BLACK WALLET

BLACK WALLET
BEST PRACTICES GUIDE

Insights on what Fintechs offering payment services should consider in countering Money Laundering and Terrorist Financing

POLIISI
KESKUSRIKOSPOLIISI
Centralkriminalpolisen
National Bureau of Investigation

Polisen
Swedish Police

Table of contents

List of abbreviations **4**

Glossary **4**

Introduction **5**

Crucial role of Fintechs in preventing Money Laundering and Terrorist Financing 5

Fintechs as obliged entities 6

Money Laundering and Terrorist Financing in a nutshell 8

Recommendations for Fintechs in combating Money Laundering and Terrorist Financing **11**

Overcoming the threat of non-compliance 13

Handling the Fintech-specific features 14

Securing the transparency and traceability of the transaction 15

Cooperation with the authorities 16

What does it mean to be an obliged entity? **18**

Risk-based approach and risk assessment 19

Customer Due Diligence 20

Identification and verification of the customer 21

Obtaining information about the customer 22

Monitoring transactions and customer behavior 22

Guidelines and training 23

Reporting to Financial Intelligence Units 23

Why report? 24

What and how to report? 25

Sources **26**

Best Practices Guide is one of the end products of the Black Wallet Project. The purpose of this product is to provide Fintech companies with insights on what they can and should do to prevent Money Laundering (ML) and Terrorist Financing (TF).

Best Practices Guide is supported by two complementary end products: Black Wallet Risk Indicators and Black Wallet Reporting Guide.

Black Wallet Risk Indicators targets Payment Service Providers (PSP) and Financial Technology (Fintech) companies in order to help companies identify, assess and mitigate risks that may arise in relation to their products and services.

Black Wallet Reporting Guide is designed for the same audience but focuses on the importance of reporting suspected ML and TF activities to Financial Intelligence Units (FIU).

The Black Wallet Project would like to thank Fintech Finland, Swedish Fintech Association and Fintrail, co-founder of Fintech Fincrime Exchange, for their comments and support in creating this guidebook.

The Black Wallet Project is an EU-funded, joint project between the Finnish and Swedish FIUs with the support of other competent authorities from the respective countries. During the course of the project (March 2019 to February 2021), the aim has been to create an overall picture of the Fintech sector by focusing especially on products and services related to the transferring of funds. Ultimately, the project will help relevant law enforcement authorities and the private sector to prevent, detect and investigate ML and TF.

List of abbreviations

AML	Anti Money Laundering
CFT	Countering the Financing of Terrorism
CDD	Customer Due Diligence
Fintech	Financial Technology
FIU	Financial Intelligence Unit
KYC	Know Your Customer
ML	Money Laundering
NPM	New Payment Method
PSP	Payment Service Provider
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TF	Terrorist Financing

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 FIU.

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

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

Introduction

Crucial role of Fintechs in preventing Money Laundering and Terrorist Financing

The Fintech sector is a rapidly evolving market that offers new and innovative products and services related to the transferring of funds. Although Fintech solutions most definitely create new opportunities in a positive sense, they can also give rise to new methods of ML and TF. Fast, complex and cross-border transactions challenge the capabilities of both Fintechs and credit institutions as well as authorities.

The Financial Action Task Force (FATF) has recognised the significance of Fintechs. In the 2010 report on Money Laundering Using New Payment Methods, FATF mentions three main typologies related to the misuse of NPMs for ML and TF purposes, which are

1. third-party funding (including straw men and nominees)
2. exploitation of the non-face-to-face nature of NPM accounts
3. complicit NPM providers or their employees.

Furthermore, the report noted the following: *"Anonymity, high negotiability and utility of funds as well as global access to cash through ATMs are some of the major factors that can add to the attractiveness of NPMs for money launderers".*[1]

In addition, in 2017, the FATF held a Fintech and RegTech Forum at which it was concluded that the fight against ML and TF is a common goal. Furthermore, it was held that the only way to achieve this goal was through co-operation.[2] FATF has emphasised the need to focus on new payment products in relation to possibilities of TF.[3] FATF has also expressed strong support for responsible financial innovation in line with the FATF standards to Anti Money Laundering (AML) and counter-terrorist financing.[4]

Furthermore, the International Monetary Fund (IMF) has recognised the need for enhanced international cooperation when it comes to benefiting from Fintech and mitigating the emerging risks in relation to, inter alia, ML and TF.[5]

In other words, it is widely recognised that cooperation between authorities and Fintechs is paramount in order to prevent ML and TF.

[1] Money Laundering Using New Payment Methods 2010. Financial Action Task Force.

[2] Chairman's Summary of the FATF FinTech and RegTech Forum 2017. Financial Action Task Force.

[3] OBJECTIVES FOR FATF – XXIX (2017–2018) PAPER BY THE INCOMING PRESIDENT Priorities for the Argentine Presidency of FATF (2017–2018) EXECUTIVE SUMMARY. Financial Action Task Force.

[4] FATF FinTech & RegTech Initiative. Financial Action Task Force.

