Commission de Surveillance du Secteur Financier

Luxembourg, 10 April 2020

To all professionals under AML/CFT supervision of the CSSF

CIRCULAR CSSF 20/740

Re: Financial crime and AML/CFT implications during the COVID-19 pandemic

Ladies and Gentlemen,

The purpose of this Circular is to provide guidance to all professionals subject to anti-money laundering and counter-terrorism financing (AML/CFT) supervision of the CSSF in relation to the money laundering and terrorism financing (ML/TF) risks and AML/CFT implications of the COVID-19 pandemic. This Circular should be read in conjunction with related guidance on COVID-19 by EU, international and national authorities including the Financial Action Taskforce (FATF),[1] the European Banking Authority (EBA),[2] the Cellule de Renseignement Financier (CRF),[3] EUROPOL,[4] and INTERPOL,[5] as well as related guidance on AML/CFT previously issued by the CSSF (e.g. CSSF Circular 19/732 and CSSF Circular 17/661).[6]

The CSSF supports the measures taken and proposed by Luxembourg's government and international bodies to address the health and economic impacts of the COVID-19 pandemic. The CSSF is committed to safeguarding the integrity of the financial sector and reiterates that the fight against financial crime remains a priority. The CSSF notes that as many economies experience a downturn, financial flows are likely to diminish.[7] However, experience from past crises suggests that in many cases illicit financial flows will continue, and criminals and terrorists may seek to exploit temporary weaknesses in AML/CFT controls.[8] The CSSF therefore requires that supervised professionals continue to put in place and maintain effective systems and controls to ensure that Luxembourg's financial system is not abused for ML/TF purposes.

This guidance is structured as follows:

- Section 1 sets out several new and emerging ML/TF threats resulting from COVID-19;
- Section 2 describes several possible areas of particular vulnerability for the financial sector;
- Section 3 describes several mitigating actions that require particular focus for supervised professionals; and
- Section 4 outlines CSSF's approach to AML/CFT supervision during this period.

[1] FATF, Statement by the FATF President: COVID-19 and measures to combat illicit financing, 2020. Available here.
[2] EBA, Statement on actions to mitigate financial crime risks in the COVID-19 pandemic, 2020. Available here.
[3] CRF, Typologies COVID-19, 2020. Available here.
[4] EUROPOL, Pandemic profiteering – How criminals exploit the COVID-19 crisis, 2020. Available here.
[5] INTERPOL, INTERPOL warns of financial fraud linked to COVID-19, 2020. Available here.
[6] A full list of CSSF Circulars related to AML/CFT are available here.
[7] EBA, Statement on actions to mitigate financial crime risks in the COVID-19 pandemic, 2020. Available here.
[8] EBA, Statement on actions to mitigate financial crime risks in the COVID-19 pandemic, 2020. Available

1. Emerging ML/TF threats from COVID-19

Criminals around the world are taking advantage of the COVID-19 pandemic and are finding new ways to generate illicit funds.[9] New and emerging ML/TF threats[10] concern the most vulnerable in society as well as the general public at large. They include:

- Those crimes that represent both a significant operational risk for financial institutions and a ML/TF threat – namely cybercrime and fraud;
- Those crimes where the risk to financial institutions is primarily related to the laundering of illicit proceeds – namely bribery and corruption, trafficking in counterfeit goods, robbery or theft, and insider trading and market manipulation.

The nature of each of these threats is outlined below.

1.1 Cybercrime

The imposition of social distancing rules has increased the demand for information and supplies through online channels, significantly increasing cyber security risks for users.[11] Social engineering attacks[12] (such as phishing emails – an example of which is provided below) have increased and there have been numerous cyber-attacks against organisations and individuals (e.g. malware via malicious links and attachments). According to Europol, law enforcement partners have also reported an increase in "online activity by those seeking child abuse material" as "offenders welcome opportunities to engage with children whom they expect to be more vulnerable due to isolation, less supervision and greater online exposure".[13] Where such services are accessed via cryptocurrency payments, this may present a ML/TF threat for Virtual Asset Service Providers (VASPs).

For financial institutions, the operational risks related to cybercrimes are significant and have been amplified by the changes to work practices put in place to allow for social distancing. These "amplifiers" include: (1) the alternative/remote modes of working required; (2) utilization of different technologies; (2) less familiar modes of data exchange; (3) constraints on facility access and collaboration; (4) management and staff distraction; (5) key personnel risk; and (6) the necessary re-balancing of supply chain dynamics and reliance on third parties. These amplifiers make financial institutions and their employees particularly exposed to cybercrimes.

