cssf

Commission de Surveillance
du Secteur Financier

Agents / e-money distributors - Guidance for the prevention of money laundering and terrorism financing

Commission de Surveillance du Secteur Financier

Agents / e-money distributors - Guidance for the prevention of money laundering and terrorism financing

CONTENTS

Commission de Surveillance du Secteur Financier

Agents / e-money distributors - Guidance for the prevention of money laundering and terrorism financing

1 Purpose and scope of the guidance

The Luxembourg National Risk Assessments (hereafter the "NRA") which were published respectively on 20 December 2018 and on 15 December 2020[1] include an assessment of money laundering and terrorist financing (hereafter "ML/TF") risks of the Luxembourg money services business sector (hereafter "MVTS") which includes payment institutions (hereafter "PIs") and e-money institutions (hereafter "EMIs") established and licensed in Luxembourg as well as agents and e-money distributors located in Luxembourg and acting on behalf of PIs and/or EMIs established and licensed in other European Member States (hereafter "Member States"). The NRA concluded that residual risk exposures to ML/TF risks of the Luxembourg MVTS sector, which includes PIs, EMIs, agents and e-money distributors acting on behalf of PIs and EMIs established in other Member States is medium:

Table 1: Overview of Luxembourg's NRA dated 2020 – risks in the MVTS sector

Sector	Sub-sectors	Inherent risk	Residual risk
MVTS in Luxembourg	Payment Institutions	High	Medium
	E-money institutions		
	Agents and e-money distributors acting on behalf of PIs and EMIs established in other Member States		

National Risk Assesment of money laundering and terrorist financing

The Commission de Surveillance du Secteur Financier (hereafter "CSSF") performed a deeper analysis to better understand and assess the specificities of the agents and e-money distributors operating in Luxembourg and the ML/TF risks to which they are exposed. As the agents and e-money distributors are usually not overly familiar with the rules and regulations of the financial sector related to the prevention of money laundering and terrorist financing (hereafter "AML/CTF"), the CSSF decided to issue a guidance in order to raise the awareness of these actors as regards the ML/TF risks to which they are exposed and as to how these actors should act in respect of mitigation of ML/TF risks.

This guidance aims particularly to promote the understanding of ML/TF risks as well as the professional obligations with regards to AML/CTF. It aims to provide useful information on ML/TF risks to which agents and e-money distributors established in Luxembourg can be exposed as well as practical information on actions that can be taken to mitigate these ML/TF risks.

This guidance is also a useful document for PIs and EMIs established in Luxembourg and supervised by the CSSF for use in their oversight of the agents and e-money distributors they are using in other Member States.

2 AML/CTF regulatory framework applicable to agents and e-money distributors acting on behalf of PIs and EMIs established in other Member States

The EU Payment Service Directives which were transposed in Luxembourg through the Payment Service Law dated 10 November 2009, as amended, foresee the possibility for European PIs and EMIs to use agents and/or e-money distributors to offer their payment or e-money services in any other Member States.

Recitals 52 and 53 of the EU Directive 2015/849 on the prevention of the use of the financial system for the purposes of ML/TF (hereafter the "AMLD") lays down that, where a European PI or EMI is using an agent and/or an e-money distributor established in another Member State (the "Host Member State"), it must comply with the AML/CTF requirements of the Host Member State for all the payment/e-money services that are carried out through that agent and/or e-money distributor in the Host Member State. The National Competent Authority of the Host Member State supervises that all entities established and operating on its territory including agents and e-money distributors acting on behalf of PIs and EMIs established and licensed in other Member States comply with the local AML/CTF rules and requirements of the Host Member State.

The AMLD does not prescribe how European PIs and EMIs using agents and/or e-money distributors in other Member States must meet their AML/CTF obligations. The rules applicable to them are laid down in the national law transposing the AMLD of the Host Member States where agents/e-money distributors are established and are operating.

In Luxembourg, according to Article 2 (1) 1 of the law of 12 November 2004 on the fight against money laundering and terrorist financing (the "AML/CTF Law"), agents/e-money distributors established in Luxembourg and acting on behalf of PIs and EMIs established and licensed in other Member States fall under the scope of the AML/CTF Law. However, it has to be noted that these PIs and EMIs remain fully responsible for the acts performed by the agents and e-money distributors they are using.

The AML/CTF Law also indicates that the CSSF is the competent authority responsible for supervising that the agents and e-money distributors fulfil their AML/CTF obligations.

3 Overview of the agents and e-money distributors in Luxembourg

At the end of 2020, 22 agents and 3 e-money distributors acting respectively on behalf of 9 PIs and 3 EMIs established and licensed in another Member State were operating in Luxembourg. End of 2021, 21 agents and 1 e-money distributor on behalf of 7 PIs and 1 EMI established and licensed in another Member State were operating in Luxembourg. The number remains quite stable for 2021 when compared to 2020. The number of agents/e-money distributors and the Member State where their related PI/EMI is located is shown below:

