cssf

Commission de Surveillance
du Secteur Financier

Frequently asked questions regarding the fight against money laundering and counter terrorist financing ("AML/CTF") for individuals/ investors

Commission de Surveillance du Secteur Financier

In case of discrepancies between the French and the English text, the French text shall prevail.

Frequently asked questions regarding the fight against money laundering and counter terrorist financing ("AML/CTF") for individuals/ investors

TABLE OF CONTENTS

Question 1: What does "money laundering" mean? Modified on 15 November 2019 4

Question 2: What does money laundering "primary offence" or "predicate offence" mean? Modified on 15 November 2019 5

Question 3: What are the various stages of the money laundering process? Modified on 15 November 2019 5

Question 4: What does "terrorist financing" mean? Modified on 11 July 2016 5

Question 5: What does "international financial sanctions", in particular within the context of the fight against terrorist financing, mean? Modified on 4 March 2021 6

Question 6: Where are the documents relating to the various international financial sanctions available? Modified on 15 November 2019 6

Question 7: What are the latest developments in relation to international financial sanctions? Modified on 4 June 2021 7

Question 8: Does a consolidated list comprising all the persons and entities subject to the various international financial sanctions exist? Modified on 15 November 2019 8

Question 9: What should a financial sector professional do if a natural/legal person belonging to its business relationships is listed on the OFAC's (Office of Foreign Assets Control) sanctions lists? Modified on 4 March 2021 8

Question 10: Why is it important to fight against money laundering and terrorist financing? Published on 24 May 2012 9

Question 11: What are the main legal and regulatory texts with respect to AML/CTF applicable to the financial sector? Modified on 15 November 2019 10

Question 12: Which Luxembourg authorities are competent with respect to AML/CTF regarding professionals of the financial sector? Modified on 15 November 2019 10

Question 13: Does an international body which provides for supranational standards and monitors national AML/CTF mechanisms exist? Modified on 15 November 2019 10

Question 14: What is the CSSF's approach with respect to AML/CTF? Modified on 15 November 2019 11

Question 15: What are the powers of the CSSF in the exercise of its duties with respect to AML/CTF? Modified on 15 November 2019 12

Question 16: What are the financial sector professionals' obligations with respect to AML/CTF? Modified on 15 November 2019 12

Question 17: When do financial sector professionals have to request information from their customers for AML/CTF purposes? Modified on 15 November 2019 13
Question 18: Which documents and information shall financial sector professionals request from the customer? Modified on 15 November 2019 13
Question 19: Which information on the payer shall the financial sector professional (i.e. payment service provider) collect before transferring funds? Modified on 15 November 2019 14
Question 20: What does “PEP” mean and what are the specific risks? Modified on 15 November 2019 15
Question 21: What are the fraud mechanisms to which investors may be directly exposed? Modified on 15 November 2019 15
Question 22: Who can the investor/customer contact in the event of a prejudice? Modified on 15 November 2019 18
Useful websites: Modified on 15 November 2019 19

Commission de Surveillance du Secteur Financier

Frequently asked questions regarding the fight against money laundering and counter terrorist financing ("AML/CTF") for individuals/ investors

Question 1: What does "money laundering" mean?

Modified on 15 November 2019

Money laundering is defined as an offence which consists of knowingly facilitating, by any means whatsoever, the misleading justification of the origin of the direct or indirect income of the predicator of a crime or an offence as defined under Article 506-1 of the Penal Code. Money laundering is thus the process of making criminal funds appear to be of legitimate origin.

Moreover, the offence includes knowingly participating in an investment, dissimulation, disguise, transfer or conversion transaction of property constituting the object or the direct or indirect proceeds of a predicate offence or constituting a pecuniary benefit of any nature whatsoever from one or several of these offences.

Anyone having acquired, held or used the property constituting the object or the direct or indirect proceeds of a predicate offence or constituting a pecuniary benefit of any nature whatsoever from such predicate offence, knowing, at the time s/he received them, that they originated from one or several of the predicate offences or from the participation in one or several of these offences, shall be punishable for money laundering.

