BLACK WALLET

BLACK WALLET REPORTING GUIDE

Recommendations for Payment Service Providers on how to report suspected Money Laundering and Terrorist Financing activities to Financial Intelligence Units

POLIISI
KESKUSRIKOSPOLIISI
Centralkriminalpolisen
National Bureau of Investigation

Polisen
Swedish Police

BLACK WALLET REPORTING GUIDE

Recommendations for Payment Service Providers on how to report suspected Money Laundering and Terrorist Financing activities to Financial Intelligence Units

The Black Wallet Project is funded by the European Union's Internal Security Fund – Police. The content of this document represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Table of contents

List of abbreviations

AML	Anti Money Laundering
CFT	Countering the Financing of Terrorism
Fintech	Financial Technology
FIU	Financial Intelligence Unit
IFT	International Funds Transfer
KYC	Know Your Customer
ML	Money Laundering
PSP	Payment Service Provider
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
UTR	Unusual cash Transaction Report
TF	Terrorist Financing
XML	Extensible Markup Language

Glossary

Suspicious Activity Report (SAR): If suspicions arise in relation to the client's intentions of using the business operator's products or services to launder money or finance terrorism, a SAR containing information on the involved individuals, companies and accounts should be transmitted to the Financial Intelligence Unit (FIU).

Suspicious Transaction Report (STR): If suspicions arise as a result of one or multiple transactions (completed or refused), an STR containing the transactions should be transmitted to the FIU.

Predicate offence: The underlying criminal offence that gave rise to criminal proceeds.

Defrauded: To be a subject or victim of fraud.

Preface

The Black Wallet Project is an EU-funded, joint project between the Finnish and Swedish Financial Intelligence Units (FIU) with support from other competent authorities from the respective countries. During the course of the project, from March 2019 to February 2021, the aim has been to create an overall picture of the Financial Technology (Fintech) sector by examining products and services related to the transfer of funds. Ultimately, the goal is to help law enforcement authorities and the private sector to prevent, detect and investigate Terrorist Financing (TF) and Money Laundering (ML).

One of the cornerstones of the global Anti Money Laundering (AML) and Countering the Financing of Terrorism (CFT) framework is the reporting of suspected criminal financial flows, known as Suspicious Transaction Reports (STR) or Suspicious Activity Reports (SAR), from the private sector to Financial Intelligence Units (FIU). The reports submitted by the private sector contain valuable information that can enhance ongoing investigations or trigger new ones. This is why it is essential that the private sector continues to uphold their obligation to report suspicious activities and contribute to the fight against Money Laundering (ML) and Terrorist Financing (TF).

This guide aims to support the achievement of the Black Wallet Project's goal to quantitatively and qualitatively improve reports from the Financial Technology (Fintech) sector. It is one of the project's end products and accompanied by, for example, trainings and webinars. In order to enhance the way reporting is done in practice, the project also hopes to facilitate a transition from manual to automated reporting.

The Black Wallet Reporting Guide is for the use of obliged Fintech companies, which are most commonly Payment Service Providers (PSP). For this reason, the term PSP is used in this paper to indicate the target group of this product.

The goal of the project is to pave way for a low reporting threshold for obliged entities as well as to ensure high-quality reports. This will support the FIUs and other law enforcement agencies to combat ML and TF within the EU.

Outline

Covering why it's important to report, the first section **(Why report)** describes briefly the concepts of Money Laundering (ML) and Terrorist Financing (TF), as it is fundamental to have proper understanding of the activities that we aim to prevent. This is followed by an explanation of the specific and unique roles and responsibilities of Financial Technology (Fintech) companies in the fight against ML and TF. Next, Suspicious Activity Reports (SAR) and Suspicious Transaction Reports (STR) are described, including when they are required and what happens afterwards.

The second section **(What to report)** focuses on the elements that should be reported in order to provide a high-quality report. This includes quick tips as well as a more detailed description of what a report should contain, including mandatory and valuable information.

The focus of the last section **(How to report)** is on how Fintech companies should make the reports. The section also introduces the goAML system and explains how obliged entities should submit a report in practice.

Why report?

This section outlines the reasons why it is important to report.

Quick tips

- You make the world safer.
- It's crucial for preventing Money Laundering and Terrorist Financing.
- You are obliged to do so by law. If you don't report, authorities can set sanctions or withdraw your licenses.
- If you don't report, you might face a reputational risk.
- If you don't report, you might even commit a crime yourself.
- If you don't report, you could be personally liable for damages based on criminal or civil law.

What are Money Laundering and Terrorist Financing?

Money Laundering (ML) is the process whereby the illicit origin of criminal proceeds is given a seemingly legitimate origin. The aim is to use the money from criminal activities in the legal economy or conceal the funds for further use.

The process of laundering money typically involves three steps:

- **placement,**
- **layering** and
- **integration.**

In the initial – or placement – stage, the launderer introduces his illegal profits into the financial system.

After the funds have entered the financial system, in the second – or layering – stage the launderer engages in a series of conversions or movements of the funds to distance them from their source.