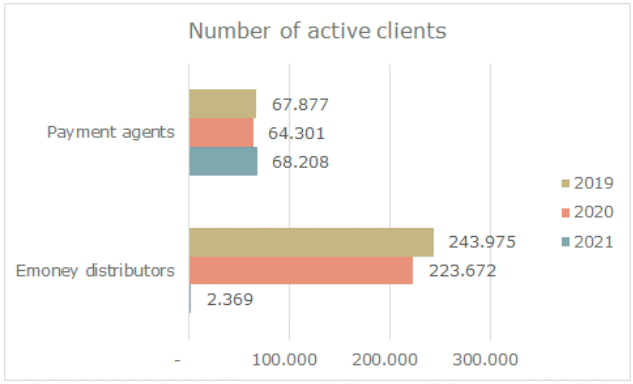
Agents/e-money distributors operating in Luxembourg

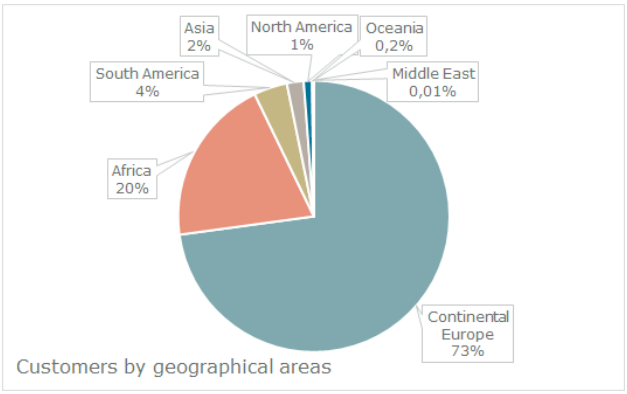
PIs/EMIs established and licensed in Member States and on behalf of which agents/e-money distributors are acting

As it can be seen, the number of agents and e-money distributors operating in Luxembourg is very limited. To put this into perspective, 109,122 agents and e-money distributors were operating within Europe in March 2022

The business model of agents and e-money distributors in Luxembourg varies from small corner shops (internet and phone stores, tobacco shops, mini market and conveniences stores…) (79%) to entities whose main activity is linked to payment services or e-money services (21%). In most instances, the entities are of a small size with on average less than 5 employees.

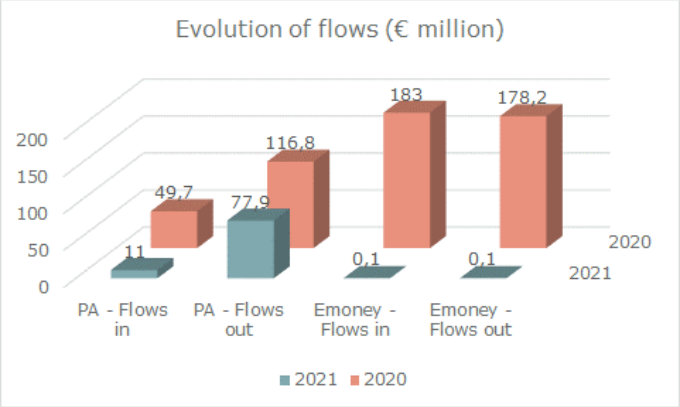
All agents are offering transfers of funds (remittance services) across customers and geographies. Agents are mainly meeting their customers on a face-to-face basis. Indeed, customers of agents are coming to their offices and mostly performing cash-based transactions (as indicated below). The customers of agents, and consistent with their business model, are natural persons and the majority of customers (73%) are coming from Continental Europe. 70% of the customers are coming from EU Member States. The vast majority of the other customers are coming from Africa (20%).





Generally speaking, e-money distributors are distributing prepaid cards and vouchers that can be used electronically to purchase goods or services on merchant websites. Given the inherent nature of their business, the e-money distributors are entering into relationships with their customers online. The sole e-money distributor operating in 2021 was distributing the e-money product (linked to a fidelity card or gift cards) which can be used in a close-loop environment (in this case a well-known European clothes shop retailer). It was servicing only natural persons which are all resident in Luxembourg. It has to be noted that the e-money distributor is no longer active since beginning of 2022. The ML/TF risk exposure is therefore very restricted.

In 2021, agents and e-money distributors have processed a total of 318,184 transactions (in and out) (315,778 by agents and 2,406 by the e-money distributor) for a total value of 89.1 million euro (88.8 million euro by agents and 0.2 million euro by the e-money distributor). It is worth noting that the consolidated value of transactions processed represents 0.03% of the volume of consolidated value of the transactions processed by PIs and EMIs which are established and licenced in Luxembourg and supervised by the CSSF for the same period and 0.01% of the total volume of payments processed in Luxembourg1. The consolidated value of transactions processed by the agents and e-money distributors can therefore be considered as low.



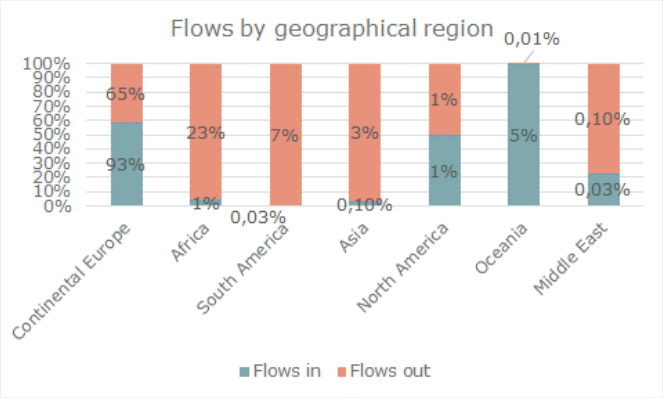
The consolidated volume of activities of agents has decreased by 47% in 2021. The decrease is mainly explained by the decrease of the amount of individual transactions processed by 55% (from 621 euro to 281 euro estimated on an average basis). The volume of activities of e-money distributors has significantly decreased from 361.2 million euro on a consolidated basis to 0.2 million euro which can be linked to the decrease of the number of active e-money distributors and the decrease in the number of customers (decreased by 99%).