The money laundering offence is punishable by imprisonment and/or a pecuniary penalty.

The introduction of criminal money into the financial system is one of the money laundering methods used by criminals. There is, therefore, a risk that professionals of the financial sector are used for the purpose of money laundering.

In order to avoid that money launderers take advantage of the financial system to facilitate their criminal activities, Luxembourg, as well as a large number of other States, imposed certain internationally agreed professional requirements on institutions of the financial sector operating in Luxembourg. Amongst these requirements, it is worth mentioning the following: identifying the customers (including beneficial owners), performing continued monitoring (on customers and transactions), keeping appropriate records, establishing internal procedures to train staff members to recognize money laundering and to report any indications of money laundering to the competent authorities.

These professional requirements aim to allow an efficient fight against money laundering (but also against terrorist financing, cf. below) and against crime in general. They also aim to ensure the stability and reputation of the financial sector in general and in particular of the professionals of the financial sector.

Question 2: What does money laundering "primary offence" or "predicate offence" mean?

Modified on 15 November 2019

Crimes or offences which generate the funds to be laundered are commonly referred to as money laundering primary offences or predicate offences.

Primary offences include illicit trafficking of narcotic drugs, acts of terrorism or terrorist financing, corruption, weapons trafficking, criminal organisation or criminal association, certain tax offences, trafficking in human beings, sexual exploitation, including of children, kidnapping, illegal detention and hostage-taking, fraud and scam, environmental crimes and offences or counterfeiting of money.

In general, any offence punishable by a minimum term of imprisonment of at least six months is considered as a money laundering primary offence.

The money laundering offence committed in Luxembourg is punishable in Luxembourg, even if the primary offence was committed abroad.

Question 3: What are the various stages of the money laundering process?

Modified on 15 November 2019

At a first stage, i.e. the injection phase, e.g. in a banking context, the launderer introduces illegal earnings into the financial system. This introduction may be carried out by dividing large sums of cash into smaller and thus less suspicious sums, or by acquiring various monetary or financial instruments (e.g. cheques, transfer orders, securities, etc.) before depositing them in a banking account.

The second stage, i.e. the layering phase, consists of successive transfers of the deposited funds to move them away from their source. The funds may thus, for instance, be transferred by way of purchase or sale of financial instruments or transferred to a series of accounts opened with various banks throughout the world.

Finally, the last stage, i.e. the integration phase, consists of the integration by the launderer of laundered funds into legitimate economic activities, for example by acquiring real estate property, luxury goods or by creating business companies.

Question 4: What does "terrorist financing" mean?

Modified on 11 July 2016

An act of terrorism, as defined in Article 135-1 of the Penal Code, refers to any crime or offence which may, by its nature or context, seriously damage a country, an international organisation or body, and which has been committed with the intention of intimidating the population, compelling public authorities to do or abstain from doing any act or destabilising or destroying the structures of a country.

Terrorist financing is defined in Article 135-5 of the Penal Code notably as the unlawful and wilful provision of funds, assets or goods of any nature, with the intention that they should be used or in the knowledge that they are to be used in order to carry out an act of terrorism, even if they have not actually been used for that purpose.

Terrorism and terrorist financing are autonomous offences which are punishable the same way as money laundering, but which also constitute primary offences to money laundering. The same applies to certain acts linked to terrorism, such as acts of provocation, terrorist recruitment or training, which are henceforth punishable by criminal law under certain conditions.

As autonomous offences, acts of terrorism and terrorist financing are offences or crimes which are punishable by imprisonment and/or a fine.

Question 5: What does "international financial sanctions", in particular within the context of the fight against terrorist financing, mean?

Modified on 4 March 2021

International financial sanctions within the context of the fight against terrorist financing may consist of the prohibition or restriction of financial activities, the seizure of goods, freeze of funds, assets or other economic resources, as well as of the prohibition or restriction to provide certain financial services.