[5] The Bali Fintech Agenda, *IMF Policy Papers*. International Monetary Fund.

Since the majority of the Fintech companies offering services related to the transferring of funds are obliged entities, they are required to report suspicious activities to the FIU in their jurisdiction. Reporting suspicious activities is crucial in tackling ML and TF and preventing criminals from exploiting the products and services in the long run. Obliged Fintechs that are under AML legislation should combat ML and TF because

- non-compliance can lead to supervisory authorities revoking the licence to offer services
- non-compliance may lead to severe financial losses in terms of penalties set by the supervisory authorities
- non-compliance can lead to liability for damages based on civil or criminal legislation
- not complying with the AML legislation may lead to reputational harm.

As discussed above, Fintechs and authorities need to cooperate. Furthermore, it is unequivocally everybody's business to prevent ML and TF. As authorities can't do it alone, your contribution matters.

Fintechs as obliged entities

In general, Fintechs are defined as technology-based companies that provide financial services and products or attempt to streamline the financial system. Fintech as an umbrella term covers various services, which include payments and related services, e.g. regulatory technology such as Know Your Customer (KYC) and monitoring. However, it is not defined by law and does not have a legal status. Therefore, no single definition of the concept exists.

Payment services, as defined in the Payment Service Directive 2 (PSD2), can be provided by credit institutions and entities regulated by the PSD2.6 Even though credit institutions are the most common PSPs, payment institutions, which are relatively new, are nowadays regulated entities allowed to provide their services in the market.

In principle, there can be two types of payment institutions as PSPs:

1. **Payment institution** is an authorised PSP.
2. **Exempted payment institution** is a PSP exempted from the authorisation.

Fintechs are considered regulated entities if the service they provide constitutes a regulated service and they operate under the AML Directive (AMLD).[7] As only regulated entities are obliged entities, not all Fintechs are considered obliged entities. The significance here is that only obliged entities are required to assess ML and TF risks, to conduct Customer Due Diligence (CDD), that is, performing KYC measures and to report suspicious transactions to FIUs.

Obliged entity refers to the AML obligation of financial institutions, which includes performing KYC measures and reporting of suspicious financial activities and suspicious transactions to the FIUs.

A Fintech company that provides purely technical services to another Fintech who is a PSP is not an obliged entity. However, the Fintech company might simultaneously provide another regulated service or services and therefore fall within the scope of the AMLD. Subsequently, this makes the company an obliged entity.

In short, Fintechs can be categorised in the following ways:

- **Provides services defined as payment services in the PSD2** and thus falls within **the scope** of the **AMLD**. In this case, the Fintech company would commonly be referred to as PSP → obliged entity.
- **Provides services that are not payment services in the PSD2 but might be regulated in another capacity under AMLD** → obliged entity.
- **Provides services that fall neither in the PSD2 nor AMLD** (e.g. purely technical services, such as ID verification or technology for transaction monitoring) → non-obliged entity, i.e. an external entity to whom some of the functions are outsourced.

In addition, institutions that provide other payment services may also issue e-money, which is defined in the Electronic Money Directive.[8] Issuing e-money is a regulated service, and the service provider issuing e-money has to predominantly be licensed to do so. Therefore, e-money institutions are obliged entities as well.

[7] DIRECTIVE (EU) 2015/849.

[8] DIRECTIVE 2009/110/EC.

Money Laundering and Terrorist Financing in a nutshell

Most organised crime shares a common denominator: a financial motive.[9] Generating profit is the goal of a large number of criminal acts. ML refers to the processing of criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables criminals to enjoy these profits without revealing their source.[10] ML is an offence in and of itself but can also be related to other forms of serious and organised crime as well as the financing of terrorism. Areas of organised crime include, e.g. illegal arms sale, child sexual exploitation, smuggling, drug trafficking and human trafficking.

The scale and scope of ML is difficult to assess but considered to be significant. The United Nations Office on Drugs and Crime (UNODC) estimates that between 2–5% of the global GDP is laundered each year. This equates to 715 billion to 1.87 trillion EUR per year.[11]

TF has a different aim from ML, as the objective is to conceal the purpose for which the funds are used rather than the illegal origin. Terrorists require financing to recruit and support members, maintain logistics hubs, and conduct operations. Terrorist organisations may be supported by direct contributions or indirect methods, such as gathering, receiving or transferring funds and other assets. Purchases of materials to be used in terrorist attacks also fall under the category of TF.

The funding mechanisms of TF consist of diverse licit and illicit sources. The European Union Terrorism Situation and Trend Report 2017 acknowledges the young age of a large proportion of jihadists and their ability to use a variety of modern technological financial services. These financial services and applications are fluid, encrypted and partially anonymised, which provides a desirable channel for terrorists seeking borderless, real-time and small-value transfers.[12]

Despite the difference in aims, ML and TF schemes use similar methods to move and hide funds. Therefore, both ML and TF fall within the scope of the European AML framework.

