CLIFFORD

CHANCE

CORONAVIRUS: FINANCIAL CRIME AND AML/CTF IMPLICATIONS

On 10 April 2020, the CSSF issued a new Circular 20/740 to provide guidance in relation to the money laundering and terrorism financing (ML/TF) risks and AML/CTF implications of the Covid-19 pandemic. The CSSF notes that despite the economic downturn, illicit financial flows will continue and criminals and terrorists may seek to exploit temporary weakness in AML/CTF controls. The supervised professionals are therefore required to put in place and maintain effective systems and controls to ensure that Luxembourg's financial system is not abused for ML/TF purposes. The new circular provides guidance in this context for the CSSF-supervised professionals on new and emerging ML/TF threats, possible areas of particular vulnerability, the mitigating actions as well as the AML/CTF supervision during this period.

Key aspects

- New ML/TF threats are emerging as a consequence of the Covid-19 pandemic.
- The CSSF identifies certain sectors which may be of particular vulnerability during the current crisis.
- The circular describes areas requiring particular focus in order to adapt the changing nature of ML/TF threats.
- The CSSF remains fully operational and its on-site AML/CTF inspections and off-site supervisory activities continue to be performed.

This briefing speaks as of 12 April 2020.

NEW AND EMERGING THREATS

The CSSF identified two categories of ML/TF threats which are emerging as a consequence of the Covid-19 pandemic: (i) crimes that represent both a significant operational risk for financial institutions and a ML/FT threat, and (ii) crimes where the risk to financial institutions is primarily related to the laundering of illicit proceeds.

Crimes representing significant operational risk and a ML/TF threat

- **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 (in particular, social engineering attacks and online activity linked to child abuse have increased). For financial institutions, the operational risks related to cybercrimes are significant and have been amplified by the changes to work practices. The CSSF has identified six amplifiers that make financial institutions and their employees particularly exposed to cybercrimes (such as, for example, alternative/remote modes of working and utilisation of different technologies).
- **Fraud**. The CSSF notes rapid growth in the number of frauds related to Covid-19 across Europe and the adaptation of well-known fraud schemes to target individuals, citizens, businesses and public organisations during

the pandemic (e.g. Covid-19 used as a pretext to divert payments). For financial institutions, the operational and business risks related to such frauds are significant (e.g. liability for fraud losses and reimbursement, higher operational costs to work on fraud cases and increased negative experience for customers).

Crimes where risks primarily relate to the laundering of illicit proceeds

- **Bribery and corruption related to government support schemes**. The exceptional circumstances, unprecedent size and urgency of various stimulus packages adopted by governments in the context of Covid-19 (e.g. direct grants, tax advantages, state guarantees for loans) create opportunity for abuse and therefore pose a material ML/TF threat for financial institutions. Such threat may also materialise with the increasing risk of bribery of customs or other officials in the context of closure of airports, ports and other facilities for international trade.
- **Trafficking in counterfeit medicines and other goods**. Distribution of counterfeit and/or sub-standard goods (e.g. pharmaceutical products, fake Covid-19 home tests) has been identified as the key area of criminal activity in relation to the current pandemic. The possible laundering of proceeds from such crimes creates a material ML/TF threat for supervised professionals.
- **Robbery and theft**. The pandemic also created new opportunities for organised crime groups involved in thefts, burglaries, robberies and other scams (e.g. burglaries of commercial premises and medical facilities). The laundering of proceeds from such activities creates a ML/TF threat for supervised professionals as they can be used to inject, layer or integrate the proceeds of these primary offences.
- **Insider trading and market manipulation**. The threat of market abuse is also likely to have grown during this period, given *inter alia* a higher number of employees and other persons having access to insider information (e.g. due to the transmission of information via unusual channels) and the complexity of the impact assessment of Covid-19 on issuers' activities leading also to delays in publication of financial information. Furthermore, 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 and the financial institutions may be misused by criminals to commit such crimes and/or laundering the proceeds thereof.

EMERGING VULNERABILITIES

Although the CSSF encourages all professionals to remain vigilant considering that any area of the Luxembourg financial sector could be exploited by the emerging threats, it stresses that the following vulnerabilities may be particularly relevant in this context:

- **Online payment services**. The surge in online purchase is likely to increase both the volume and the value of online payments services, including the use of internet banking which may create more opportunity for criminals to conceal illicit funds within a greater amount of legitimate payments made online.
- **Clients in financial distress**. The economic impact of Covid-19 could place some clients of supervised professionals in distress (e.g. commercial

borrowers), creating opportunities from criminals to exploit them in order to lauder illicit proceeds.