Having successfully processed his criminal profits through the first two phases, the launderer then moves them to the third stage – integration – in which the funds re-enter the legitimate economy. The launderer might choose to invest the funds into, for example, real estate, luxury assets, or business ventures.[1]

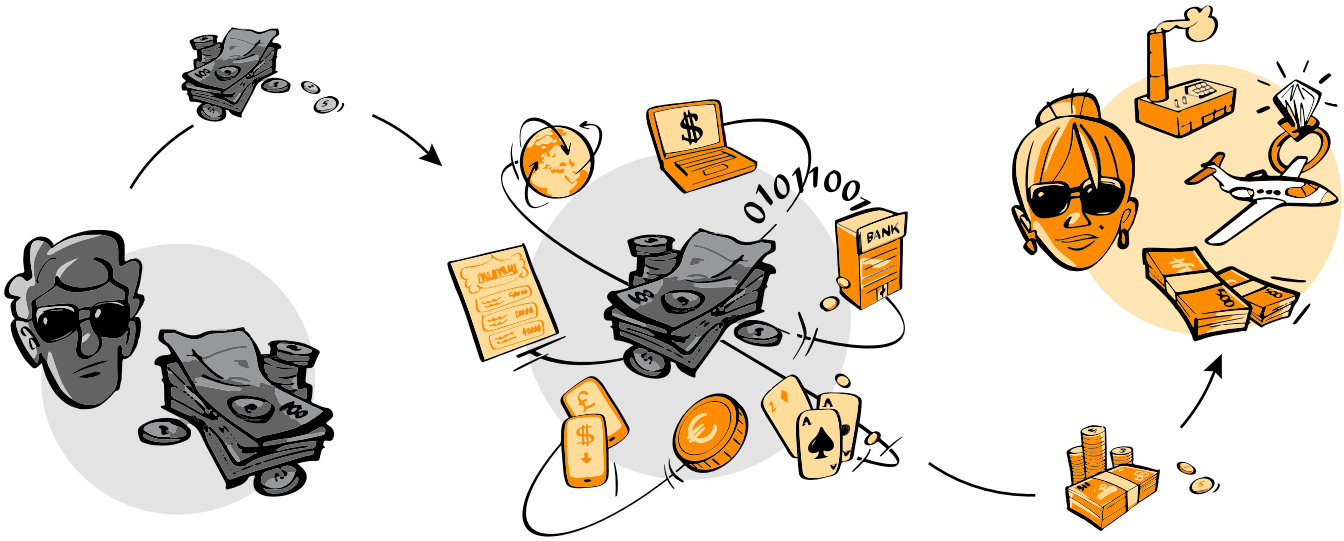
[1] What is money laundering, Financial Action Task Force

Why report?

Terrorist Financing (TF) is the financing of terrorist acts, and of terrorists and terrorist organisations.[2] TF is distinct from money laundering in that it aims to conceal the purpose for which the funds are used, rather than the origin. Such schemes aim to financially support terrorism by direct contributions or indirect methods, such as gathering, receiving or transferring funds and other assets. The funds can come from both legal and illegal sources. Purchases of materials for potential terrorist attacks also fall under the category of TF.

Despite the difference in aims, ML and TF schemes use similar methods to move and conceal funds. Therefore, they are both covered under the scope of the European Anti Money Laundering (AML) framework.

Simplified image of a Money Laundering flow



- **Placement** of the proceeds of crime into the financial system
- **Layering** of the money in order to hide their illegal origin
- **Integration** of the money into the legal economy

[2] Glossary, Financial Action Task Force

Simplified image of a Terrorist Financing flow

- **Placement** of legal/ illegal money into the financial system
- **Layering** of money in order to conceal the purpose of the funds.
- **Storing** funds connected to a terrorist organisation
- **Moving** funds to individual terrorists or terrorist operations

The role and responsibility of Fintechs in the fight against Money Laundering and Terrorist Financing

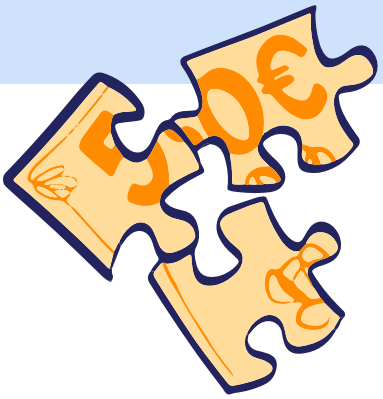
The Fintech sector is a rapidly evolving market that has created innovative financial services. However, the development of new technologies also presents new challenges to the current Anti Money Laundering (AML) framework, including the Suspicious Transaction Report (STR) and Suspicious Activity Report (SAR) regime and the prerequisites for transaction monitoring. There are plenty of opportunities for combating Money Laundering (ML) and Terrorist Financing (TF), as the Fintech companies, for instance, collect important data and can have a bird's eye view of the transaction chains involving several obliged entities.