- ML refers to the processing of criminal proceeds to disguise their illegal origin.
- TF aims to conceal the purpose for which the funds are used.
- ML and TF schemes use similar methods to move and hide funds.

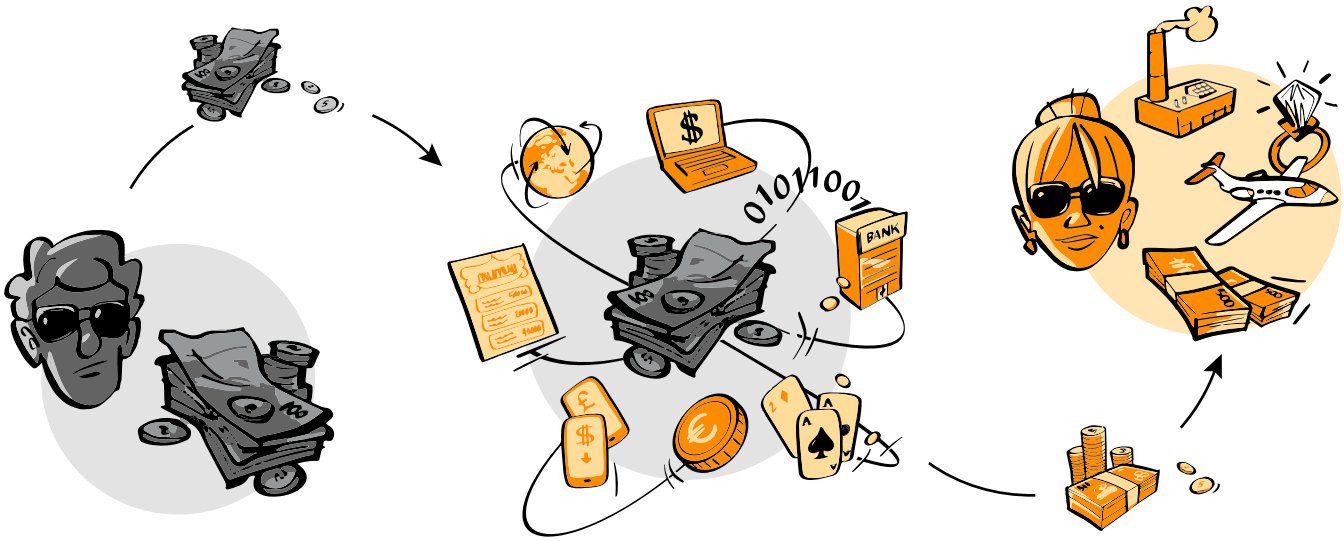
[9] Money Laundering, Europol.

[10] What is Money Laundering, Financial Action Task Force.

[11] Money Laundering and Globalization, United Nations Office on Drugs and Crime.

[12] European Union Terrorism Situation and Trend Report 2017.

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 its illegal origin
- **Integration** of the money into the legal economy

The process of laundering money typically involves three steps: Placement, Layering and Integration.[13] In practice, the perpetrator will first generate money via a predicate offence, such as child sexual exploitation, trafficking of human beings, fraud, cybercrime, tax evasion, or drug trade.

The perpetrator will place the proceeds of crime (Placement) into the financial system by, e.g. using a bill payment service at a PSP's agent. The PSP's agent, in turn, transmits the money to accounts controlled by the perpetrator but opened by another person.

The perpetrator then creates a layer (Layering) of distraction by making payments to a different PSP's payment accounts, which he or she can use via payment cards or a payment application.

By now, the perpetrator has a payment method with seemingly legal money at his or her disposal. Having successfully processed his or her 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, business ventures, or financing further criminal activities.

[13] What is money laundering, Financial Action Task Force.

Simplified image of a Money Laundering 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

Terrorist acts can arguably be executed with relatively small sums of money. Therefore, the flow of money related to such acts may be low and possibly hard to detect. For this reason, the associated red flags may differ when looking at TF. Nevertheless, everything in the world costs something: clothes, cars, gasoline, food and flight tickets are expenses for the terrorists just like for everybody else.

TF can happen in various ways. For example, a terrorist cell can start using social media for falsely promoting an opportunity to provide charity to children in need. People who sympathise can be attracted by the idea and start collecting donations, not knowing that they are actually collecting funding for terrorists.They may want to collect the funds to their bank accounts and subsequently to their PSP's payment accounts. Then they can transfer the funds onwards to the next level of money collectors who have their payment accounts held by another PSP in another country and who eventually direct the funds to be used for terrorist purposes.