Persons, entities and groups falling under these prohibitions and restrictive measures are, for example, persons and entities associated with the Al-Qaida network or Taliban.

As regards professionals of the financial sector, the CSSF is the competent authority to monitor the implementation of these restrictive measures.

There are other financial prohibitions and financial restrictive measures in addition to those set out above which are taken within the context of the fight against terrorist financing. In this respect, the regulations of the European Union which are directly applicable to Luxembourg should be mentioned in the context of, for example, the situation in Belarus, North Korea, Egypt, Iran, Libya, Syria or Tunisia.

Question 6: Where are the documents relating to the various international financial sanctions available?

Modified on 15 November 2019

As the Minister of Finance is competent to deal with any questions and challenges regarding the implementation of the financial prohibitions and restrictive measures against some specific persons and entities, it is also competent to ensure the publication of the various texts relating to international financial sanctions.

The documentation is available on the website of the Ministry of Finance (https://mfin.gouvernement.lu/en.html), under the section Topics - *Sanctions financières internationales* (International financial sanctions).

The CSSF provides the publications on its website (www.cssf.lu/en), under the section "Financial crime".

On both websites, additional documentation is available i.a. in the form of good conduct guides, notification forms, lists and FAQs.

Question 7: What are the latest developments in relation to international financial sanctions?

Modified on 4 June 2021

The Law of 19 December 2020 on the implementation of restrictive measures in financial matters, which entered into force on 27 December 2020, provides new insights on this topic. Indeed, the purpose of this law is the implementation of restrictive measures in financial matters by the Grand Duchy of Luxembourg in respect of certain States, natural and legal persons, entities and groups. Restrictive measures in financial matters must be applied by:

a) natural persons of Luxembourg nationality, who reside or operate in or from the territory of the Grand Duchy of Luxembourg or abroad; and

b) legal persons having their registered office, a permanent establishment or their centre of main interests on the territory of the Grand Duchy of Luxembourg and which operate in or from the Grand Duchy of Luxembourg or abroad;

c) branches of Luxembourg legal persons established abroad and branches in the Grand Duchy of Luxembourg of foreign legal persons; and

d) all other natural and legal persons operating on the territory of the Grand Duchy of Luxembourg.

The natural and legal persons that are required to implement the restrictive measures provided for in this law shall inform the Minister responsible for Finance of the enforcement of each restrictive measure taken in respect of a State, natural or legal person, entity or group designated in accordance with the above law and the regulatory implementing texts, including attempted transactions.

The Commission de Surveillance du Secteur Financier is, in particular, responsible for the supervision of the professionals falling within its competence for the purposes of the implementation of this law. To this end, it may apply all the measures and exercise all the powers, including sanctioning powers, conferred on it, in accordance with the applicable legal provisions. Without prejudice to the application of more severe penalties provided for by other legal provisions, where applicable, infringements of this law shall be punishable by a term of imprisonment of eight days to five years and a fine of between EUR 12,500 and EUR 5,000,000 or by one of these penalties only.

For further details on the content of this law, please refer to the CSSF website under "International financial sanctions" and/or the following link: Journal officiel du Grand-Duché de Luxembourg (public.lu)

Question 8: Does a consolidated list comprising all the persons and entities subject to the various international financial sanctions exist?

Modified on 15 November 2019

There is a consolidated list of the European Union comprising all the persons, groups and entities subject to the various financial sanctions, including those relating to terrorist financing. This list is available on the CSSF website, section "Financial crime" under "International financial sanctions" – "Prohibitions and restrictive financial measures with respect to the fight against terrorist financing" – "Texts adopted by the EU" or directly through the following link:

https://eeas.europa.eu/headquarters/headquarters-homepage/8442/consolidated-list-sanctions_en

The United Nations also publishes a consolidated list which are available under the following link, also available on the abovementioned CSSF website:

https://www.un.org/securitycouncil/content/un-sc-consolidated-list

All these lists are also available for consultation on the website of the Ministry of Finance, as indicated above. No consolidated list exists with respect to the Luxembourg ministerial regulations.