Case Study 1: Phishing scams in Luxembourg using World Health Organisation (WHO) name

Phishing and email scam campaigns are typically designed to obtain personal information, which can then be used by criminals to steal funds. There has been a significant increase in the amount of scam campaigns related to COVID-19 since January 2020, with research by internet security company Sophos suggesting that the volume of COVID-19 email scams nearly tripled in one week during the end of March, with almost 3% of all global spam now estimated to be Covid-19 related.[14]

Several of these scams have attempted to use the WHO brand to obtain personal information from victims. In Luxembourg, the government has confirmed one such scam in which senders purporting to be from the WHO or travel agents sent malware-ridden links to a COVID-19 interactive map.[15]

[9] EUROPOL, Pandemic profiteering – How criminals exploit the COVID-19 crisis, 2020. Available here.
[10] "Threats" include predicate offences that generate illicit proceeds which could give rise in particular to ML
[11] EUROPOL, Pandemic profiteering – How criminals exploit the COVID-19 crisis, 2020. Available here.
[12] In the context of cyber security, "social engineering attacks" are the psychological manipulation of people into performing actions or divulging confidential information
[13] EUROPOL, Pandemic profiteering – How criminals exploit the COVID-19 crisis, 2020. Available here.
[14] SOPHOS, Facing down the myriad threats tied to COVID-19, 2020. Available here.
[15] US Embassy in Luxembourg, Security Alert – Beware of Fraud During COVID-19, 2020. Available here.

1.2 Fraud

Criminals have also been "very quick to adapt well-known fraud schemes to target individual citizens, businesses and public organisations" during the pandemic.[16] Such frauds include adaptations of existing telephone schemes (e.g. criminals call victims pretending to be clinic or hospital officials, who claim that a relative of the victim has fallen sick with the virus and request payments for medical treatment), scams related to fake medical and protective equipment (as shown in the case study below) and those related to internet banking accounts.[17] Across Europe, the growth in the number of frauds related to COVID-19 has been rapid, with one country reporting a 400% increase in March.[18]

For financial institutions, the operational and businesses risks related to such frauds are significant. Criminals may attempt to exploit the operational weaknesses that arise from home working (e.g. more limited operational resources, slower systems) and the increased activity in markets (e.g. fund redemptions, changes to payment volumes, foreign exchange transactions) may allow them to more easily circumvent controls. Financial institutions may then be liable for fraud losses and reimbursements (which are likely to rise); they may face increasing operational costs to work on fraud cases (e.g. due to rising numbers of customers affected); and they may have more customers that receive a negative experience (e.g. due to longer waiting periods to deal with cases). Fraud therefore represents both an operational and business risk, as well as a ML/TF threat (i.e. if illicit proceeds from fraud are laundered through financial institutions).

Case Study 2: COVID-19 used as a pretext to divert payments (from the CRF typologies report)[19]

"CEO and Business E-Mail Compromise (BEC) fraud are well-known and have been the subject of extensive prevention campaigns. Fraudsters are now taking advantage of the situation created by the COVID-19 pandemic, including the containment and social distancing measures as well as economic dislocation, to evade the diligence thresholds of targeted companies.

The following two examples illustrate this:

1) Fraudsters impersonate the director of a legitimate company and contact the company's financial institution. The purported director explains that the entire business is currently disrupted and that he or she is working from home. He or she argues that it is therefore not possible to follow the usual procedures (in particular countersignatures) and insists on a communication exclusively by e-mail.

2) Under the pretext of corporate disruption, fraudsters argue that payments are no longer to be made to the company's central banking accounts, but directly to the banking accounts of the relevant production sites. They may also argue, for example, that they are experiencing cash flow problems or problems with their accounting department. This scheme allows payments made within the framework of an existing business relationship to be diverted to fraudulent accounts."