Recommendations for Fintechs in combating Money Laundering and Terrorist Financing

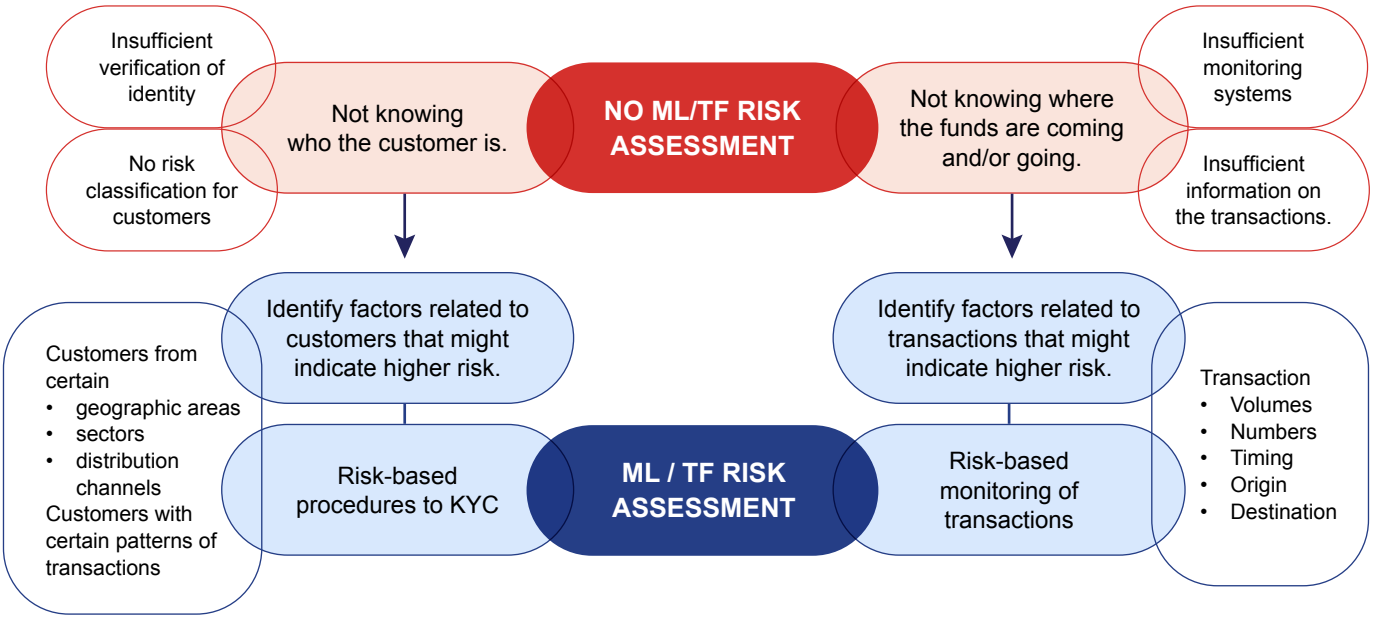
PSPs facilitate payments between private persons or between companies and their customers. In addition, a PSP might provide payment accounts, payment cards or e-money services that are inherently connected to movement of funds from one place or person to another.

Many PSPs and other types of Fintechs aim to provide services that make payments effortless and easy for customers. They provide fast transactions, which is a good thing from a regular customer's point of view but also enables criminals to move their funds faster. PSPs and Fintechs also primarily provide services online without the need to visit a physical location. This is convenient for most customers and for criminals as well.

PSPs should always assess risks related to the products and services they provide, their customers, the geographic areas in which they provide services, and the distribution channels they use. Failing to conduct a risk assessment will affect the PSP's ability to comply with other AML/Countering the Financing of Terrorism (CFT) obligations that should be applied following a risk-based approach. This will cause vulnerabilities and shortages in mitigation measures, as illustrated below.

The risk scenario

Funds from illicit origin may be moved from one place/person to another using payment services or stored on a payment account provided by payment service provider. This can be avoided with proper risk assessment and mitigation measures.

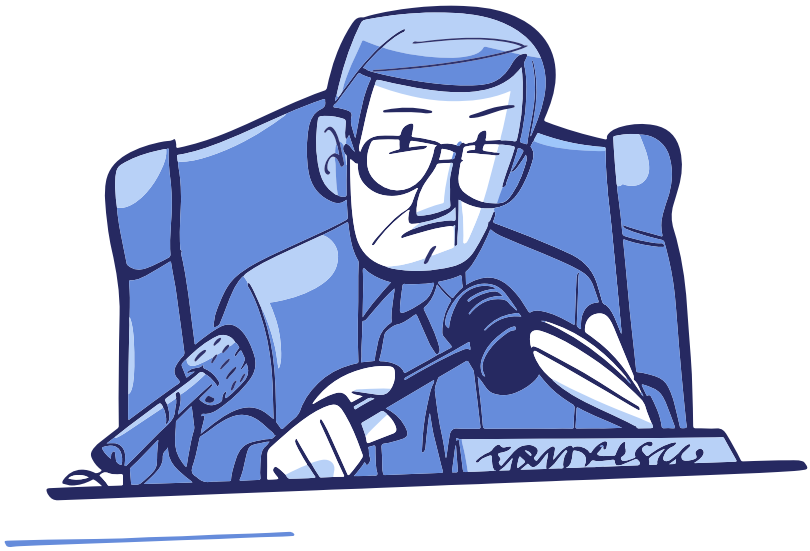


The following chapters will offer you quick tips on what to take into account when preventing ML and TF. These issues are divided into four topics:

1. Overcoming the threat of non-compliance
2. Handling the Fintech-specific features
3. Securing the transparency and traceability of transactions
4. Cooperation with the authorities

Black Wallet Risk Indicators is a product dedicated for helping Fintechs in detecting ML and TF.