The annual report from Sweden's Financial intelligence Unit (FIU) has pointed out that Fintech solutions are commonly used in ML/TF: *"In the deceptive layering stage of money laundering, 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 services are frequently used."*[3]

The Black Wallet Project has identified several challenges inherent to Fintech companies that offer payment or money transfer services. In the Risk Indicators Report[4], the Project Group concluded that Fintech services, in particular Payment Service Providers (PSP), face numerous risks related

[3] Annual Report 2019, FIU Sweden

[4] Black Wallet Risk Indicator Report, 2020



to their products and services. The specific challenges faced by Fintech companies ultimately affect their ability to prevent, detect and mitigate financial crime. However, these challenges can be addressed through adequate customer due diligence as well as customer and transaction monitoring. Proper Know Your Customer (KYC) measures and monitoring provisions form a direct link to high-quality STRs and SARs.

Some Fintech companies that offer part of a payment service, money transfer services or a third party service, such as transaction monitoring or KYC service, might have no obligation or direct ways to report to FIUs. In these cases it's important that they provide the obliged partner who can and should report with accurate and detailed information and data for them to make a high-quality report. If the full picture they see is connected to several business partners and they are not allowed to share all data, they need to work on how to describe the situation so that the indications for the suspicion aren't lost.

Fintechs who are obliged entities should recognise the risks of ML and TF and have the capability to send high-quality reports to FIUs. They should not rely on or hand over the responsibility of reporting to other entities, such as banks or other parties involved in a transaction. A criminal could, for example, use several money transmitters or different banks as sources of payments, and a single PSP has the ability to detect additional money flows or is the only one able to see the full picture. A report from a Fintech company can also be a very important piece of a puzzle and help the law enforcement to solve a large case.

PSPs have great possibilities to detect and report TF, as they can, for instance, see patterns in low-value transactions that could indicate fundraising for terrorist purposes. The data they collect can reveal a lone wolf (or lone-actor terrorist) potentially preparing for terrorism activity. During the layering phase PSPs are attractive to use, but many red flags may be triggered and the transactions can be stopped and reported. As the destination of the funds in TF is important, PSPs have an essential role in verifying the payee and/or transferring the information to parties involved in the transaction.

Fintech companies have the technical knowledge, skills and agility to collect data that will be valuable for financial investigations. They are used to handling data such as IP addresses. They have a lot of experience of Extract, Transform and Load (ETL) data projects, which makes them quick to adapt to new things. For them, handling structured data – such as Extensible Markup Language (XML) or JavaScript Object Notation (JSON) and Application Programming Interfaces (API) – is business as usual. Their enthusiasm for process automatisation leads to reports of better quality in the long run and benefits both parties.

It's extremely important that Fintech companies collect and share relevant transaction data with connected business operators in order to see the full transaction chain. This is crucial for being able to create high-quality reports. Also, sharing data shouldn't be prevented by competition between companies over valuable customer data. If the EU Regulation regarding information accompanying transfers of funds[5] isn't followed and the related issues can't be solved, perhaps the business relationship should be terminated or the supervisory authority informed.

The lack of internal guidelines and compliance is a vulnerability in some Fintech companies. It's important to have personnel familiar with relevant legislation and requirements concerning AML/CFT and guidelines for compliance with the ML/TF reporting obligation. The Fintech companies submitting high-quality reports often have created an internal process on how to act when a red flag is identified, for example who will investigate and what happens if the transaction is deemed suspicious.

By sending good-quality STRs/SARs to the local FIU, PSPs can contribute to revealing suspicious behaviour and consequently combatting ML and TF.

What is a Suspicious Activity Report or a Suspicious Transaction Report?

One of the cornerstones of the global Anti Money Laundering (AML) and Countering the Financing of Terrorism (CFT) frameworks is the designation of obliged entities to report suspicious transactions or activities to Financial Intelligence Units (FIU). The reporting framework aims to prevent and detect abuse of the financial system by criminals seeking to launder profits of illegal activities or finance terrorism.

Suspicious Transaction Reports (STR) or Suspicious Activity Reports (SAR) should contain information about the circumstances that form the basis for suspected Money Laundering (ML) or Terrorist Financing (TF). They are distinct from a police report, as submitting evidence regarding money laundering, an associated predicate offence or terrorist financing is not required – only the circumstances that indicate suspicion need to be supplied. However, any documentation that confirms or supports the information in the report should be delivered together with the report, such as account or bank statements, identification documents, contracts or receipts.

In other words, the obligation to report only refers to the suspicion itself. If the relevant FIU assesses that the suspicion reaches a certain threshold, the matter will be forwarded to the relevant law enforcement agencies for further investigation. Therefore,

[5] EU Regulation (EU) 2015/847 on information accompanying transfers of funds

a high-quality report is crucial for the FIU to properly handle potential ML and TF cases.

In order for the FIU to be able to thoroughly investigate a report, the suspicious transaction or activity must be described adequately by the obliged entity. As a rule of thumb, the obliged entity should strive to answer the following key questions:

- Who is conducting the suspicious transaction or activity?
- What instruments or mechanisms are being used to facilitate the suspicious transaction?
- When did the suspicious activity or transaction take place?
- Where did the suspicious activity or transaction take place?
- Why does the obliged entity have reason to believe that the transaction or activity is suspicious?

The format of STRs and SARs differs between countries, although the most common report form is an electronic report. For instance, the Swedish Police Authority has been authorised to issue provisions on how obliged entities reporting is to be done, which state that goAML is to be used as a system for submitting reports. Please check the guidelines of the FIU in your jurisdiction.