End of 2021, around 88% of the transactions processed by agents were cash-based representing 85% of the total consolidated volume in euro. As regards the e-money distributor2, the main funding payment method was payment cards (94%). The remaining 6% is cash-based (gift cards).

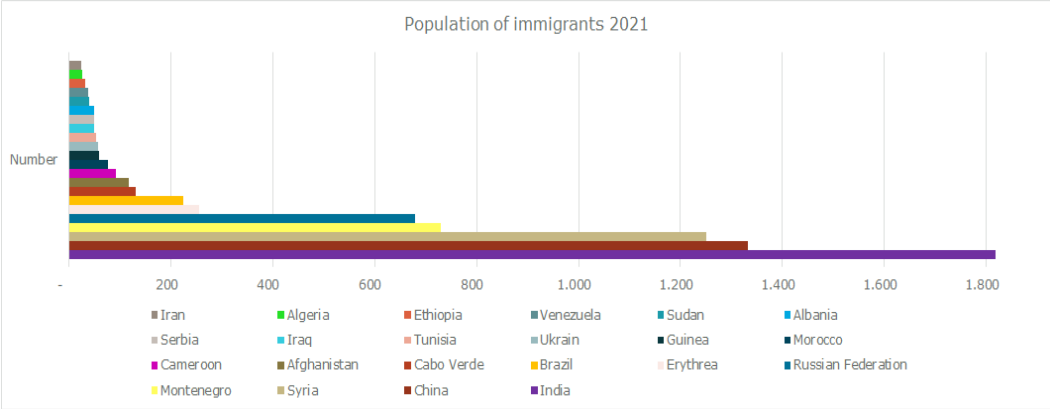
[1] *BCL payment statistics 2021*

[2] *It has to be noted that the e-money distributor is no longer active since beginning of 2022*

In 2021, the activity of agents and e-money distributor has a global reach which is common for the sector. 93% of the consolidated flows are coming from Continental Europe (88% of which coming from Member States) and 65% are transferred to Continental Europe (61% of which transferred to Member States). The vast majority of the remaining consolidated flows are linked to Oceania (5%), South America (7%) and Africa (24%).



Against the background of this data, one should keep in mind that the population in Luxembourg[1] is international and that Luxembourg is a European country welcoming immigrants requesting international protection[2] (with approximately 9,800 persons having received international protection or a residence permit).



[1] *Statistics Portal Grand Duchy of Luxembourg January 2021*
[2] *Ministry of Foreign Affairs – Review of the 2019 year in terms of asylum and immigration*

4 ML/TF risks

As regards agents, they are commonly used for fast transfers of money across customers and geographies, some customers being located in countries with less mature financial systems. As highlighted in the NRA, customers are often using agents to repatriate funds to their country of origin to support their community or families. Some customers might also be frail and vulnerable persons and their personal affairs can be easily exploited by criminals who coerce them to act as "front men". Such customers are often facing difficulties to enter the traditional financial sector and are using agents instead in order to process their transactions.

It is worth highlighting that globally, agents are particularly vulnerable to TF risks. Among the customers, one can notably find migrants coming from countries where terrorist activities might be more significant and who are remitting funds home. It might be difficult for agents to detect transactions from/to normal families not linked to terrorist groups from transactions processed on behalf of terrorist groups.

In Luxembourg, as highlighted in section 3 above, the major part of the outflows (65%) are processed within Continental Europe and the major part of the customer base resides in Member States (70%). The number of transactions sent to countries where terrorist groups are more inclined to be active is also marginal and represent 0.8% of the total number of transactions processed.

It is also worth noting that payments through agents are particularly attractive as cash transactions can be easily made, transfers are quickly processed and the transaction fees are usually lower. Intrinsic to the business model, many transactions are one-off/occasional, preventing the agents from establishing a durable relationship with their customers. Hence, there is often no possibility to assess the customer's behaviour and monitor its transactions. In Luxembourg, and as detailed in section 3 above, 85% of the transactions processed are cash-based in terms of volume in euro.

Customers can also use forged documents which are nowadays more and more difficult to detect due to the increasing quality of such documents. Given their business model (small shops), agents are less familiar with these documents and hence more likely to not identify when such documents are forged. E-money distributors can also face the same issues keeping in mind that the relationship with the customers is internet based (non-face-to-face relationship). While this risk (use of forged documents) can be materialised it is however not specific to agents and e-money distributors as all types of financial institutions are facing this issue.

Commission de Surveillance du Secteur Financier

Globally, e-money distributors are mainly distributing prepaid cards and vouchers that can be used to buy goods and services from a wide range of merchants. These prepaid cards and vouchers might offer a degree of anonymity when they are used as the buyer of the goods and services is not identified by the merchants. In addition, customers can buy the prepaid cards and vouchers which in turn can be used by another person to whom the customers have given the prepaid card or voucher as gift. Generally, for such prepaid card or voucher, the customers receive a PIN code that can be used on the internet for example for payment of goods and services such as gambling services or online games. Additionally, certain types of prepaid cards can be used by multiple customers which renders it even more difficult to obtain identification information from the parties involved.