Question 9: What should a financial sector professional do if a natural/legal person belonging to its business relationships is listed on the OFAC's (Office of Foreign Assets Control) sanctions lists?

Modified on 4 March 2021

It should be underlined that only Luxembourg, European and UN lists governed by the provisions of the Law of 19 December 2020 (op. cit.) are applicable to the professionals under the AML/CFT supervision of the CSSF and are subject to mandatory reporting to the Ministry of Finance, which is competent in this matter, with a copy to the CSSF.

Nevertheless, these professionals may be required (depending on their legal situation) to consult other financial restrictive measures lists, as published by foreign authorities, including the US OFAC lists.

As a consequence, the responsibility to analyse and apply the relevant measures to a business relationship listed on an OFAC list rests, where applicable, with the professional. From an AML/CFT point of view, the professional will also have to assess the impact of this situation in terms of ML/TF and whether, in such case, additional diligence measures must be applied in order to mitigate these risks. It should be emphasised that it is not the CSSF's responsibility to take a decision neither on the application of OFAC-related measures, nor on the termination of the business relationship concerned, as these decisions rest with the professional's personal assessment based on the information available to it and which emerges from its Know Your Customer (KYC)/Know Your Transaction (KYT) files.

In this context, it should however be reminded that, in case of money laundering/terrorist financing suspicion, the relevant professional must transmit a suspicious transaction report to the Financial Intelligence Unit (FIU) via the following GoAML platform: https://justice.public.lu/fr/organisation-justice/crf/goaml.html.

Question 10: Why is it important to fight against money laundering and terrorist financing?

Published on 24 May 2012

Money laundering, which consists of disguising the illegal origin of income, is inextricably linked to criminal activities. Failing to combat money laundering, the society would accept that criminal individuals benefit from activities prohibited by criminal law without incurring any sanctions.

Both money laundering and terrorist financing are likely to have severe consequences on the economy of the concerned countries as well as on the international financial stability. Indeed, such activities are likely to dissuade foreign investors and to disrupt international capital flows.

Another significant consequence of dirty money laundering is the development of a black economy, thus avoiding State taxation on large amounts of money and entailing a significant loss of income for States.

As money laundering is mostly committed through the use of the financial system of a country, this might moreover challenge the integrity and stability of the institutions and financial system which are based on legal, professional and high ethical standards. The stake does not only cause a serious harm to the reputation of all financial players, but also a decrease in the confidence of the investors in the financial sector.

Question 11: What are the main legal and regulatory texts with respect to AML/CTF applicable to the financial sector?

Modified on 15 November 2019

All the relevant applicable legal and regulatory texts are available on the CSSF website (www.cssf.lu/en/), section "Financial crime", under "Anti-money laundering and counter-terrorist financing" (https://www.cssf.lu/en/anti-money-laundering-and-countering-the-financing-of-terrorism/) and "International financial sanctions" (https://www.cssf.lu/en/international-financial-sanctions/).

On the same website, the CSSF circulars clarifying the laws and regulations on AML/CTF are included in the sub-heading "Circulars" of the heading "Anti-money laundering and counter-terrorist financing heading".

Finally other relevant documentation, as for example the Luxembourg National ML/TF Risk Assessment Report can be found in the same section.

Question 12: Which Luxembourg authorities are competent with respect to AML/CTF regarding professionals of the financial sector?

Modified on 15 November 2019

From a criminal point of view, the Luxembourg authority which is mainly competent for AML/CTF is the Financial Intelligence Unit ("FIU") of the Public Prosecutor's Office. The FIU is in charge of receiving suspicious transaction reports in respect of money laundering and/or terrorist financing from professionals, and of analysing and using them, where appropriate, in investigations or criminal proceedings.