Please check it for more information.

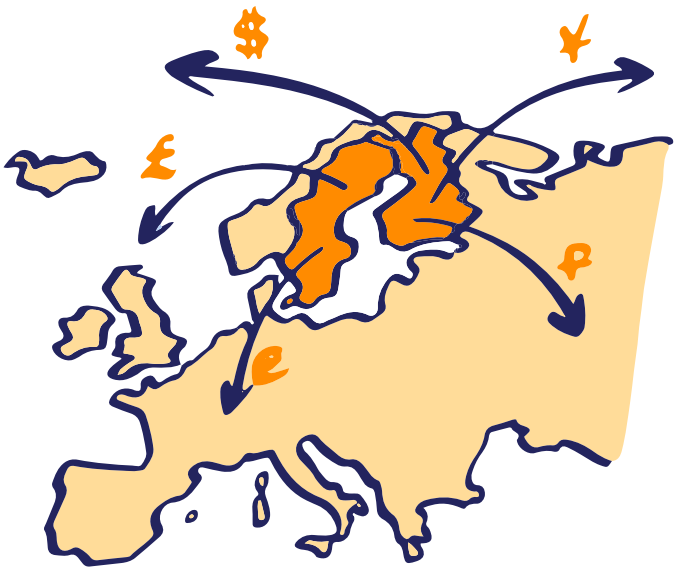


Overcoming the threat of non-compliance

There will always be perpetrators looking for ways to use financial services for illicit purposes. This poses a threat to Fintech companies' capacity to comply with legal obligations, especially if the companies aren't aware of the underlying risks in their services.

Quick tips

- Conduct the risk assessment and make sure it is relevant specifically to your services.
- Make sure your KYC procedure is solid.
- Make sure your staff is trained and there are adequate systems to detect relevant red flags.
- Make sure to report suspicious activity and transactions to the FIU in your jurisdiction.
- Make sure to continuously update the above steps.



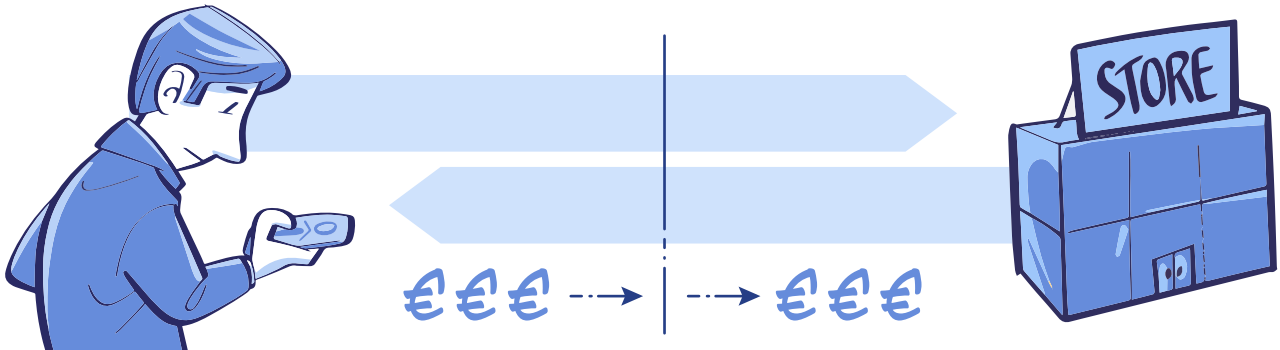
Handling the Fintech-specific features

Fintech companies typically provide easy-to-use, fast-paced and complex transaction services in multiple geographical locations through online platforms or applications. As such, Fintech companies might not have the capabilities to deal with perpetrators who seek to exploit these features for illicit purposes.

Quick tips

- Make sure to map the vulnerabilities in your product or service, such as possible issues with anonymity.
- Make sure you have proper red flags in place to detect possible ML and TF cases.
- Make sure your monitoring matches the speed of your service.
- Make sure you are aware of the risks related to other geographical locations.
- Make sure that you have proper control measures for money travelling across borders.

Securing the transparency and traceability of the transaction



If Fintech companies offer services that provide a degree of anonymity or where traceability of transactions is cumbersome, there is a threat that perpetrators will take advantage of it. In addition, Fintech services often rely on other services, which can lead to a situation in which data is separated among different entities. It is also possible that Fintechs offer services to people who are not their own customers.

Quick tips

- Make sure that the Application Programming Interfaces (API) between you and others – credit institutions or other PSPs – allow transmitting at least the mandatory information.
- If you are the payer's PSP, make sure to transmit the mandatory information with the funds.
- If you are the intermediary PSP, make sure that you retain the mandatory information with the funds.
- If you are the payee's PSP, make sure to check that the mandatory information accompanies the funds.
- Remember that the reporting threshold of suspicious activity is low.
- Make sure you don't pass reporting because you expect somebody else to do it. Double reporting is not a problem, but non-existing reports can have a severe effect.