1.3 Bribery and corruption related to government support schemes

Across the world, governments have adopted substantial stimulus packages to support businesses throughout the economic downturn associated with COVID-19, creating the potential for abuse by those who administer them. These measures include direct grants, tax advantages, advance

[16] EUROPOL, Pandemic profiteering – How criminals exploit the COVID-19 crisis, 2020. Available here.
[17] EUROPOL, Pandemic profiteering – How criminals exploit the COVID-19 crisis, 2020. Available here.
[18] ActionFraud, Coronavirus-related fraud reports increase by 400% in March, 2020. Available here.
[19] CRF, Typologies COVID-19, 2020. Available here.

payments, state guarantees for loans taken from banks, subsidised public loans, and numerous other measures. The exceptional circumstances, unprecedented size[20] and urgency of such measures may create opportunity for abuse, and therefore poses a material ML/TF threat for financial institutions. The threat also extends beyond government support schemes, with the closure of airports, ports and other handling facilities for international trade increasing the risk of bribery of customs and other related officials.

1.4 Trafficking in counterfeit medicines and other goods

Europol has also identified the distribution of counterfeit and/or sub-standard goods as a key area of criminal activity in relation to the COVID-19 pandemic.[21] This includes specific activities related to personal protective equipment (PPE), pharmaceutical products, and other healthcare products, including the distribution of fake COVID-19 home testing kits (as shown in the case study below). This activity is occurring both online and offline and is likely to continue to increase, in particular if counterfeiters use shortages in the supply of some goods to provide fake alternatives. The possible laundering of proceeds from these crimes therefore creates a material ML/TF threat for supervised professionals.

Case Study 3: INTERPOL Operation Pangea – Criminals taking advantage of the high demand in hygiene products driven by the COVID-19 outbreak [22]

Operation Pangea, a global operation coordinated by INTERPOL, targeted the trafficking of counterfeit medicines from 3-10 March 2020 as criminals began to take advantage of the high demand in hygiene products driven by the COVID-19 outbreak. The operation involved 90 countries worldwide and resulted in 121 arrests.

During the operation, authorities around the world seized 37,000 unauthorised and counterfeit medical devices (mostly surgical masks and self-testing kits for HIV and glucose monitoring) and EUR 13 MM in potentially dangerous pharmaceuticals (e.g. unauthorised antiviral medications and the antimalarial chloroquine). Painkillers and antibiotics also represented a significant portion of the seizures.

1.5 Robbery or theft

The pandemic has also created new opportunities for organised crime groups involved in thefts, burglaries, robberies and other scams.[23] This includes organised burglaries of commercial premises and medical facilities, as well as specific schemes targeting vulnerable members of society such as the elderly. In some cases, criminals have been known to approach "victims at home by pretending to be law enforcement or healthcare officials offering testing for COVID-19 and other pretences to enter homes and steal valuables". The laundering of proceeds from such activities creates a ML/TF threat for supervised professionals, because they could be used to inject, layer or integrate the proceeds of these primary offences.

[20] For details, see for example: European Council, COVID-19 coronavirus outbreak and the EU's response, 2020. Available here.

[21] EUROPOL, Pandemic profiteering – How criminals exploit the COVID-19 crisis, 2020. Available here.

[22] INTERPOL, Rise of fake "corona cures" revealed in global counterfeit operation, 2020. Available here .

[23] EUROPOL, Pandemic profiteering – How criminals exploit the COVID-19 crisis, 2020. Available here. EUROPOL refers to these crimes collectively as "organised property crime". This encompasses a range of different criminal activities carried out predominantly by mobile organised crime groups operating across the EU. Organised burglaries, thefts and robberies as well as motor vehicle crime and the trafficking of cultural goods all fall into this broad category of criminal activity.

Case Study 4: "Faking and entering" scams

Multiple European Member States have reported similar modus operandi for "faking and entering" scams. In one Member State, "the perpetrators called the victim to inform them that a relative is infected and in hospital. They claimed that doctors would have to come and take an immediate 'corona test'. These fake doctors came to the victim's home in protective clothing and masks in the middle of the night. The suspects then took an apparent swab sample from the victim's mouth and wiped his forearms with apparent strips of paper to test it. He was then told that the evaluation of the test would take about five hours".[24]

The Luxembourg government has confirmed several attempted cases. "In the regions of Mamer, Capellen, and Holzem, individuals have reportedly offered to disinfect the homes of the elderly in order to gain access. In neighboring countries, fraudsters have disguised themselves as medical staff for the same purpose".[25]

1.6 Insider trading and market manipulation

The threat of market abuse is also likely to have grown during this period. The particular nature of information related to COVID-19's impact on issuers, and the sometimes unusual channels the information is transmitted, may result in a higher number of employees and other categories of persons having access to insider information (and therefore increase the risk of abuse). The assessment of anticipated direct and indirect impact of COVID-19 on the activities, the performance, or the outlook of an issuer is a complex issue and publication of financial information may have to be delayed in order to take this properly into account.