The CSSF is, in its capacity as financial sector supervisory authority, responsible for the preventive part of the fight against money laundering and terrorist financing, i.e. compliance with the professional obligations with respect to AML/CTF by all the persons subject to its supervision/licence/registration, as well as to prevent the use of the financial sector by criminals.

As already mentioned above, the Minister of Finance is specifically responsible for international financial sanctions, in particular with respect to the fight against terrorist financing.

Question 13: Does an international body which provides for supranational standards and monitors national AML/CTF mechanisms exist?

Modified on 15 November 2019

The Financial Action Task Force ("FATF"), an intergovernmental body created in Paris by the G-7 in 1989, is such an international body.

The FATF's mission consists of planning and promoting AML/CTF standards and policies at international level. To this end, 40 recommendations on combating money laundering and the financing of terrorism and proliferation were developed by the FATF, and revised in 2012. All Member States of the FATF, including Luxembourg, must implement all these recommendations in their domestic laws.

In order to assess the compliance of the national AML/CTF regimes with the 40 recommendations as well as their overall effectiveness, the FATF regularly evaluates its Member States. The purpose of these mutual assessment processes is first to examine the measures and the actions taken at national level, then to issue recommendations to combat more efficiently money laundering and the financing of terrorism and proliferation.

In February 2010, the FATF has conducted a mutual evaluation of Luxembourg. Luxembourg was removed from the assessment process in 2014. The Luxembourg AML/CTF framework will be assessed again within the context of the fourth round of AML/CTF mutual evaluations by the FATF which started in 2013. The next evaluation of Luxembourg will take place in 2020.

In addition, Luxembourg and the CSSF, can be and have been evaluated by European bodies, including the European Banking Authority, for implementing the European AML/CTF framework, notably the AML directive 2015/849 and its implementing measures.

Question 14: What is the CSSF's approach with respect to AML/CTF?

Modified on 15 November 2019

Within the framework of its statutory mission, the CSSF is in charge of ensuring that all the persons subject to its supervision/licence or registration comply with the professional AML/CTF obligations.

The CSSF ensures that professionals implement a risk-based approach in order to allocate the appropriate means and resources to the customers and products which represent higher risks.

Moreover, the CSSF ensures that persons maintaining relationships with organised crime, including, *inter alia,* money laundering or terrorist financing offences, cannot take control, in any form whatsoever, over persons subject to its supervision.

Professionals are required to fully cooperate with the CSSF as well as the FIU with respect to AML/CTF. The CSSF, in turn, cooperates closely with the FIU. These two authorities are authorised to exchange information necessary to perform their respective duties. Moreover, the CSSF can also exchange information with other AML/CTF competent authorities, on a national or on an international level.

The AML/CTF supervision (off-site and on-site supervision) by the CSSF is organised pursuant to the principles of a risk based approach that takes into account the money laundering and terrorist financing risks to which the supervised entities and the sectors at large are exposed to.

Question 15: What are the powers of the CSSF in the exercise of its duties with respect to AML/CTF?

Modified on 15 November 2019

The CSSF has all the supervisory and investigatory powers provided for in the AML/CTF Law of 2004 and in various sectoral laws for the purpose of carrying out its duties. For instance, the CSSF is entitled to have access to any document it deems necessary and to obtain a copy thereof. It may also request information from any person subject to its supervision, notably by summoning this person or by carrying out on-site inspections.

Where a person subject to the AML/CTF supervision of the CSSF does not comply with the provisions relating to AML/CTF, the CSSF has a power of injunction against this person. If after expiry of the time limit set by the CSSF, the supervised person has not fixed the situation, the CSSF may follow up with an administrative sanction against this person.

Moreover, the CSSF has broad sanctioning powers. It may issue warnings, reprimands, administrative fines or occupational prohibitions against persons subject to its AML/CTF supervision. These sanctions will, generally, be made public by the CSSF.