Cooperation with the authorities

To be successful in fighting ML and TF it's highly recommended to cooperate with authorities and also with other businesses and networks. For example, information of new modus operandis for ML and TF are distributed by the local FIU (e.g. via the reporting system to registered obliged entities) or by supranational authorities, such as The Financial Action Task Force (FATF), Interpol and Europol.

The concept of intensive cooperation between public agencies and private financial institutions has become mainstream. Such partnerships can support the sharing of tactical information, enhance ongoing law enforcement investigations, and, at a strategic level, enable the exchange of insights relating to financial crime threats and risks.[14]

It can be highly useful in other contexts as well to share knowledge of, for example, best practices, modus operandis and technical solutions, which can help combating ML and TF. This can happen in various ways: in conferences, in communication within the industry, and through domestic or global expert networks, such as Fintech FinCrime Exchange (FFE).[15]

[14] For further information: Survey Report: Five years of growth in public-private financial information-sharing to tackle crime. Global coalition to fight financial crime.

[15] For further information: FinTech FinCrime Exchange (FFE) website.

Quick tips

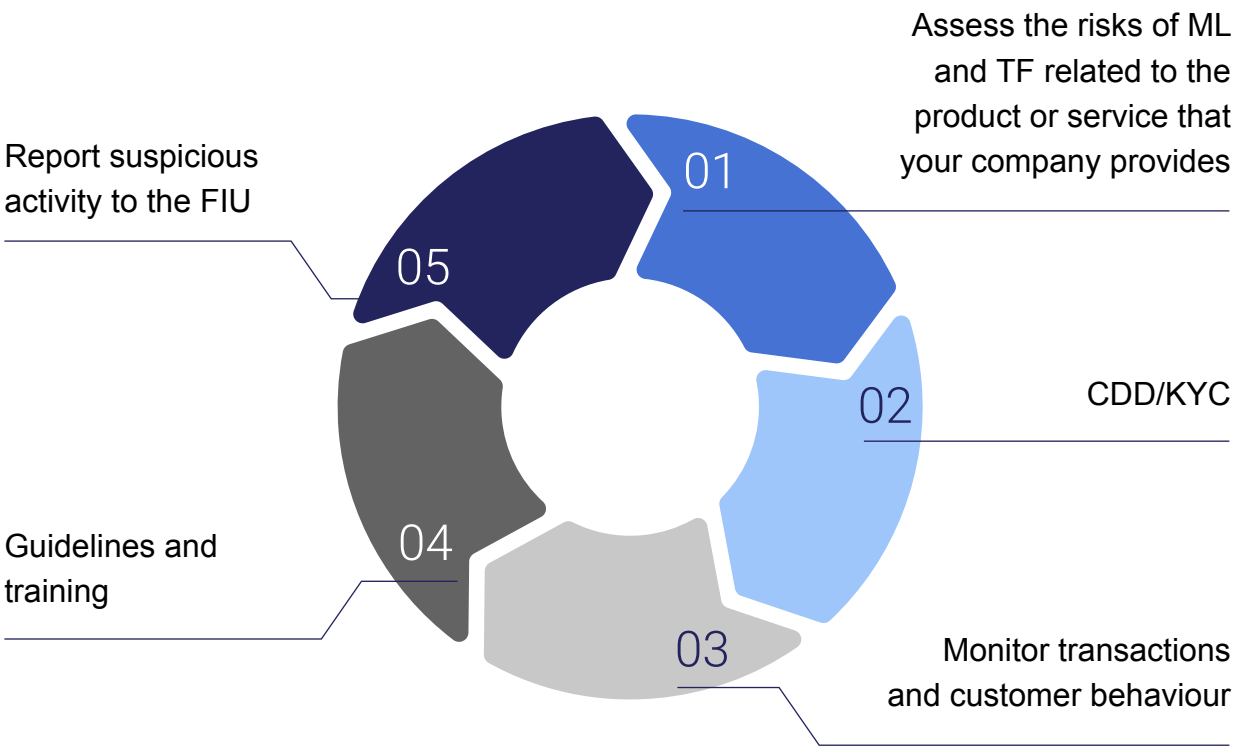
- Remember the value of Public-Private Partnership. Cooperate with authorities and also with other businesses and networks.
- Remember that by actively helping the authorities in understanding your service you will receive less questions asking for something you do not know or have.
- Remember to have adequate and correct contact details available for authorities. Make sure the authorities know them.
- Through cooperation you influence the capabilities of authorities. This means that authorities have better capabilities to detect and investigate ML and TF cases.
- Prepare for authorities a summary of the service you are providing and roughly what kind of data can be requested from your company. That information will save you from futile, time-consuming inquiries and make the authorities more efficient.

What does it mean to be an obliged entity?