In addition, high volatility in financial markets increases the risk of persons trying to take advantage of inside information or to manipulate the market for their benefit (e.g. via dissemination of false information),[26] and criminals may misuse financial institutions to commit such a crime and/or launder the proceeds. The threats of market abuse are particularly relevant in the sectors linked directly to COVID-19, such as the pharmaceutical sector (which has reacted with large price swings to information relating to potential vaccines). Furthermore, there is an increased risk that inside information may be leaked in the current circumstances, as persons in possession of inside information may use insufficiently secure communication channels in the context of remote working arrangements. Competent market authorities have stressed the importance for issuers to take particular care of their information obligations under the market abuse regulations and to publish significant information as soon as possible.

2. Emerging ML/TF vulnerabilities

The CSSF acknowledges that it is possible that specific areas in the Luxembourg financial sector could be exploited by emerging ML/TF threats like those described above, and therefore encourages all professionals to remain vigilant. Notwithstanding this, there are several vulnerabilities[27] that may be particularly relevant. These include: (1) online payment services; (2) clients in financial distress; (3) mortgages and other forms of collateralised lending; (4) credit backed by government guarantees; (5) distressed investment products; and (6) delivery of aid through non-profit organisations. The nature of each is outlined below.

2.1 Online payment services

The social distancing rules imposed in Luxembourg and many other countries have resulted in

[24] EUROPOL, Pandemic profiteering – How criminals exploit the COVID-19 crisis, 2020. Available here.
[25] US Embassy in Luxembourg, Security Alert – Beware of Fraud During COVID-19, 2020. Available here.
[26] For similar typologies, see for example: FATF, Guidance for risk-based approach – securities sector, 2018. Available here.
[27] "Vulnerabilities" are those things that can be exploited by the threat or that may support or facilitate its activities

consumers turning to online channels for purchases of goods and services. For example, research suggests that in some countries, online food delivery services have risen by ~40% year-on-year and this trend is likely to continue.[28] This surge in online purchases is likely to increase both the volume and value of online payments services, including the use of internet banking. This may create more opportunity for criminals to conceal illicit funds within a greater amount of legitimate payments made online.

2.2 Clients in financial distress

The economic impact of COVID-19 is likely to be significant and Luxembourg's national statistics bureau has stated it will downgrade short-term economic prospects for the country.[29] This contraction in economic activity could place some clients of supervised professionals in distress (more likely commercial borrowers such as corporates and SMEs, but also including individuals). In turn, this has the possibility to create opportunities for them to be exploited by criminals seeking to launder illicit proceeds. For example, if an SME is called to make a significant payment by a credit institution, circumstances could arise in which it is forced to accept proceeds from an organised crime syndicate in order to finance the payment. This may be done in exchange for an ownership share in the business, facilitating integration of illicit proceeds.

2.3 Mortgages and other forms of collateralised lending

The economic impact of the pandemic may also affect those clients with collateralised term loans who are required to make regular fixed payments. Some clients could be pushed into financial distress as a result (see above). Furthermore, credit institutions may re-value existing collateral and request additional collateral to be placed against current or new loans. If controls on the origin and source of funds and wealth are relaxed to obtain such collateral, this could facilitate the entry of illicit proceeds into the financial system.

2.4 Credit backed by government guarantees

Through the Temporary Framework for State Aid Measures, Luxembourg and the European Commission have provided support to businesses to counter the economic impact of COVID-19. These measures include repayable advances and guarantees in loans to companies by Banks.[30] However, there is the potential that such schemes could be misused by criminals. This could include fraudulently obtaining funds without intention of repaying them (e.g. the beneficiary declaring bankruptcy once the repayments are due) as well as misusing the scheme to launder money. For example, in the latter case, a criminal owning or controlling a corporate structure which is eligible to receive support (e.g. because it qualifies as an SME) could use repayment of the loan as a justification to transfer funds of illicit origin deposited elsewhere into their accounts in Luxembourg.[31]

2.5 Distressed investment products

Due to the economic impact of COVID-19, many stock markets and investment products around the world have experienced significant declines in value.[32] Where assets are valued at a significant discount,

[28] earnest, Coronavirus is changing how we spend money, 2020. Available here.
[29] STATEC, Coronavirus threat becomes a reality, 2020. Available here.
[30] For further details see: European Commission, Temporary Framework for State aid measures to support the economy in the current COVID-19 outbreak, 2020. Available here.
[31] Similar typologies can be founded in: FATF, Money laundering and terrorist financing through the real estate sector, 2007. Available here.
[32] European and American stock markets fallen over 30% since February. See: STATEC, Coronavirus threat becomes a reality, 2020. Available here.

investors may be looking to offload and minimise losses. This could provide an opportunity for criminals offering to purchase or re-finance such distressed assets (using the backing of illicit funds).