Why is it important to report suspicious transactions and suspicious activities?

When obliged entities report suspicious transactions and suspicious activities, the Financial Intelligence Unit (FIU) is able to gain a clearer and more detailed picture of Money Laundering (ML) or Terrorist Financing (TF) schemes. The financial intelligence provided in the reports is a core component of financial investigations. High-quality information increases the FIUs' ability to analyse and make appropriate operational decisions, which can result in uncovering and solving crimes that would otherwise remain undetected. Therefore, it is essential that the supervised entities that are obliged to report suspicious transactions and activities actually do so if the efforts of FIUs to combat money laundering and terrorist financing crimes are to be successful.

Beyond triggering investigations, the reports also provide the FIUs with valuable information on how criminals conceal and move funds, which in turn helps to identify risks, patterns and emerging threats. This type of financial intelligence is crucial for strategic purposes in order to inform and support policy decisions.

Effective and high-quality reporting leads to improved feedback from the FIUs. It can also help the process of creating best practices or methods for reporting, such as the Black Wallet Reporting Guide.

When is a Suspicious Transaction Report or Suspicious Activity Report required?

The international standards regarding reporting have changed over the years. There have been discussions on whether the obliged entities report all transactions above a certain amount, only transactions seemingly connected to criminal activity, or a combination of these.[6] The Financial Action Task Force (FATF) recommendations state that *"if a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU)."*[7] In other words, the obligation of financial institutions to report is intended to provide FIUs with information on transactions, which could stem from criminal activity or from an indication to Terrorist Financing (TF). In addition, the report should be done promptly, without a delay between the arising of the suspicion and actually making the report.

In each EU Member State, the Anti Money Laundering Directive (AMLD) is nationally enforced with domestic Money Laundering (ML) legislations. Without looking into each Member States' acts separately, we could in general state that obliged entities that have reasonable grounds to suspect that a transaction or activity is connected to ML or Terrorist Financing (TF) must submit a Suspicious Transaction Report (STR) or a Suspicious Activity Report (SAR) to the FIU within their jurisdiction. Countries can also have different criteria for what types of reports should be used. For example, in some jurisdictions UTRs (Unusual cash Transaction Report) or IFTs (International Funds Transfer) are submitted. How the report can be submitted also varies between EU Member States.

In the perspective of a "reporting mindset", the Black Wallet Project encourages a low threshold for reporting. It is paramount to acknowledge that without the input from the obliged entities, the FIUs are missing out on crucial information.

Timely and adequate reports from the Payment Service Providers (PSP) form the basis for actions of the FIUs. In other words, if the Fintechs are not doing their part by submitting the reports to the FIUs, the possibilities of combating TF and ML are alarmingly poor.

As a rule of thumb, if you are wondering whether or not to report to the FIU, the Black Wallet Project recommends you to always choose to report.

[6] Financial Intelligence Units: An Overview, p.41, International Monetary Fund, 2004

[7] International Standards on Combatting Money Laundering and Terrorism & Proliferation 2019, p.17, Financial Action Task Force

Why report?

1. What is suspicion or reasonable suspicion?

The FATF recommendations do not explicitly define what a reasonable suspicion is. The recommendations state that *"if a financial institution* suspects or has reasonable grounds to suspect..."[8], which means that countries can give more precise definitions in their national legislation. Consequently, what constitutes a reasonable suspicion can vary in domestic legislation among Member States within the EU and beyond.

The financial institution offering the service has the best capabilities to detect whether the use of their product or service is suspicious or not[9]. Therefore, the definition of what constitutes a reasonable suspicion, which triggers the obligation to report, is determined by what is considered reasonable. This includes normal business practices and systems in the sector in question. It is also good to note that the report only needs to include a description of the suspicion – no evidence of the alleged crime is required.

Within the Payment Service Providing sector, the Black Wallet Project has identified sector-specific red flags, which can be of help when considering the matter of suspicion or reasonable suspicion. These red flags are presented in the Black Wallet Risk Indicators Report. Many triggers can occur together, which generally leads to stronger suspicion, but each case must be assessed on the basis of the circumstances and the customer knowledge available. In addition, other useful indicator listings have been created by supranational organisations (such as FATF[10], EBA[11], EU[12] and Europol[13]), national entities and private companies.

2. What is criminal activity?

The FATF recommendations connect the reporting obligation to criminal activity or TF by stating that *"if a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a* ***criminal activity, or are related to terrorist financing..."***[14]

In practice, offences that constitute *"criminal activity"* vary globally among countries, even though in most countries the obligation is connected to ML.[15]

The crucial point here is the difference between other criminal activities and TF. Criminal activities refer to situations in which the origin of the funds is criminal. In TF, the funds can originate from a legal source, but the intent for which the transaction is done is illegal.[16]

[8] Ibid, p.17

[9] Financial Intelligence Units: An Overview, p.46, International Monetary Fund, 2004

[10] Terrorist Financing Risk Assessment Guidance 2019, Financial Action Task Force

[11] The Risk Factor Guidelines, 2017, European Banking Authority

[12] Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, 2019, European Commission

[13] Internet Organized Crime Threat Assessment, 2019, Europol

[14] International Standards on Combatting Money Laundering and Terrorism & Proliferation 2019, p.17, Financial Action Task Force

[15] Financial Intelligence Units: An Overview, p.46, International Monetary Fund, 2004

[16] Ibid. p.48

Police report and non-disclosure rules

A Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) is not the same as a police report. A police report may be filed by a Financial Intelligence Unit (FIU) once a report has been processed and there are sufficient reasons to do so. However, a police report could, for instance, be filed for completed frauds. It is recommended that the defrauded client files a report directly to the police. The Payment Service Provider (PSP) should also submit a Money Laundering (ML) report about the fraud, if a suspicion of ML or Terrorist Financing (TF) exists simultaneously.