Such administrative or prudential sanctions are without prejudice to the imposition of criminal sanctions (imprisonment and/or a fine) by criminal courts against professionals which deliberately violated the legal provisions which apply to them in this regard.

Question 16: What are the financial sector professionals' obligations with respect to AML/CTF?

Modified on 15 November 2019

Financial sector professionals shall, in any event, comply with the professional obligations arising from AML/CTF texts, and more specifically customer due diligence obligations, adequate internal management requirements and cooperation requirements with the authorities.

Furthermore, and where applicable, they must comply with the obligations arising from Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, applicable as from 26 June 2017. In particular, financial sector professionals must respond, without delay, to any request for information from the competent AML/CTF authorities and relating to information accompanying transfers of funds.

Question 17: When do financial sector professionals have to request information from their customers for AML/CTF purposes?

Modified on 15 November 2019

Financial sector professionals are required to apply customer due diligence measures (i) when establishing a business relationship; (ii) a) when carrying out occasional transactions amounting to EUR 15,000 or more; b) when carrying out an occasional transaction that constitutes a transfer of funds as defined in Regulation (EU) 2015/847; (iii) when there are suspicions of money laundering or terrorist financing and (iv) when there are doubts about the veracity of the information provided.

These customer due diligence measures shall also be carried out during the course of the business relationship if circumstances so require.

Question 18: Which documents and information shall financial sector professionals request from the customer?

Modified on 15 November 2019

Financial sector professionals shall identify the customer, the beneficial owner and the representative, where appropriate, as well as verify their identity, on the basis of documents, data or information from a reliable and independent source.

In addition, financial sector professionals shall obtain information on the purpose and intended nature of the business relationship which includes information on the origin of funds. Throughout the business relationship, they shall carry out an ongoing due diligence of this business relationship, including by examining the transactions concluded and/or the origin of the funds. They shall update the documents, data and information obtained.

The extent of the due diligence may be adapted according to the relevant customer's risk profile, business relationship, product or transaction and delivery channel used. Thus, it is the responsibility of each financial sector professional to determine the information and documents s/he deems necessary to comply with his/her legal obligations.

Due diligence shall be applied to both new customers and existing customers. Financial sector professionals may thus request additional documents from existing customers during the business relationship.

Question 19: Which information on the payer shall the financial sector professional (i.e. payment service provider) collect before transferring funds?

Modified on 15 November 2019

Pursuant to aforementioned Regulation 2015/847 (EU), transfers of funds shall be accompanied by complete information on the payer (i.e. generally the payer's name, account number and address) and on the payee (i.e. generally the name of the payee and the payee's payment account number). The address may, however, be substituted with the payer's date and place of birth, a customer identification number or national identity number. Where the payer or the payee does not have an account number, the financial sector professional may substitute it by a unique transaction identifier.

Different requirements are applicable depending on the role of each payment service provider, i.e. whether the professional is an intermediary payment service provider, intervenes for the account of the payer or of the payee.

By way of a derogation from the complete information requirement, the account number or a unique transaction identifier may be sufficient where the payment service providers of the payer and of the payee are both situated within the European Union.

Concerning transfers of funds within the European Union, the obligation to make information available upon request depends also on whether the amount of the transfer, executed in a single or in several transactions, exceeds EUR 1,000.

Finally, where the information on the payer is missing or incomplete, the payment service provider of the payee shall take appropriate measures as for example rejecting the transfer or requesting complete information[1].

[1] *As further explained by the European Supervisory Authorities' Joint Guidelines on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, as adopted by Circular CSSF 18/680.*

Question 20: What does “PEP” mean and what are the specific risks?

Modified on 15 November 2019

PEPs are defined as politically exposed persons, i.e. natural persons who occupy or hold prominent public functions, and refers also to family members or persons closely associated with them. These include national and international PEPs.