2.6 Delivery of aid through non-profit organisations

COVID-19 has highlighted once again the vital work of charities and NPOs in addressing public health emergencies. FATF has highlighted that most NPOs carry little or no ML/TF risk and the FATF Standards do not require all NPOs to be considered high risk. However, where there are increased financial flows through NPOs to higher risk countries, there may be an increased risk of illicit activity and special attention should be paid to the risks of TF. In addition, there remains the potential for tax advantages afforded by charitable donations to be misused by those seeking to launder illicit funds. FATF has therefore encouraged countries to work with relevant NPOs to ensure that much needed aid is getting to its intended recipients in a transparent manner.[33]

3. Mitigation of emerging ML/TF risks

In response to new and emerging risks, CSSF expects supervised professionals to continue to implement and maintain effective systems and controls to ensure that the financial system is not abused or misused for ML/TF purposes. In order to adapt to the changing nature of the ML/TF risk created by the pandemic, the CSSF would like to stress several areas that require particular focus for supervised professionals. These are: (1) AML/CFT business continuity; (2) transaction monitoring; (3) customer due diligence (CDD); (4) ML/TF risk assessment; and (5) cooperation with authorities. In addition to the below, CSSF also encourages professionals to consult the CRF's recent guidance on COVID-19 typologies, which includes several indicators of suspicious activity.[34]

3.1 AML/CFT business continuity and governance

The CSSF acknowledges the business continuity challenges presented by the pandemic but encourages all professionals to ensure that sufficient focus is given to operating AML/CFT controls in a manner compliant with the obligations set out in the Law of 12th November 2004 (as amended) on AML/CFT (hereafter the "2004 AML/CFT Law"). Adequate attention should be given to ensuring that AML/CFT controls remain fully operational. In particular, professionals should ensure that effective processes are in place to apply AML/CFT controls whilst staff are working remotely (e.g. access to relevant databases and screening systems, capability to receive and review relevant documents electronically). They should also ensure that adequate communication and information exchange between colleagues continues (for instance, Compliance Officers could make themselves available for periodic Q&A video conferences to replicate ad-hoc in-person questions from colleagues). In addition, professionals should give appropriate attention to checking key decisions are correct (i.e. given that errors may be more likely in the current working environment), including those related to controls over third party AML/CFT outsourcing. Professionals should ensure there is sufficiently close collaboration across business, operations, analytics, compliance, risk and IT functions to ensure immediate information flow.

The CSSF also encourages all professionals to confirm the robustness of their cyber risk controls. The CSSF has provided guidance on the minimum IT security conditions recommended for remote access in its press release of March 3rd, 2020 and on its live COVID-19 FAQ.[35] The CSSF now suggests that professionals reflect on whether their measures in these areas are appropriate and functioning. Professionals may wish to consider: (1) rapidly deploying a cyber-risk awareness campaign (e.g. via targeted emails or an all-staff webinar); (2) checking and confirming access arrangements and controls

[33] FATF, Statement by the FATF President: COVID-19 and measures to combat illicit financing, 2020. Available here.
[34] CRF, Typologies COVID-19, 2020. Available here.
[35] CSSF, FAQ COVID-19, 2020. Available here.

(e.g. check lists used for name-screening are correctly downloaded); (3) reviewing current monitoring, logging, and data loss prevention arrangements (e.g. confirm there has been no unauthorised modifications of transaction monitoring rules); (4) identifying where systems and application security needs to be strengthened; and (5) engaging with cyber security community and proactively exchanging "indicators of compromise" (IOCs).[36]

3.2 Transaction monitoring

The CSSF requires professionals to continue to monitor transactions and pay particular attention to any unusual or suspicious patterns in customers' behaviour and financial flows. Professionals should take risk-sensitive measures to establish the legitimate origin of unexpected financial flows, in particular where these flows stem from customers in sectors that are known to have been impacted by the economic downturn and COVID-19 mitigation measures. Examples of such businesses can include: (1) cash intensive businesses in the retail sector; (2) companies involved in international trade; and (3) any corporate structure operating in a sector facing an economic downturn which may keep a similar volume of financial flows in the absence of real economic activities. Professionals should also closely monitor those customers who may see significant increases in financial flows, for example pharmaceutical companies, gaming companies and supermarkets.