E-money products can also be bought using cash which provides anonymity to some extent. In cases where the products can be loaded/reloaded, the sources of funding might also be obscure as the methods of payment are multiple ranging from cash to electronic means. The e-money distributor in Luxembourg is however less exposed to the ML/TF risks linked to cash-based transactions as there are very limited transactions in cash.

Appendix A of this report provides "red flag" indicators that agents and e-money distributors can use in particular for detecting suspicious behaviours and transactions.

5 Professional AML/CTF obligations

The aim of this section is not only to remind and emphasize the AML/CTF obligations as laid down in the legal and regulatory texts applicable in Luxembourg (notably the AML/CTF Law, the Grand-ducal regulation dated 1 February 2010 providing details on certain provisions of the AML/CTF Law, (hereafter the "Grand-ducal Regulation") and the CSSF Regulation N°12-02 dated 14 December 2012 on the fight against ML/TF (hereafter the "CSSF Regulation")) but also to share some practical recommendations on how to best comply with these obligations considering the particularities of agents and e-money distributors business and their operating models.

Agents and e-money distributors established and operating in Luxembourg are subject to the AML/CTF Law in accordance with Article 2 (1). As such, they shall comply with the requirements laid down in the legal and regulatory texts applicable in Luxembourg without prejudice of a stricter regime applied by the PI and EMI on behalf of which they are acting.

All relevant applicable Luxembourg legal and regulatory texts are available on the CSSF website – Regulatory framework – Themes: Financial crime.

5.1 Obligation to perform an AML/CTF risk assessment

Article 2-2 (1) of the AML/CTF Law and Article 4 of the CSSF Regulation require that professionals shall understand the ML/TF risks to which they are exposed through their business activities. In this respect, they shall identify and assess the ML/TF risks by considering risk factors related to their customers, countries or geographic areas, products, services, transactions or delivery channels.

Why

The risk assessment is the corner stone to determine the risk appetite, meaning the level of risk professionals are ready to assume, as well as to determine the due diligence measures and controls that must be applied to their business relationships in order to mitigate the identified ML/TF risks.

Practical recommendations

Agents and e-money distributors must clearly understand the ML/TF risks they can be and are exposed to through the provision of their payment or e-money services and in particular in situations representing a higher risk. The better they understand the ML/TF risks they are exposed to, the better they can apprehend what measures, including controls, they shall perform to mitigate these risks.

When assessing the risks, and in case of doubts or questions, agents and e-money distributors shall refer to the PIs/EMIs on whose behalf they are acting in order to obtain further guidance.

5.2 AML/CTF policies and procedures

Under Article 4 (1) of the AML/CTF Law, Article 7 (1) of the Grand-ducal Regulation and Article 38 of the CSSF Regulation, professionals are required to put in place and document policies, controls and procedures to mitigate and manage effectively the ML/TF risks to which they are exposed. The policies and procedures shall be proportionate for example to the specificities and size of the professionals and be reviewed and updated where necessary, on a regular basis and in particular in case of amendments to the AML/CTF legal framework. Policies and procedures can be based on the PIs and EMIs established in other Member States on whose behalf they are acting but must comply with the AML/CTF rules and regulations applicable in Luxembourg.

Why

AML/CTF policies and procedures are essential for the staff to understand the AML/CTF processes as well as the tasks and controls to be performed.

Practical recommendations

Agents and e-money distributors shall have procedures/policies and controls in place which shall cover for example the customer due diligence, record-keeping, the detection of unusual or suspicious transactions/activities and the obligation to report ML/TF suspicious transactions/activities[1] to the authorities without delay.

In practice, agents and e-money distributors should have clear and documented working instructions for their staff in order for them to understand the specific checks they shall perform as well as guidance and practical information in order to be able to correctly use the different systems/tools.

The working instructions for the staff shall specify at least the following (non-exhaustive list):

The minimum identification information and documents to be requested/gathered for individual or corporate customers,

The additional information to be collected and checks to be performed when facing a situation of higher risk,

The information to be gathered when executing a transfer of funds and in particular the necessary information about the ordering party (which is the customer) and the beneficiary of the transactions,

How employees shall react in case they detect that the customer has a potentially suspicious behaviour, to whom employees shall escalate these potentially suspicious customers' activities/behaviours.

5.3 Entering into business relationship or not

Professionals decide for themselves whether to enter into a business relationship or not, or whether they would need to refrain from processing a transaction. However, where a professional suspects that a relationship or a transaction relates to ML/TF, it shall not proceed unless this would create suspicions with the customer, and report without delay the case to the FIU, as required by Article 3 (4) 6th indent of the AML/CTF Law.