PEPs must, in principle, be subject to enhanced due diligence, notably because they may be targets for acts of corruption, i.e. an infringement consisting of the behaviour by which offers, promises, donations, gifts or benefits are requested, received, proposed or given for the purpose of performing or refraining from performing an act, obtaining particular favours or benefits or exercising undue influence to get jobs, contracts or other favourable decisions.

Corruption is considered passive where it is instigated by the corrupted party and active where it is the result of the corrupting party.

The corruption offence includes not only (i) the corruption of persons holding public authority or public officials or law enforcement officials or agents entrusted with an elective public mandate or with a public service mission, including from another State, EU officials and in general the staff of the institutions of the European Union and international organisations, and also magistrates, i.e. PEPs, but also (ii) the corruption of individuals who manage or work for a private sector entity. Corruption is punishable by deprivation of liberty and a pecuniary fine.

The predicate offence which may give rise to a money laundering offence is limited, in principle, to the public or private passive corruption of the individuals referred to above, including PEPs, given that it is the concealment by the corrupted party of the source of the corruption’s proceeds that constitutes money laundering.

While higher risks may be present in the relationship, it shall not be concluded that all PEPs are criminals.

Question 21: What are the fraud mechanisms to which investors may be directly exposed?

Modified on 15 November 2019

Examples:

(a) Nigerian connection

This mechanism was initially developed by persons who claimed to live in Nigeria, thus giving rise to the name assigned to it. However, the use of this mechanism spread and may be initiated from any country nowadays.

The principle is to contact persons or companies, notably in Luxembourg, in order to request their assistance to take out money (blocked due to national restrictions in relation to the currency of the home country) by drawing up false bills and cashing the amount of these bills on a Luxembourg bank account. In return, an important commission on the sums taken out of the home country is promised.

However, the real purpose of this operation is to ask the persons to agree to advance certain fees.

Needless to say, those who pay the requested fees never hear from their distant correspondents again.

(b) Boiler-Room

The boiler room is a fraudulent mechanism, the purpose of which is to sell overpriced securities to investors. The most common form consists for persons or entities to purchase low-value securities on a market lacking transparency, and then to artificially raise the value and to resell these securities at very high prices to investors.

Originators of the boiler room often send brochures containing a set of information, which seems to be accurate, and well-written financial analyses on known securities.

The veracity of the advice given is underlined by indications such as “If you have followed our advice included in brochure XY, you have realised a gain of 20% within less than two months”, i.e. in most cases unverifiable information.

The brochure will also include an indication as to a very positive development for a less known or unknown company. The boiler room then contacts the investor by telephone to offer him/her to acquire the securities of this company, with a special emphasis on the above-mentioned passage of the brochure.

(c) Recovery Room

In the event of a recovery room which often follows a boiler room, the investor who purchased securities which became valueless or which never had any value is offered by another person or entity to repurchase his/her securities at a higher price than their current value or their acquisition value.

In return, the investor must advance certain fees or invest in another transferable security.

Once the fees or investment have been paid, the investor never hears from the entity or the person who contacted him again.

(d) Pyramidal mechanisms

This mechanism consists of the payment of an amount of money to an entity, with the hope of recovering a multiple of this amount if a certain number of other persons are hired and persuaded to pay the same amount of money to the pyramidal organisation. These mechanisms always constitute scams.

(e) IT frauds

The IT frauds consist of any kind of criminal offences which might be committed on or by means of an IT system which is usually connected to a network. These treats which are likely to target investors directly, have almost always a greedy nature, i.e. are aimed to obtain financial, material or any other gain.

The most frequent threats are attacks via email such as “phishing”. In respect of “phishing”, fraudsters send an email in the name of a bank to a person under whatever pretext (for instance a technical breakdown, an internal investigation, etc.) in order to attract the investor to a website similar to the real website of the bank, but which is fake. Once connected to the fake website, the investor is prompted to enter his/her web-banking code, password or credit card details.

Another frequent threat is the “pharming” which consists of diverting the access of a website (usually by means of a Trojan horse, a worm or a virus) to a fake website on which the investor is prompted to enter personal data such as his/her web-banking code, password or credit card details.