Professionals should also be aware that there may be a large increase in false positives from transaction monitoring and fraud prevention systems that use machine learning techniques. This is the result of such software being trained and based on data from periods of normal economic activity. Professionals should be prepared to adapt these models and may need to employ more manual identification and classification of alerts. They should be aware that such systems may fail to capture new and emerging threats (as those outlined above) and Compliance functions should review critically the rules and thresholds in place to ensure they are adequate and continue to work effectively.

Professionals should also confirm the adequacy of third party outsourcing related to transaction monitoring (and other key AML/CFT processes). This should include verifying the adequacy of business continuity arrangements taken by third parties providing outsourcing arrangements and considering necessary (additional) measures to ensure effective monitoring.

3.3 Customer due diligence (CDD)

The CSSF encourages professionals to continue to apply the CDD measures required under the 2004 AML/CFT Law and to consider how these can be strengthened to mitigate the impact of a lack of face-to-face contact with customers. Any enhanced measures should be done in line with a risk-based approach and take into account the specific threats mentioned above. Measures could include performing more frequent checks against lists of Politically Exposed Persons (PEPs) and conducting additional or more detailed checks as part of enhanced due diligence processes (that are able to be done remotely, such as adverse media screening). It is particularly important to employ appropriate CDD processes when approving applications for government support, due to the short timelines often associated with such requests and the possible additional associated ML/TF risk (see above for examples of possible typologies).

The CSSF also echoes FATF's call to use financial technology (Fintech) to manage some of the CDD issues presented by COVID-19. As outlined in FATF's recent statement, "use of digital/contactless payments and digital onboarding reduce the risk of spreading the virus" and "in line with the FATF Standards, the FATF encourages the use of technology, including Fintech, Regtech and Suptech to the fullest extent possible". CSSF encourages professionals to consult the FATF's Guidance on Digital ID[37] which highlights the benefits of trustworthy digital identity for improving the security,

[36] Indicators of compromise (IOCs) are pieces of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network

[37] FATF, *Guidance on Digital ID*, 2020. Available here.

privacy and convenience of identifying people remotely for both onboarding and conducting transactions while also mitigating ML/TF risks. In line with this guidance, the CSSF encourages professionals to consider that digital ID systems should rely upon technology, processes, governance and other safeguards, that provide an appropriate level of trustworthiness. This can be determined by considering the three questions for professionals set out in the FATF guidance: (1) Is the digital ID system authorised by government for use in CDD?; (2) Do you know the relevant assurance level/s of the digital ID system?; and (3) Is the digital ID system appropriate for the ML/TF risk situation?

The CSSF however stresses that these measures need to be compliant with the requirements as introduced by the law of 25 March 2020 into the 2004 AML/CFT Law (Articles 3(2) a), 3(2) b), 3(6), 3-3 and Annex IV.2.c)). In this context, CSSF would like to draw the attention to the CSSF FAQs on AML/CFT and IT requirements for specific customer on-boarding/KYC methods for the identification/verification through video chat.[38] Thus the verification of customer identity via live video-chat, or the use of electronic identification means, could be considered an appropriate safeguard in view of the above-mentioned requirements (i.e. lack of face-to-face contact). The CSSF highlights that other mitigation measures in such situations may include: (1) the collection of additional documents; (2) the certification of documents; (3) the reliance on a third party having already identified the customer (e.g. other professionals of the financial sector, or service providers offering document verification services); and (4) the check by means of a first transfer of funds from a bank account in the name of the customer with a credit institution established in Luxembourg, in the EU, or in any other country respecting equivalent AML/CFT obligations and being supervised for that purpose.