[1] *For the purpose of this document, the references to suspicions of ML/TF always include associated predicate offences, as notably foreseen in Article 5 (1) of the AML/CTF Law.*

Why Customer acceptance is the beginning of the business relationship between a professional and its customers. It is also the first step in exposing the professional to ML/TF risks and to damage its reputation in case bad events occur.
Practical recommendations Agents and e-money distributors shall refrain from accepting any relationship with a customer or carrying out any transaction where the customer has not been properly identified or has a suspicious behaviour or is providing inconsistent information and where therefore agents/e-money distributors suspect they are facing a ML/TF case. In case of doubt, they should not hesitate to contact the PIs or EMIs on whose behalf they are acting in order to seek further guidance and advice. To this end and in accordance with Articles 11 (2) and 25 of the CSSF Regulation, agents and e-money distributors are expected to document the difficulties they encounter during the identification and verification process. They should also document the reasons why they decided to refuse to enter into a relationship with a customer or to execute a transaction. Where necessary, they should without delay report the suspicious activity or transaction to the FIU.

5.4 Know Your Customers / Customers due diligence checks

Article 3 (2) of the AML/CTF Law provides the obligation to perform customer due diligence including the identification and verification of the customers (including the beneficial owner and proxyholder, where applicable) when entering into a business relationship, when carrying out an occasional transaction, when there is a suspicion of ML/TF and when there are doubts about the veracity or adequacy of previously obtained customer identification data as well as the obligation to assess and understand the purpose and the intended nature of the relationship by obtaining information on the purpose and nature of the business relationship and finally the obligation to monitor on an ongoing basis the business relationship with the customers. According to Article 3 (5) of the AML/CTF Law the extent of these customer due diligences can be adapted on a risk-sensitive basis. In this context please also refer to Article 1 (4) of the Grand-ducal Regulation.

Chapter 4 of the CSSF Regulation provides practical information on the data and documents to be requested and the controls to be performed on a risk-sensitive basis (as for example the application of Enhanced Due Diligence measures in case of high-risk customer).

In a nutshell and as indicated in Articles 16 (1) and 18 (1) of the CSSF Regulation, professionals must identify the customer and verify his identity based on official identification documents. Similar requirements can be found in Articles 16 (2) and 19 (1) of the CSSF Regulation for legal persons.

The professionals shall also ensure that the customers, the persons on whose behalf they are acting, proxyholders, the beneficial owners (in the case of legal persons) which have been identified and verified at the beginning of the relationship are not known criminals or sanctioned persons and that the appropriate name screening checks with respect to international financial sanctions as applicable in Luxembourg, are performed.

Where a customer is acting on behalf of another person, professionals must also identify and verify that other person. In the case of legal persons, the person who is representing the customer, has also to be identified and verified. The professionals shall not only obtain the information on the customer and the proxyholder itself but also on the beneficial owner.

Knowing the customers also means understanding why they want to use the services of the professionals or to carry out a transaction (purpose and intended nature of the relationship or of a transaction). It also includes the necessity to establish the origin of the funds involved in the relationship and/or in the transaction (so called source of funds e.g. the origin of the funds involved). Further details can be found in Article 24 of the CSSF Regulation.

Article 3-1 of the AML/CTF Law refers to Simplified Customer Due Diligence and Article 3-2 of the AML/CTF Law treats the Enhanced Customer Due Diligence. The said law provides the information which the professionals shall gather and the steps they shall follow where they are facing a situation with either a lower or a higher risk.

Why

Customer due diligence checks are crucial for managing the ML/TF risks previously identified as it is the first step in ensuring that the customer is not a criminal, is not acting on behalf of a criminal (as explained in section 4, customers which are vulnerable persons might be used as "front men"), and is not trying to launder "dirty" money or to finance criminal activities including terrorist activities. This is also the basis for determining to which risk category the customer belongs and to ensure an appropriate monitoring of the customer's activities.

Practical recommendations

Agents and e-money distributors shall obtain all necessary and pertinent information to understand who the customer is and why he/she is coming to their offices/shops.

For individual customers and as indicated in Article 16 (1) of the CSSF Regulation, they must collect at a minimum the following data: the first and last name of the customer, his/her date and place of birth, his/her nationality(ies), his/her full postal address (main residence) and where appropriate, the official national identification number. To verify the information of natural persons, they shall obtain one valid authentic official identification document issued by a public authority and which bears the customer's signature and picture such as the customer's passport, his ID, his residence permit, his driving licence or any other similar document (Article 18 (1) of the CSSF Regulation).

For legal persons, they shall collect at least the following data (Article 16 (2) of the CSSF Regulation): denomination of the company and its legal form (e.g. S.A., S.à r.l.) postal address of the registered office, the names of the directors, the confirmation that the person representing the customer can engage the company and has the authorization from the company to enter into the relationship. The beneficial owner of the company must also be identified and verified.

For the verification of legal persons, agents and e-money distributors shall at least obtain the last coordinated or up-to-date articles of incorporation and a recent and up-to-date extract from the companies register.

In addition to the data listed above, the questionnaire/document shall include a question in order to validate whether the customer is acting on his own account, to document the purpose and intended nature of the relationship as well as the source of funds (for example the revenues).

Agents and e-money distributors shall not hesitate to question and challenge the customer until they are satisfied that the customer is who he/she says he/she is, they have sufficient assurance that the source of funds does not constitute the proceeds from crimes and they know the beneficiary of the transactions they will process.

5.5 Customer risk categorisation

For the purpose of Article 3 (2a) of the AML/CTF Law and in accordance with Article 5 (1) of the CSSF Regulation, professionals shall categorize their customers by considering the different ML/TF risk levels. In a nutshell, all customers shall receive an individual risk rating and such risk level determines the level of due diligence requirements to be applied to the customer.