AML and CFT obligations can be summarised into five points as follows:

1. Assess the risks of ML and TF related to the product or service that your company provides.
2. CDD/KYC:
   a. Identify your customer and verify the customer's identity
   a. Obtain information on the customer's activities, the nature and extent of their business, and the grounds for the use of the service or product
   a. Create a risk classification of the customer
3. Monitor transactions and customer behaviour.
4. Update and implement guidelines and training.
5. Report suspicious activity to the FIU.

All the stages mentioned above should be done following a risk-based approach.



Risk-based approach and risk assessment

A risk-based approach to AML and CFT requires every obliged entity to conduct a risk assessment, in which the purpose is to assess the risk of ML and TF connected to the products and services provided. The aim is to ensure that every obliged entity identifies and understands the risks of ML and TF related to its activities. Once the obliged entity has identified and assessed the risks, it will be able to adjust its risk management methods (KYC procedure, monitoring) in proportion to the risk. Risk-based compliance is not possible without conducting a risk assessment.

There is no standard format for a risk assessment. Each obliged entity must conduct it in a way that fits the company's specific purpose. In addition, legislation and directives can describe what should be taken into account when assessing the risks.

However, the obliged entity should document how the risk assessment was made in order to be able to describe the process to the competent authority if necessary.

The risk assessment should include, for instance, the entity's perspective on the following matters:

- How can the products or services provided by the obliged entity be utilised in ML or TF?
- How are the risks of ML and TF related to new and existing customers, countries or geographical areas, products, services and transactions as well as distribution channels and technologies taken into account (risk-based assessment)?
- What methods are used to prevent the use of the products and services in ML and/or TF (mitigation methods)?
- What vulnerabilities are related to the mitigation methods and what actions are taken to address the vulnerabilities?
- What is the assessment of the obliged entity on the level of risk remaining (residual risk) after the estimated impact of the mitigation methods on the risk?
- View of whether the level of residual risk is acceptable or whether actions will be taken to reduce it further.

The results of the risk assessment steer the actions related to CDD. Hence, the risk assessment must have an effect on the CDD actions, and these should not be conflicting. For example, customers should not be categorised based on factors that have not been identified as risk factors in the risk assessment.

Customer Due Diligence

The AMLD requires member states to ensure that obliged entities apply CDD measures in the following circumstances, which are most relevant from the perspective of PSPs:[16]

a. when *establishing a business relationship;*

b. when carrying out *an occasional transaction* that:

   (i) amounts to EUR 15 000 or more, whether that transaction is carried out in a single operation or in several operations which appear to be linked; or

   (ii) constitutes a transfer of funds, as defined in point (9) of Article 3 of PSD2, exceeding EUR 1 000 ;

c. when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;

d. when there are doubts about the veracity or adequacy of previously obtained customer identification data.

In each European Union Member State, the national law might pose additional obligations or lower threshold limits. It is essential for PSPs to define/determine which customers the CDD procedures should be applied to. If customers need to sign up for the service and create an account in order to use the service, this is usually considered to establish a business relationship.

CDD obligation includes the following stages:

- Identify your customer and verify the customer's identity.
- Obtain information on the customer's activities, the nature and extent of their business, and the grounds for the use of the service or product.
- Create a risk classification of the customer.

[16] DIRECTIVE (EU) 2015/849.

Identification and verification of the customer

Identification and verification of a customer's identity tend to get mixed up in discussions. The difference can be illustrated with a simple example:

Identification and verification of a customer in a bank

1. Identification of a customer

2. Verification of a customer's identity

Identification and verification of a customer online

1. Identification of a customer

If Bob is using, for example, an **online payment service**, he probably needs to first sign up for the service. The sign-up process first requires Bob to fill out his name, address and some other information, such as his phone number and e-mail address.

2. Verification of a customer's identity

After providing this information, Bob is directed to a service, where he needs to verify his identity by using for example strong electronic identification

Obtaining information about the customer

AML and CFT regulation does not only require identification and verification of a customer's identity but also requires obliged entities to gather information about their customers. National legislation might require PSPs to gather certain standard information, such as contact details for customers. In addition, PSPs should gather information needed to determine customer's risk and define what kind of behaviour is normal for the specific customer or group of customers.

CDD: activities, nature and extent of business, and the reason for using services.

However, the PSPs should as part of their own risk-based approach determine what specific information is important when taking into consideration the risks associated with the services and products that they offer. The collected information determines also what information can be monitored as part of the ongoing monitoring of customer relationship.

In cases where a customer is a high-risk customer, or there are other reasons to monitor his/her activity more closely, Enhanced Due Diligence (EDD) might be needed. In such cases, the customer may need to provide more information, or the transactions are monitored more actively.

Monitoring transactions and customer behavior

The third important part of the AML and CFT regulation is the monitoring of transactions and customer behaviour.

The purpose of monitoring is to detect actions that differ

- in general from what is typical for the service
- from the behaviour of a specific customer.

The PSP's own risk assessment forms the basis for their procedures, guidelines and monitoring.

