anti-Money Laundering Act, Chapter 4, Section 4, second paragraph(^{16})</td>
<td>47</td>
<td>133</td>
<td>239</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>10,170</strong></td>
<td><strong>13,322</strong></td>
<td><strong>16,551</strong></td>
<td><strong>19,306</strong></td>
<td><strong>21,709</strong></td>
</tr>
</tbody>
</table>

---

\(^{12}\) The categories correspond to the categories in the Anti-Money Laundering Act from 2017, but business operators (companies) may have several kinds of licenses with the Financial Supervisory Authority and thus report in various categories in the Financial Intelligence Unit’s web reporting system. The web reporting system is unable to verify that reporting is always done in the correct category. Companies that run businesses with different licenses must consider in which of its businesses the suspicion arose and choose the web reporting category accordingly.

\(^{13}\) .. Indicates that the sector submitted five or fewer reports during the year. The reports are included in the total and the accounting method has been used since 2016.

\(^{14}\) Companies registered at the Financial Supervisory Authority but not subject to supervision.

\(^{15}\) The category *Payment services* includes payment institutions and registered payment service providers, including currency exchange.


\(^{17}\) The category professional trading in goods includes auction centres and companies trading in vehicles, scrap metals, precious stones, antiques and art with a value that exceeds EUR 15,000. From 1 August 2017, the threshold value is EUR 5,000.
Restraint orders
The Financial Intelligence Unit is authorised to issue restraint orders for property that it suspects is used for money laundering or terrorist financing. The restraint order is a temporary ban on moving or otherwise making use of the property. The order applies for at most two working days, and must be examined by a prosecutor during that time. In addition, restraint orders may only be issued if delay entails risk and there is reason to believe that the property otherwise may be removed. Furthermore, the reasons for the measure must counterbalance the intrusion or any other disadvantages which the measure would imply.

Table 2. Number of restraint orders and total value 2015–2019

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of restraint orders</th>
<th>Total value (SEK)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>72</td>
<td>7,210,685</td>
</tr>
<tr>
<td>2016</td>
<td>58</td>
<td>21,461,634</td>
</tr>
<tr>
<td>2017</td>
<td>70</td>
<td>15,393,404</td>
</tr>
<tr>
<td>2018</td>
<td>96</td>
<td>64,087,514</td>
</tr>
<tr>
<td>2019</td>
<td>179</td>
<td>168,362,550</td>
</tr>
</tbody>
</table>

In 2019, the Financial Intelligence Unit issued 179 restraint orders with a total worth of more than SEK 168 million. This is an 86 percent increase compared to the number of restraint orders issued the previous year, and an increase of more than 148 percent during the last five years. The amounts that were subjected to restraint orders increased by approximately 260 percent compared to the previous year, and by approximately 2,330 percent during the last five years. The probable explanation is that business operators and the Financial Intelligence Unit, acting on their own and together:

- Have improved their awareness of what may be subjected to restraint orders.
- Have improved their procedures.
- Have set aside more resources to implement them.

However, it is also likely that there is an actual increase, mainly of fraud; this is a predicate offence for which restraint orders are a very appropriate and useful tool.

Filed reports
The level of suspicion required for a business operator to report to the Financial Intelligence Unit is low. The legislation refers to behaviour that deviates from what the business operator may reasonably expect, considering its know your customer information and the products and services it provides, or alternatively behaviour that does not deviate but may be presumed to be a part of a money laundering or terrorist financing scheme. The purpose of the low level of suspicion required for reporting is that the Financial Intelligence Unit should have the possibility to assess reports in cases where other information, unknown to the business operator, may be of vital importance. Frequently, information from several different sources is crucial for further measures.

A consequence of the low level of suspicion required for reporting is that the Financial Intelligence Unit at times does not take any further measures on reports received. However, all reports that are received are assessed, and a large part is processed. Intelligence sharing is mainly done with other law enforcement agencies. At this stage, a report has usually not been filed and no preliminary investigation has been initiated, which means that the work is surrounded by strict secrecy. In this work, information is an important but not crucial part.

In certain cases, the Financial Intelligence Unit already at this stage makes the assessment that there is a sufficient level of suspicion to initiate a preliminary investigation, normally concerning money laundering. In these cases, the Financial Intelligence Unit files a police report. This happened 242 times in 2019. The number has increased compared to the previous year, when the Financial Intelligence Unit filed 177 police reports.
FAQ

What happens when a report is submitted to the Financial Intelligence Unit?
When the Financial Intelligence Unit receives a report, the report is assessed along with other information that is available to the Financial Intelligence Unit. The information may be processed and shared with other entities outside the Financial Intelligence Unit to aid them in their work.

It may also be investigated further within the Financial Intelligence Unit. 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 Financial Intelligence Unit, and what does “reasonable grounds for suspicion” really mean?
The assessment of whether to report to the Financial Intelligence Unit must be based on the business operator’s know your customer information and risk assessments. The level of suspicion required for reporting to the Financial Intelligence Unit 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 most correct way of acting 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.

Are we allowed to tell anyone that we submitted a report to the Financial Intelligence Unit?
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 Financial Intelligence Unit. However, this information may be shared with supervisory authorities and law enforcement authorities, among others, and in certain
circumstances within the group. For more information, see Chapter 4, Section 9, second paragraph of the Anti-Money Laundering Act.

**Is a report to the Financial Intelligence Unit 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 Financial Intelligence Unit is the only operator that has access to the information. A police report may be filed by the Financial Intelligence Unit when a report on money laundering has been processed, if there are sufficient reasons to do so.

A police report should be filed for completed frauds. It is recommended that the defrauded client does this at the police’s website (https://polisen.se/utsatt-for-brott/polisanmalan/) or alternatively at the police’s phone number 114 14. Then, the business operator submits a money laundering report about 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.

**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.

**If the Financial Intelligence Unit asks a question regarding a person, are we supposed to report that person to you?**

When the Financial Intelligence Unit asks a question, it does not equal a suspicion of crime.

A business operator that reviews its client following a request from the Financial Intelligence Unit and finds behaviour that deviates from what may be expected according to its know your customer information should report as per the usual procedure. If, on the other hand, such a review finds no deviating transactions or behaviour and no suspicions arise, the client should not be reported.

**Is it possible to request advice from the Financial Intelligence Unit on whether to submit a money laundering report on a client?**

The Financial Intelligence Unit will not give advice that concerns individual cases, only general advice.