In practice, it is often seen that professionals rate customers into 3 categories: low risk, medium risk and high risk. In accordance with Article 5 (1) of the CSSF Regulation, the risk level shall be assessed according to a combination of risk factors which should include among others but not limited to, risk factors linked to the type of customers (individuals or legal persons including proxyholders, beneficial owner), the countries and geographic areas, the products, services and transactions provided to the customer, or the delivery channel (for example face-to-face business relationship or not).

One important preliminary step is to screen its name against all the official sanctions' lists like the European and Luxembourg financial sanctions (i.a. the ministerial regulations) which are published i.a. on the CSSF website as it will determine whether the relationship can be accepted, if a reporting shall be made to a competent authority and it will be a factor that will be used in determining the risk profile of the customer. Another important check is whether the customer, its proxy or beneficial owner is a Politically Exposed Person ("PEP"), that would mandatorily require the application of enhanced due diligence.

Why

Customer risk categorization consists of attributing a risk rating to the customers which reflects the level of ML/TF risks of the customer. It is essential in order to determine the level of due diligence which will be applied on the customer and in order to request the appropriate documentation and information and to apply the appropriate level/intensity of the verification process and the related frequency of the monitoring of the business relationship in accordance with the risk rating of the customer. As regards the application of simplified due diligence measures, the professional must have clearly (and justifiably) identified that the relationship presents a lower risk of ML/TF before applying them.

Practical recommendations

Agents and e-money distributors shall know the customer's risk rating in order to request the appropriate type of documentation and information and take adequate risk-based measures.

In view of the ongoing monitoring, agents and e-money distributors shall understand the factors that may impact the customer's risk profile and rating such as, for instance, the fact that the customer/proxy/beneficial owner is or became (during the relationship) a PEP, that transactions are not coherent with the transactions expected considering the customer profile or with transactions usually processed by the customer, that the transfer of funds is coming from/going to high risk countries or any other events. In such cases, and if further guidance is needed by the agent and e-money distributor, they shall liaise with the PIs and EMIs on whose behalf they operate in order to clarify the actions to be taken and in particular to ensure that the level of due diligence and monitoring of the customer is adapted to the ML/TF risks. For identifying PEPs, the professional can check commercial databases available or take other measures, as described in Article 30 (1) of the CSSF Regulation.

5.6 Ongoing monitoring, name screening and transactions monitoring

Article 3 (2) (d) of the AML/CTF Law, Article 1 (3) of the Grand-ducal Regulation and Article 32 of the CSSF Regulation specify that a professional shall conduct ongoing due diligence of the relationship with their customers including scrutiny of the transactions executed during the relationship.

As part of the ongoing monitoring, the professionals shall ensure that the documents, data and information they have in the customers' files are up to date. It helps the professionals to better know their customers during the life cycle of the relationship. In this respect, they shall notably understand how often the files must be reviewed. The higher the customer's risk profile is, the more frequent the review shall be (Article 35 of the CSSF Regulation). In the specific case of an occasional client processing a one-off transaction, the data and information shall be maintained and updated should the client want to execute a new transaction subsequently.

In accordance with Article 33 of the CSSF Regulation, they are also requested to screen their data on a regular basis and at a minimum, and without delay, notably against new lists of sanctioned persons upon their publication. Indeed, the risk profile of the customers, on whose behalf they are acting or the beneficial owner in case of legal persons may change over time: whilst a customer might not be on the lists the day the professionals entered into the business relationship, it might appear on the lists the day after.

The professionals shall also be alerted where transactions are not consistent with their knowledge of the customers and shall analyse such situation. In accordance with Article 39 (2) of the CSSF Regulation, the professionals shall use an automated system for the transaction monitoring except when they can prove that the volume and nature of the customers and the transactions to be supervised do not require such automation.

Why

The prevention of ML/TF risks does not stop after the establishment of the business relationship with the customer. Ongoing monitoring is crucial as the customer risk rating may change over time. In simple words, customers might behave normally and provide valid documentation the first day, but they may start misusing the system the day after.

Practical recommendations

Agents and e-money distributors must have a good knowledge of their customers notably to determine their transaction behaviours. Let's remember also that agents and e-money distributors should be in a position to answer any questions that PIs and EMIs can have when they are analysing any alert or any question from a competent and/or judicial authority. This implies also that they must be in a position to provide any documentation that supports the information. Hence, agents and e-money distributors must ensure that the information and identification documents they have in the customer's files are sufficient, adequate and up to date. Agents and e-money distributors shall review the customers rated high risk at least once a year (Article 35 (1) of the CSSF Regulation).

As regards the name screening, it has to be ensured that an analysis of the results is performed and potential "hits" are duly assessed (hits being cases where the customer's name appears on a list which was screened). In this respect, agents and e-money distributors are reminded that they have to understand and be aware of the lists which have to be screened on a regular basis and at minimum after each publication (without delay), being all the official sanctions' lists like the European and Luxembourg financial sanctions (i.a. the ministerial regulations) which are published i.a. on the CSSF website and control them against their customer data base. In the event of a hit, the professional needs to take the relevant measure (e.g. freeze of funds) without delay.