Furthermore, information and risk classification of the customer determines what kind of behaviour might be assessed as suspicious.

Taking into consideration the volume of transactions conducted through PSPs, the monitoring of transactions is primarily done using automated or semi-automated monitoring systems that flag or freeze transactions for further examination by the PSP's personnel. In order for the monitoring system to be efficient, hits generated by the monitoring system should be examined relatively quickly for the purpose of follow-up actions, such as further investigations and possibly reporting suspicious activity to the FIU.

Obliged entities should remember that they also have a responsibility to further investigate whether a transaction or customer's behaviour is suspicious or cannot be reasonably explained. Of course, changes in a customer's behaviour can occur due to other, non-criminal reasons. For example, the customer may have moved to a different country, which might affect the transaction flow.

Black Wallet Reporting Guide is a product dedicated for helping Fintechs in reporting possible ML and TF to FIUs.

Please check it for more information.

Guidelines and training

Obliged entities should have guidelines and manuals available for their personnel on how to comply with AML and CFT regulations. It is important for the whole personnel to understand why certain procedures are in place and what the bigger picture behind them is. This is why all obliged entities should have at least some kind of training regarding AML and CFT issues for their personnel.

Reporting to Financial Intelligence Units

According to the AMLD, all suspicious transactions, including attempted transactions, shall be reported. A PSP's monitoring system should flag transactions or customer behaviour that are unusual. As explained above, the first step is to investigate whether there is a natural, unsuspicious explanation for the transaction or behaviour. If this is not the case, the PSP should report to the relevant FIU.

One of the cornerstones of the global AML and counter-terrorism framework is the designation of obliged entities to report suspicious transaction or activities to FIUs. The reporting framework aims to prevent and detect potential abuses of the financial system by criminals or criminal groups that seek to launder profits of illegal activities or finance terrorist activities.

Why report?

The Financial Action Task Force (FATF) recommendation:

"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 FIU."

The reports from the obliged entities are paramount in order to combat ML and TF. Timely and adequate reports from the PSPs form the basis for actions of the FIUs. In other words, without reports from the obliged entities, the possibilities of combating ML and TF are alarmingly poor. If you are wondering whether or not to report, remember that the threshold for reporting suspicious activity is low.

Quick tips

- ✓ You make the world safer.
- ✓ It's crucial for preventing ML and TF.
- ✓ You are obliged to do so by law. If you don't report, authorities can set sanctions or withdraw your licences.
- ✓ If you don't report, you might face 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 either based on criminal or civil law.

What and how to report?

Reporting to the FIU does not require that you have any evidence that ML or TF has occurred. A mere suspicion is enough. The report should be done promptly, which means that timely actions are necessary.

However, STRs or SARs should contain information about the circumstances that form the basis for suspected ML or TF.

Even though other systems exist, in many countries SARs and STRs are submitted through the IT software goAML.

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 good to provide a brief description of this in the report.
- If the report contains a lot of text, please divide it into sections.
- Contact your FIU and register as a reporting entity.
- Consider conducting automated reports.

Sources

Legislation

DIRECTIVE (EU) 2015/849. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849

DIRECTIVE (EU) 2015/2366. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366

DIRECTIVE 2009/110/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009L0110

Other

Financial Action Task Force, FATF FinTech & RegTech Initiative. https://www.fatf-gafi.org/fintech-regtech/fatfonfintechregtech/?hf=10&b=0&s=-desc

Financial Action Task Force, FATF FinTech and RegTech Forum 2017. https://www.fatf-gafi.org/publications/fatfgeneral/documents/fatf-fintech-regtech-forum-may-2017.html

Financial Action Task Force, Money Laundering Using New Payment Methods 2010. https://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf

Financial Action Task Force, Objectives for FATF – XXIX (2017–2018). Paper by the Incoming President. http://www.fatf-gafi.org/media/fatf/documents/Objectives%20for%20FATF%20XXIX%20(2017-2018).pdf

Financial Action Task Force, What is Money Laundering. https://www.fatf-gafi.org/faq/moneylaundering/

United Nations Office on Drugs and Crime, Money Laundering and Globalization. https://www.unodc.org/unodc/en/money-laundering/globalization.html

Sources

International Monetary Fund, The Bali Fintech Agenda. IMF Policy Papers. https://www.imf.org/en/Publications/Policy-Papers/Issues/2018/10/11/pp101118-bali-fintech-agenda

European Union Terrorism Situation and Trend Report 2017. https://www.europol.europa.eu/tesat/2017/

Europol, Money Laundering. https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/economic-crime/money-laundering

Black Wallet Risk Indicators 2020.

Black Wallet Risk Indicators Report 2020.

Black Wallet Reporting Guide: Recommendations for Payment Service Providers on how to report suspected Money Laundering and Terrorist Financing activities to Financial Intelligence Units 2020.


POLIISI
KESKUSRIKOSPOLIISI
Centralkriminalpolisen
National Bureau of Investigation


Polisen
Swedish Police