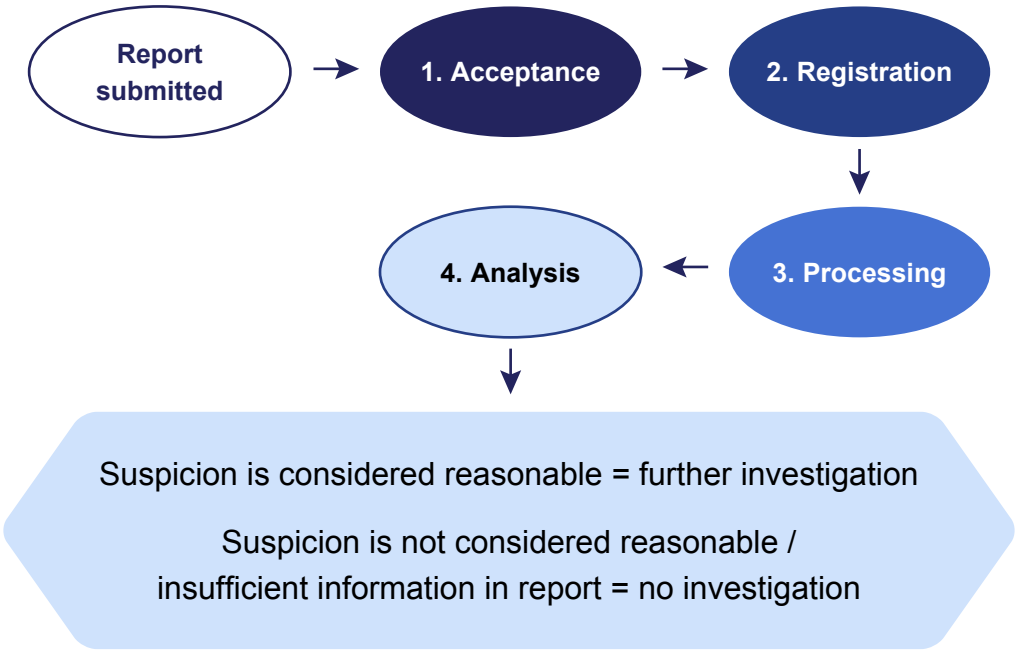
Due to the low level of suspicion, information such as who reported what to the FIU is covered by strict confidentiality. This also applies to individuals and entities of whom the report concerns. This means that the PSP is not allowed to disclose to the customer or client concerned or other third persons that a report or related information was submitted to a FIU.

This issue of confidentiality also has a flip side, as it often could be useful if suspicious activities of a certain entity would be shared with other PSPs. The legal framework for ML and TF includes exceptions so that a company perhaps can share their suspicions with, for instance, third parties involved in a transaction. Please consult your legal team or supervisory authority on this matter.

[16] Ibid. p.48

What happens with a Suspicious Transaction Report or Suspicious Activity Report?

All incoming reports are handled and examined by the FIU equivalent to the following steps:



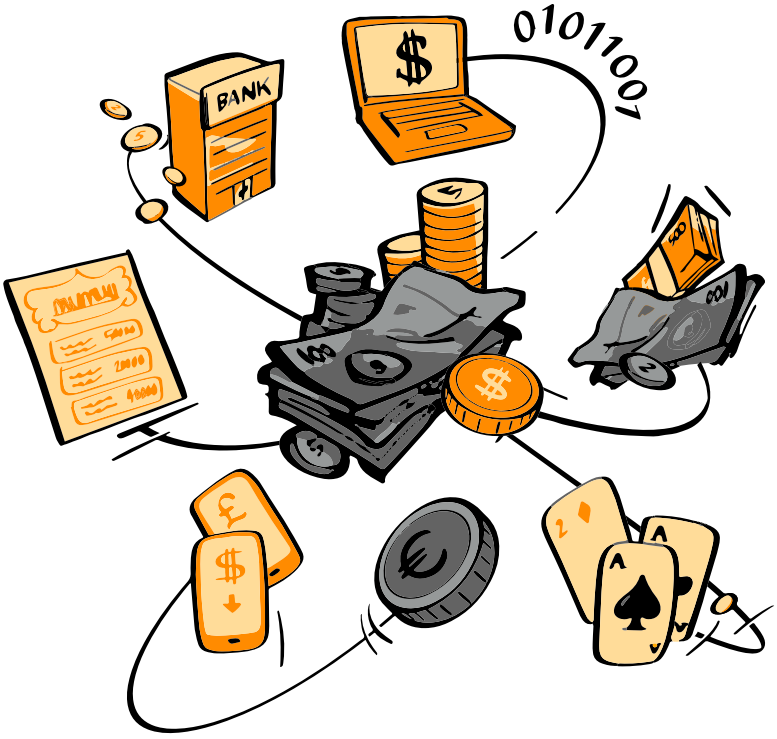
The Financial Intelligence Unit (FIU) investigates whether the reported transactions or activities in the report can be linked to a particular crime or part of a crime related to Money Laundering (ML) or Terrorist Financing (TF). If the FIU finds that the suspicion is sufficiently grounded or otherwise of interest, the report is transmitted for further investigation where the report is enriched with data from several sources available to the FIU and analysed. The FIU might retrieve additional information by request from, for example, the reporting entity, and other entities or FIUs. The result from the report is then disseminated to relevant authorities either separately or in a larger case as a piece of a puzzle, or the report is transmitted to other FIUs. The precise flow and information gathering can vary a little, as FIUs can be established in different ways, but the core function of receiving, analysing and disseminating reports from the obliged entities remains.