As regards the transactions processed when the customers are coming to the office of the agents, they shall question the customers in instances where the transaction does not make sense compared to transactions usually processed or for example where the transaction consists of transfers to high risk countries or an identified PEP. In case of cash-based transactions, they shall understand the source of the cash used and why the transaction is made in cash. Additionally, agents and e-money distributors shall review retrospectively the transactions executed ("ex post") which consists of examining the history of transactions and potentially detecting suspicious patterns. This will help agents and e-money distributors to take necessary measures considering the risks they have identified as part of their AML/CTF risk assessment.

It is also key for agents and e-money distributors to be aware of the list of high-risk countries so that they can immediately react (and ask and challenge the adequate information/documentation) in case a customer wants to process a transfer to or receive funds from such countries.

5.7 Cooperation with the authorities

Under Article 5 of the AML/CTF Law, Article 8 of the Grand-ducal Regulation and Articles 47 and 48 of the CSSF Regulation, the professionals, their directors, managers and employees are obliged to cooperate with Luxembourg authorities responsible for the fight against ML/TF and to inform promptly the Luxembourg FIU when they know, suspect or have reasonable grounds to suspect that a ML/TF predicate offense is committed. Professionals are also obliged to provide without delay any information requested by the FIU.

Additionally, where a professional suspects that a transaction relates to ML/TF, the professional shall refrain from carrying out and executing the transaction and make a suspicious transaction report to the FIU.

Importantly, according to Article 5 (5) of the AML/CTF Law, the professionals shall understand that they are not authorized to disclose to the customer or any other third party the fact that they have made a report to the FIU or they are in contact with them unless they have the express consent of the FIU.

Why

Reporting suspicious behaviours, activities or transactions is decisive to contributing to stopping ML and avoiding TF, arresting criminals or avoiding a terrorist attack taking place and to freezing illegal funding of such attacks or criminal acts.

Practical recommendations

Importantly, agents and e-money distributors shall understand that any suspicious activity or transactions they discover must be reported to the FIU.

Agents and e-money distributors shall also understand which indicators may lead them to consider that they are facing a ML/TF case and they must therefore make a report to the FIU. In this respect and if the agents and e-money distributors need further guidance, they should contact the PIs/EMIs on whose behalf they are acting and they should seek guidance from that institution.

Additionally, agents and e-money distributors should know the point of contact of the judicial authorities that they should liaise with, should they be contacted directly by foreign judicial authorities in order to cooperate (name, phone number etc.).

It is reminded that the Financial Investigation Unit in Luxembourg is the Cellule de Renseignement Financier – "CRF". All information related to the process for reporting suspicious activities or transactions to the CRF can be found on their website: https://justice.public.lu/fr/organisation-justice/crf.html

5.8 Cooperation with the authorities pursuant to name screening results, i.e. as regards "states, persons, entities and groups subject to restrictive measures in financial matters"

In accordance with Article 3 (2) of the AML/CTF Law and Articles 33 and 39 of the CSSF Regulation and in order to comply with the law dated 19 December 2020 on the implementation of restrictive measures in financial matters, the professionals shall identify without delay "states, persons, entities and groups subject to restrictive measures in financial matters" whether or not they are involved in a transaction. In case such persons are identified, the professionals shall without delay inform the Luxembourg Ministry of Finance. A copy of the communication shall be sent to the CSSF at the same time.

Why

To know that funds or other economic resources of "states, persons, entities and groups subject to restrictive measures in financial matters" have been subject to a freeze is decisive for Luxembourg authorities that are in charge of financial restrictive measures.

Practical recommendations

Agents and e-money distributors shall understand their obligations as regards the identification without delay (i.e. within hours of the publication of the list) of "states, persons, entities and groups subject to restrictive measures in financial matters", the obligation of immediately freezing the funds upon detection of such persons and/or the detection of any transactions from/to such persons and the importance of reporting without delay the detection of such persons and/or the detection of any transactions from/to such persons to the Luxembourg Ministry of Finance.

Additionally, agents and e-money distributors should know the point of contact from the Luxembourg Ministry of Finance with whom they should liaise.

All information related to "restrictive measures in financial matters" can be found on the Luxembourg Ministry of Finance website: https://mfin.gouvernement.lu/fr/dossiers/2018/sanctions-financiaires-internationales.html

Additional information and guidance including a Frequently Asked Question can be found on the CSSF website: https://www.cssf.lu/en/international-financial-sanctions/

5.9 Record-keeping obligations

Article 3 (6) of the AML/CTF Law, Article 1 (5) of the Grand-ducal Regulation and Article 25 of the CSSF Regulation lay down that professionals shall retain documents, data and information that supports the customer identification and verification as well as supporting evidence and records of the transactions they have executed. The data, documents, information (including results of analysis for example) shall be kept for a period of 5 years after either the end of the business relationship with the customer or the date of an occasional transaction.

Why

Record-keeping is fundamental to assist for example judicial authorities in case of potential investigations of ML/TF cases.

Practical recommendations

Agents and e-money distributors should be in a position to immediately handle any request from the Luxembourg FIU or other competent authorities. This implies that agents and e-money distributors should be in a position to retrieve immediately any information and documents that support the request and that therefore their files have to be well organized.

Where agents and e-money distributors have paper-based documentation, they shall ensure that their archives are protected against any external damages that could destroy the documents (as for example a protection against fire). Agents and e-money distributors are encouraged to obtain the adequate administrative and technological support from the PIs and EMIs on whose behalf they are acting.