The CSSF would like to remind professionals that in case the identification of the customer cannot be fully performed, or where it raises suspicions on the identity of the customer, the professionals must refrain from entering into a business relationship and cooperate with the authorities. The CSSF encourages professionals to consult CSSF Circular 17/661 and the ESA's Guidelines on ML/TF Risk Factors and Simplified and Enhanced Customer Due Diligence for further information.[39]

3.4 ML/TF risk assessment

CSSF encourages professionals to take a dynamic approach to ML/TF risk assessments and incorporate the risks associated with COVID-19 as part of these activities. This is particularly relevant for those risk assessments completed at the product or business unit level. Specifically, CSSF encourages professionals to: (1) identify and assess the risks of specific ML/TF arising from COVID-19 which relate to their specific business model; (2) implement additional mitigating measures (as appropriate and on a risk-basis) to combat these risks; and (3) communicate these risks across their organisation, for example through an all-staff communication.

3.5 Cooperation with authorities

CSSF reminds professionals of the importance of continuing to cooperate closely with competent authorities. This includes reporting suspicions of ML/TF to the CRF without delay (including in relation to new and emerging ML/TF risks as described above), as well as continuing to interact with CSSF as part of its supervisory activities (e.g. responding in a timely manner to information requests, keeping regular communication in relation to deadlines). Professionals should also be proactive in using industry bodies, fora, committees and working groups (including CSSF's AML/CFT Expert Working Groups) to share typologies and trends in real-time to help collectively combat these new ML/TF threats. Facilitating swift information flow from these fora can better enable professionals to take the appropriate actions required in relation to adapting transaction monitoring, CDD etc.

[38] CSSF, Frequently asked questions on AML/CTF and IT requirements for specific customer on-boarding/KYC methods, 2020. Available here.

[39] ESAs, Guidelines on risk factors and simplified and enhanced customer due diligence, 2017. Available here.

4. CSSF approach to AML/CFT supervision during COVID-19

The CSSF remains deeply committed to combatting ML/TF and ensuring that the risks arising from and within the Luxembourg financial sector are effectively managed and mitigated. The CSSF will continue to support the financial sector through this difficult time (in particular through issuing information through press releases and up-to-date FAQs) and has re-focused its interventions in order to maintain those which are currently key to preserving financial stability and protecting investors and consumers. The CSSF also continues to coordinate actively with the European authorities, such as the European Central Bank (ECB), the European Securities and Markets Authority (ESMA) and the European Banking Authority (EBA).

The CSSF remains fully operational and has implemented several measures to ensure it meets the operational challenges associated with AML/CFT supervision during this time. The CSSF has created an internal coordination committee to manage its response to the pandemic, which meets daily and remains in close contact with relevant national and international authorities. Through the implementation of its business continuity plan its agents are working remotely and interacting with supervised professionals via digital and secure channels.

Whilst the priority of the CSSF is the health of its staff, the CSSF will continue AML/CFT supervisory activities during this period. AML/CFT on-site inspections that have already commenced will be completed and the CSSF will also commence inspections on a remote basis during this period. Off-site supervisory activities are also continuing. Regarding the CSSF Circular Letter of 31st January 2020 on the annual AML/CFT online survey ("Survey") for the year 2019,[40] the CSSF has extended the deadline for submission to 10th April 2020 (today).[41]

The CSSF continues to communicate with supervised professionals in relation to AML/CFT throughout this period. Communications can be made in the following way:

- All communications should be done either through the eDesk for those who have registered, or by e-mail rather than regular mail;
- All outgoing communications from the CSSF will be done by e-mail, carrying no handwritten signature from the CSSF. Please verify that it originates from the domain name @cssf.lu, and please remain vigilant as to potential frauds. If you have any suspicion as to the message received, please phone your usual contact person at the CSSF, or our switchboard; and
- CSSF remains available for meetings by telephone or videoconference.

The CSSF will also continue to cooperate closely and exchange information with other national authorities in order to maintain and further strengthen Luxembourg's national AML/CFT regime. The CSSF is in constant and close contact with the CRF, Commissariat aux Assurances (CAA) and relevant government Ministries and will continue to take steps to combat new and emerging ML/TF risks as identified in this guidance.

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Claude WAMPACH Director	Marco ZWICK Director	Jean-Pierre FABER Director
Françoise KAUTHEN Director	Claude MARX Director General	

[40] CSSF, Circular letter, Re: 2019 Survey related to the fight against money laundering and terrorist financing, 2020. Available here.
[41] CSSF, Circular letter, Re: 2019 Survey related to the fight against money laundering and terrorist financing: extended deadline, 2020. Available here.