If TF or predicated crime is suspected, an intelligence file is usually sent immediately to the relevant law enforcement agency for further assessment.

Even if the report does not reach the level of suspicion required to take action, it does not automatically mean that it is discarded. The FIUs save reports that are not transmitted for further investigation in case new information appears or new connections are made that warrant a re-examination of the file.

Furthermore, the reports are very important, as they are used as a basis for larger analyses and to detect early stage trends or new methods of ML and TF. These analyses are used, for instance, to provide information, training and feedback for authorities and the private sector for the purpose of creating mitigation measures for ML and TF. The analyses will also contribute to information for the public about how to avoid being utilised by criminals.

Due to the fact that there are many scenarios for the outcome of a report, it's often difficult to give feedback on a specific report. The feedback required from the FIU to reporting entities may vary between Member States, but the aim should be to give it to the full extent possible. Often it is possible to provide early feedback on the quality of the report, e.g. if it contains errors, whereas the possible result from a report is difficult to give. Feedback is therefore often given in general or sector-specific guidelines, trainings, or in meetings discussing a broader set of reports.



What to report?

Quick tips

- Briefly summarise your suspicions.
- Include a description of the events in chronological order.
- Write clearly, concisely and simply, and avoid unnecessary repetition.
- Structure your report in a logical way and include all relevant data.
- Avoid abbreviations and internal industry jargon that can be misunderstood.
- If a service or technical aspect of the work is described, it is advisable to provide a brief description of this in the report.
- If the report contains a lot of text, divide it into sections.

Essential elements of a report

A Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) should identify the essential elements of the suspicious activity or transaction being reported. In addition, as sub-matters of these elements, there are several attributes that can be useful to the Financial Intelligence Units (FIU).

Below you can find the essential elements:

1. Who?

Person or company: The report should include information about the involved individual(s) / company or companies. This includes but is not limited to the name, address, social security or tax ID, birth date, driver's license number, passport number, occupation, e-mail address, account number and phone numbers of all parties involved in the suspicious transaction or activity.

Any known relationships among the parties should be disclosed.

2. What, when and where?

Transaction and account: The report should describe, in as much detail as possible, what suspicious activity or transaction is being reported, as well as when and where it/they took place or were first flagged by the obliged entity.

The instruments or mechanisms used in the suspicious transaction or activity should be described, such as, but not limited to, wire

transfers, credit institutions, trade instruments, casinos, bank accounts, shell companies, bonds/notes, stocks, insurances, credit/debit cards, payment accounts, digital/virtual currencies.

If the transaction or activity takes place over an extended period of time, an indication of when the suspicion first arose should be noted, as well as a description of the duration of the activity.

If the suspected activity or transaction involves a foreign jurisdiction, the name, address and any account number of the foreign institution(s) should be given.

For some Fintech companies situations may occur when it's difficult to understand which transactions to report. It's then good to focus on the actual suspicion in the transaction chain and provide the full picture, including all relevant transactions. Such cases could be further discussed with your local FIU.

3. Why and how?

The report should also include a description of the suspicious transaction or activity. In other words, the obliged entity should, in as much detail as possible, provide a description/explanation of why the transaction or activity is unusual for the customer.

If possible, a description of the method of operation (modus operandi) of the subject conducting the suspicious transaction or activity should be given. Any pattern identified in the customer's behaviour should be described and provided as completely as possible.

4. Have any measures been taken by the reporting entity? If so, what and when?

In addition, the obliged entity should include an explanation of any measures that have been taken against the reported suspicious transaction or activity. For instance, if the customer relationship has been terminated, services (e.g. international transfers) temporarily stopped, or additional information requested from the customer that might be available at a later stage.

If a police report has also been submitted, the reference should be added so that important information from the money laundering register can be added to the preliminary investigation.

Mandatory vs valuable data

In addition to what was discussed above, we can make a distinction between mandatory and valuable data, as there are different types of data enclosed in the reports from obliged entities. **Some of the data is mandatory and some is not.**

It is also important to note that the desired or required format of data in reports can vary between EU Member States.