Despite a cessation of activities, the 5 years period for keeping the completed document after the end of the relationship or after the date of the transactions has been processed needs to be respected. For the relationships which have not yet been terminated as at the date of the cessation of the activities, the 5 year period starts upon the cessation of activities which is considered as ending the relationship.

5.10 AML/CTF training

Article 4 (2) of the AML/CTF Law and Article 46 of the CSSF Regulation state that professionals shall set up an ongoing training programme so that their employees are informed about new AML/CTF developments including techniques, methods and trends in ML/TF and to help them recognize operations which may be related to ML/TF. Where the training programme is developed abroad, for instance by the PIs and EMIs established in other Member States, it shall mandatorily integrate the legal and regulatory rules applicable in Luxembourg.

Why
Training on AML/CTF matters is essential for staff to understand the ML/TF risks and the related AML/CTF requirements and processes and to adopt an adequate behaviour to identify suspicious activities and transactions.
Practical recommendations
Agents and e-money distributors shall be proactive in improving their knowledge and the knowledge of their employees with respect to the management of ML/TF risks. In particular, they shall ensure that the employees are able to identify for example forged documents (while such documents are more and more difficult to detect) and to recognize the indicators that a customer's behaviour or a transaction is suspicious.

6 CSSF initiatives

The CSSF has identified the following initiatives in order to further enhance its AML/CTF supervision over agents and e-money distributors:

Further enhance the communication with other regulators. As it is already the case today, the CSSF will continue to cooperate with the competent authorities of the Home Member States of the PIs and EMIs on whose behalf agents and e-money distributors are acting.

Continue gathering data to support its supervisory activities. In this respect, the CSSF will continue sending and analysing the AML/CTF questionnaire on an annual basis. Where deemed necessary, the AML/CTF questionnaire will be refined, by taking into account the results of its analysis of the questionnaires submitted in the previous years.

Further promote understanding of ML/TF risks and AML/CTF obligations. The CSSF will continue analysing the ML/TF risks to which agents and e-money distributors are exposed in order to further promote the understanding of the ML/TF risks and the related AML/CTF obligations. The CSSF will also continue to visit agents and e-money distributors in order to verify that they are complying with the AML/CTF obligations. Such visits are also a good opportunity to educate agents and e-money distributors on AML/CTF related matters. Last, the CSSF will keep on organizing conferences with the payment/e-money private sector including agents and e-money distributors to share best practices.

7 APPENDIX A – Red flag indicators

This list of indicators has been established using the factors identified in the ESA's Risk Factors Guidelines dated January 20181, in the FATF Guidance for a Risk-Based Approach for Money or Value Transfer Services dated February 20162, in the FATF Guidance for a Risk-Based Approach to prepaid cards, mobile payments and internet-based payment services dated June 20133. Agents and e-money distributors are encouraged to read these documents.

Customer risk The key risk factors that agents and e-money distributors should consider are:	- The customer is reluctant or refuses to provide the data or document requested or the agent/distributor has reasonable grounds to suspect that the provided information is incorrect or insufficient - The customer refuses to disclose the source of funds - The officer suspects that the customer is using fake/forged identification documents or the customer provides such documents - The officer suspects the customer is acting for another person but is evasive or reluctant to provide information - The customer is associated with a person known to be involved in criminal activities or to politically exposed person suspected of corruption - There is a lack of apparent relationship between the customer and the beneficiary of the funds being transferred - The customer is evasive about the reason why he/she is doing the transaction - The customer is in a hurry to complete the transaction and promises to provide supporting information the day after - The customer is playing on the cord stating the beneficiary of the transactions needs the funds and cannot live without them

[1] *https://esas-joint-committee.europa.eu/Publications/Guidelines/Guidelines%20on%20Risk%20Factors_EN_04-01-2018.pdf*

[2] *https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-money-value-transfer-services.pdf*

[3] *FATF Guidance for a Risk-Based Approach to prepaid cards, mobile payments and internet-based payment services*

Country or geographic risk The provision of services may be of a higher risk when they are connected to a higher risk country:	- Frequent transfers to higher risk countries - Transfers to beneficiaries located in higher risk countries without reasonable explanation - Transfers to countries where groups are committing terrorist offences or are known to operate - The customer has no evident relationship with the country where he/she sends/receives the money and cannot explain why the money is sent/received to/from there
Transaction risk Risk factors indicating transactions/services provided are used to assist money launderers or terrorist financing can include:	- The transaction is inconsistent with the customer socio-economic profile - The activity or transaction volume is not consistent with the customer profile (age, occupation,…) - The transaction is inconsistent with the declaration of the customer - Series of transactions are executed within a short time period without reason - Multiple senders are transferring money to the same beneficiary - Money is received from the same individual from different agent locations - Numerous transactions are executed by a customer over a short period of time such that the amount of each transaction is not significant but the cumulative total is significant - Funds received from religious or charitable organisations and transfer of funds within a short period to another person or to person located in highest risk countries - Unusually large cash transaction - Presence of counterfeit banknotes - Cash transactions followed closely by transfer of funds on the same day at another point of time or the next day - Significant discrepancies between the customer declaration of the total amount of cash and the counted amount - The customer shows no interest in the transfer costs even if the latter are very important - The customer offers a bribe or a tip to have the transaction processed

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