With the data collected, fraudsters can easily plunder the accounts of the relevant investor.

(f) CEO fraud

According to the typologies report of the FIU of April 2019, the so-called CEO fraud consists of the following:

The fraudster contacts the accounting department of a company (either by email or by phone), pretending to be the CEO or a board member of the company. While insisting on the confidentiality of the conversation, the fraudster provides details on an important contract which is about to be concluded urgently.

The author of the fraud has generally an in-depth knowledge of the company’s structure and uses a significant number of forged documents that had been prepared in advance, to make the transaction appear real and serious.

The fraudster manages, with the supporting documents provided, to persuade the accountant to execute a cash transfer to an account abroad.

In most cases, the fraudsters do not act alone, but belong to an organised group: one person will take on the role of the group's CEO, another person will claim to be the lawyer or the notary in charge of the transaction. In certain cases, the fraudsters did not hesitate to claim to be State or international authorities, notably with the purpose of persuading the financial institutions to keep up their business relationship with the client in order to continue receiving the proceeds of other ongoing or past frauds.

The employee who did not notice the fraud might even be requested to carry out additional transactions. In most cases, the accountant noticed the fraud only several days after the transfer of funds.

The analyses of the FIU evidenced that the frauded funds are often transferred to a first account held with a European bank, then split up into one or several other accounts in third countries. This splitting-up of the funds into several transfers allows fraudsters to maximise their chances to protect at least part of the frauded funds.

For further details and other types of fraudulent behavior, you may consult the abovementioned report under the link:

https://justice.public.lu/dam-assets/fr/legislation/circulaires/CRF-note-faux-virements.pdf.(in French)

Question 22: Who can the investor/customer contact in the event of a prejudice?

Modified on 15 November 2019

If an investor/customer suffers a prejudice, in particular through one of the fraud mechanisms described under question 19 above or in relation to a money laundering offence (excluding terrorist financing offences, for which only the Luxembourg district authorities are competent), the investor/customer may lodge a complaint in the hands of the State Prosecutor with the *Tribunal d'arrondissement* (District Court) of Luxembourg, at the following address:

Parquet de Luxembourg

Bâtiment PL

Cité judiciaire

L-2080 Luxembourg

or in the hands of the State Prosecutor with the *Tribunal d'arrondissement* (District Court) of Diekirch, at the following address:

Palais de Justice op der Kluuster

Place Guillaume

B.P. 164

L-9202 Diekirch

The investor may also lodge a complaint directly in the hands of the investigating judge (*juge d'instruction*) with the *Tribunal d'arrondissement* (District Court) of Luxembourg or Diekirch. The complaint in the hands of the investigating judge implies a civil action. Such a complaint may be lodged at the following address:

Cabinet d'instruction de Luxembourg
Cité judiciaire, Bâtiment TL
L-2080 Luxembourg

or

Cabinet d'instruction de Diekirch
Tribunal d'arrondissement de Diekirch
Place Guillaume
B.P. 164
L-9237 Diekirch

The investor may also address his/her complaint to any police station or even to the General Police Directorate. Contact details of the various police services are available on the police's website (www.police.public.lu).

Further information on the filing of a complaint are available on the website www.justice.public.lu under "Affaires pénales – Dépôt de plainte".

Useful websites:

Modified on 15 November 2019

www.fatf-gafi.org/, bottom section of the Homepage presents several Frequently Asked Questions

https://justice.public.lu/fr/organisation-justice/crf.html

www.minfin.gouvernement.lu/en, under "Topics" - "Sanctions financières internationales"

www.mae.lu/en, under « Procedures » - « Restrictive measures » - International financial sanctions

Commission de Surveillance du Secteur Financier
283, route d'Arlon
L-2991 Luxembourg (+352) 26 25 1-1
direction@cssf.lu
www.cssf.lu/en/