Mandatory data

This refers to the mandatory requirements or best practices for reporting and law enforcement inquiries, which includes data that is consistently available for most Payment Service Providers (PSP). **It should be noted that since national Anti Money Laundering (AML) legislations may differ, in some countries it can be mandatory to provide data that is not mandatory in others.** However, the matter of mandatory data is also connected to the EU regulation, such as the regulation on information that accompanies transfers of funds[17], which is compelling to all.

As a rule of thumb, the following data is likely to be mandatory for you to provide:

- the name of the payer
- the payer's payment account number
- the payer's address, official personal document number, customer identification number or date and place of birth
- the name of the payee
- the payee's payment account number

You can find more detailed information about the matter of mandatory data from your local Financial Intelligence Unit (FIU) or supervisory authority. Required data is also commonly described in the instructions and manuals for reporting.

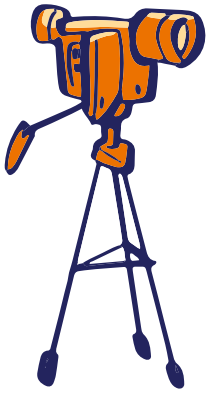
Valuable data

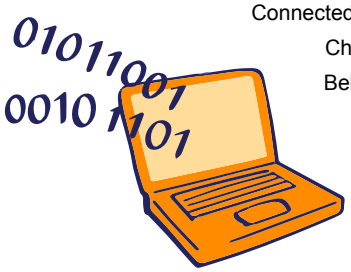
As mentioned earlier, Fintechs often collect data that can be very valuable for financial investigations, such as IP addresses, hardware used, purchased items and secondary identifiers (nicknames). FIUs are able to identify networks of suspected money launderers and terrorist financiers through pieces of information. This type of information may seem insignificant but can be very important to FIUs, as it may identify connections among individuals, entities or crimes when compared against other intelligence data. Some data perhaps can't be included in the report (such as video material), but it is advisable to inform the FIU that such data exists.

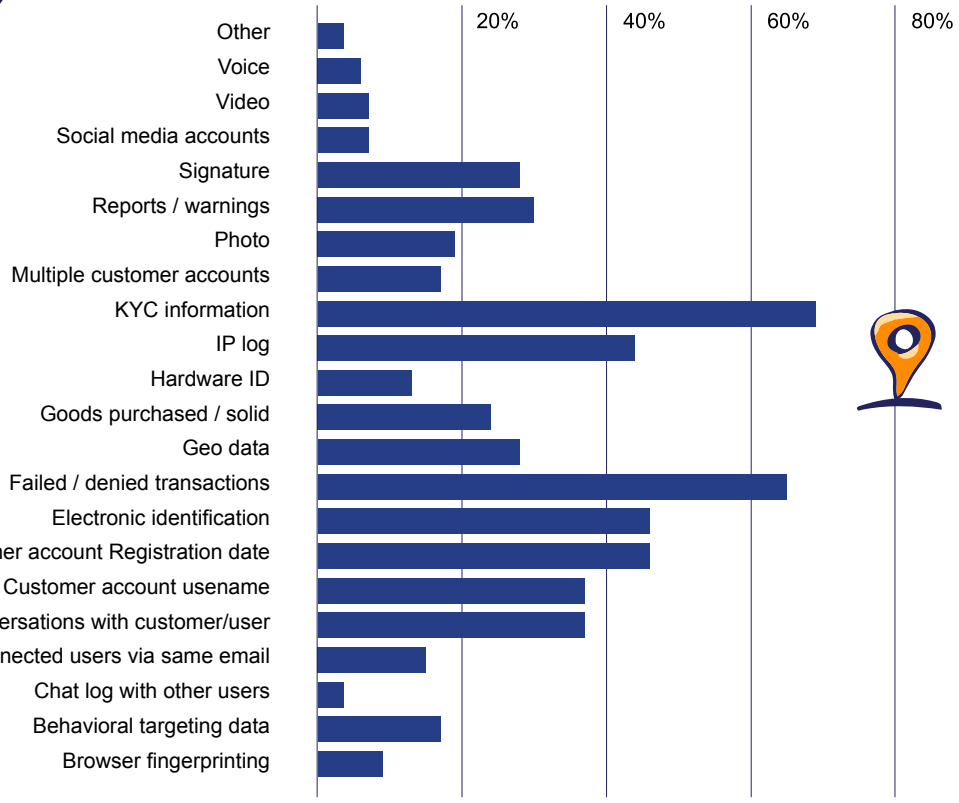
The graph on the next page shows the kind of data beyond regular transaction data collected by Fintech companies. This information was provided through a Black Wallet survey where not all the companies that answered were obliged entities.

[17] EU Regulation (EU) 2015/847 on information accompanying transfers of funds, Article 4.

Example of occurrence of valuable data among Fintech companies based on the Black Wallet Online Survey.







How to report?

This section will discuss how Payment Service Providers (PSP) should report. It is important to note that since reporting systems may vary, you should always consult the Financial Intelligence Unit(s) (FIU) of the country or countries to which you are obliged to file reports.

Quick tips

- ✓ Contact your Financial Intelligence Unit and register as a reporting entity
- ✓ Consider making automated reports
- ✓ Start reporting!

Reporting software – goAML

Even though other systems exist, in many countries Suspicious Activity Reports (SAR) and Suspicious Transaction Reports (STR) are submitted through the IT software goAML.

goAML is produced by the United Nations Office on Drugs and Crime (UNODC) and jointly developed with FIUs from all over the world. As of today (September 2020), 111 FIUs are engaged, among whom 56 have already deployed goAML[18].

The system includes a web client software for reporting entities and stake holders, and a back office client software for the FIU use. goAML is specifically designed to meet the needs of FIUs regarding data collection, management, analytical, document management, workflow and statistics.

The user of the software has to register in order to use the system. The registration has two levels – organisation and user. After FIU approval, the user may send reports to the FIU using the web client provided.

The FIU provides documentation for registration and using the software. Every FIU may configure its implementation of goAML with relevant categories and data. These are set through an Extensible Markup Language (XML) schema (XSD) where the FIU can set mandatory pieces of information and, for example, make some data obsolete altogether. The implementation

[18] What is goAML?, United Nations

instructions for goAML are distributed by each FIU through goAML and are either publically accessible or available after registration.

Reports are submitted through a web portal. All communication between the reporter and the FIU is also conducted through the portal. For instance, if a report does not meet the general requirements, the report will be declared inadmissible and the reporter will be sent a message about the missing information through the messaging function in goAML

There are two ways to report suspicious transactions and activities in the goAML web portal:

- submitting an XML file
- submitting a report manually

Entities that regularly submit reports or file complex reports are advised to create an IT solution for XML reporting. This makes reporting easier and quicker for the obliged entities. The Fintech sector has a great advantage here in that their data often already is easy to access and well categorised. The Black Wallet Project strongly recommends Fintech companies to implement automated reporting.

Reporting using an XML file

XML is a tool for saving and sharing data in a structured way by categorising data according to a specific schema. The information could be, for instance, address lists or transaction logs. Categorising the data creates a schema that facilitates data processing and enables high-volume processing.

The global XML schema for goAML is universal, but there are small differences in how local FIUs implement it. Entities planning to start reporting suspicious activities or transactions using an XML file are strongly encouraged to contact their local FIU before getting started.

The XML schema tells the user what information to include and how to structure it. It also shows what fields need to be filled in and in what unit.

Manual reporting

Obliged entities can also create reports manually by filling in and submitting an online form on the FIU's goAML website. The goAML Web is part of the goAML system, which means the report to the FIU will be structured. Therefore the input of data is required to follow the same rules as for an XML report in regards to mandatory data and format.

Conclusion

In this guide, we have sought to provide information about Money Laundering and Terrorist Financing and why and what should be reported to the Financial Intelligence Units.

If you are reading this as a representative of a Payment Service Provider, the biggest takeaway should be the realisation that what you do actually counts and you can make a difference. When you report, you can save somebody from losing money and stop a criminal. You may prevent people from getting seriously injured or even save their lives. You should always remember this when you are working at the office. Remind yourself: my work matters.

Most crimes share a common denominator: the financial motive. Fighting Money Laundering and Terrorist Financing goes hand in hand with investigating the crimes it is linked to. Often criminal activities yield profits that criminals then seek to launder, and tracing the assets means tracing the criminal, networks and organised crime groups.

One of the cornerstones of the global Anti Money Laundering and Countering the Financing of Terrorism framework is the reporting of suspected criminal financial flows. Therefore the obliged participation from your company and other stakeholders in the Fintech sector in this fight is crucial. Submitting high-quality reports will make a difference!

Sources

Legislation

REGULATION (EU) 2015/847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R0847

Other

Black Wallet Project. Black Wallet Risk Indicators Report, 2020.

European Banking Authority. The Risk Factor Guidelines, 2017. https://eba.europa.eu/sites/default/documents/files/documents/10180/1890686/66ec16d9-0c02-428b-a294-ad1e3d659e70/Final%20Guidelines%20on%20Risk%20Factors%20(JC%202017%2037).pdf

European Commission. Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, 2019. https://op.europa.eu/en/publication-detail/-/publication/0b2ecb04-aef4-11e9-9d01-01aa75ed71a1/language-en

Europol. Internet Organized Crime Threat Assessment, 2019. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment#fndtn-tabs-0-bottom-2

Financial Action Task Force. What is money laundering? https://www.fatf-gafi.org/faq/moneylaundering/

Financial Action Task Force. International Standards on Combatting Money Laundering and Terrorism & Proliferation, The FATF Recommendations, 2019. http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/fatf%20recommendations%202012.pdf

Financial Action Task Force. What is money laundering? https://www.fatf-gafi.org/glossary/s-t/

Sources

FIU Sweden. Financial Intelligence Unit Annual Report, 2019. https://polisen.se/siteassets/dokument/polisens-arsredovisning/fipos-arsrapport/financial-intelligence-unit_annual-report-2019_webb.pdf

International Monetary Fund. Financial Intelligence Units: An Overview, 2004. https://www.imf.org/external/pubs/ft/FIU/fiu.pdf

United Nations. goAML Anti-Money Laundering System. https://unite.un.org/goaml/


POLIISI
KESKUSRIKOSPOLIISI
Centralkriminalpolisen
National Bureau of Investigation


Polisen
Swedish Police