- **Mortgages and other forms of collateralised lending**. Given the economic impact of Covid-19 on their clients, credit institutions may re-value existing collateral and request additional collateral to be placed against current or new loan. Relaxation of controls on the origin and source of funds and wealth to obtain such collateral could facilitate the entry of illicit proceeds into the financial system.
- **Credit backed by government guarantees**. There is a potential that such new schemes (e.g. repayable advances and guarantees in loans by banks) could be misused by criminals (e.g. fraudulently obtaining funds without intention or repaying them and misusing the scheme to launder money).
- **Distressed investment products**. Many stock markets and investments products have experienced significant declines in value and investors may be looking to offload and minimise losses thus providing opportunity for criminals offering to purchase or refinance the distress assets using the illicit funds.
- **Delivery of aid through non-profit organisations (NPOs)**. 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 risk of TF. Tax advantages afforded by charitable donations could also be misused by those seeking to launder illicit funds.

MITIGATION OF EMERGING RISKS

The 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 purpose. The CSSF stresses that the following areas require particular focus in order to adapt the changing nature of ML/TF threats:

- **AML/CTF business continuity and governance**. All professionals should ensure that sufficient focus is given to operating AML/CTF controls in compliance with the 2004 AML/CTF Law (e.g. AML/CTF controls should remain fully operational and effective while staff works remotely, adequate communication and information exchange between colleagues continues, appropriate attention is given to checking key decisions, including those related to controls over third party AML/CTF outsourcing) and to confirm the robustness of their cyber risk controls in line with the CSSF Communiqué of 3 March 2020 and the FAQ on Covid-19.
- **Transaction monitoring**. Professionals should (i) continue to monitor transactions and pay particular attention to any unusual or suspicious patterns in customers' behaviour and financial flows (in particular with respect to sectors impacted by Covid-19, such as for example cash intensive business in the retail sector, companies involved in international trade and companies facing an economic downturn but keeping similar volume of financial flows in the absence of real economic activities), (ii) be aware that there may be a large increase in false positives from transaction monitoring and fraud prevention systems that use machine learning technique (systems may fail to capture new threats and Compliance should review critically the rules and thresholds in place), and (ii) confirm the adequacy of third party outsourcing related to transaction monitoring and other key AML/CTF processes.

- **Customer due diligence (CDD)**. Professionals should (i) continue to apply the CDD measures required under the 2004 AML/CTF Law and to consider how these can be strengthened to mitigate the impact of a lack of face-to-face contact with customers, and (ii) consider using financial technology to manage some of the CDD issues presented by Covid-19 (in particular consider the digital ID systems) in compliance with the requirements introduced by the law of 25 March 2020. The CSSF further reminds 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 business relations and cooperate with the authorities.
- **ML/TF risk assessment**. Professionals should take dynamic approach to ML/TF risk assessment and incorporate risk associated with Covid-19 as part of these activities.
- **Cooperation with authorities**. Professionals should continue to cooperate closely with competent authorities, in particular to report suspicions of ML/TF to the CRF without delay (including in relation to the new or emerging risks) and continue to interact with the CSSF as part of its supervisory activity.

AML/CTF SUPERVISION DURING COVID-19

In summary the CSSF stresses that:

- it 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;
- it has re-focused its interventions in order to maintain those which are currently key to preserving financial stability and protecting investors and consumers;
- it remains fully operational and implemented several measures to ensure it meets the operational challenges associated with AML/CTF supervision during this time (in particular an internal coordination committee has been created to manage the response to the Covid-19 pandemic);
- it will continue AML/CTF supervisory activities during this period, AML/CTF on-site inspections already started will be completed, new inspections will start on a remote basis during this period and off-site supervisory activities also continue; and
- it will continue to cooperate closely and exchange information with other authorities in order to maintain and further strengthen Luxembourg's national AML/CTF regime.

CLIFFORD
CHANCE

CONTACTS

Steve Jacoby
Partner

T +352 48 50 50 219
E steve.jacoby
@cliffordchance.com

Christian Kremer
Partner

T +352 48 50 50 201
E christian.kremer
@cliffordchance.com

Marc Mehlen
Partner

T +352 48 50 50 305
E marc.mehlen
@cliffordchance.com

Udo Prinz
Counsel

T +352 48 50 50 232
E udo.prinz
@cliffordchance.com

Boika Deleva
Associate

T +352 48 50 50 260
E boika.deleva
@cliffordchance.com

Ewa Baginska
Associate

T +352 48 50 50 490
E ewa.baginska
@cliffordchance.com

Yolanda-Alma Ghita-Blujdescu
Associate

T +352 48 50 50 489
E yolanda.ghita-blujdescu
@cliffordchance.com

Emmanuel-Frédéric Henrion
Partner

T +352 661485190
E emmanuelfrederic.henrion
@cliffordchance.com

Kristof Meynaerts
Partner

T +352 48 50 50 226
E kristof.meynaerts
@cliffordchance.com

Paul Van den Abeele
Partner

T +352 48 50 50 478
E paul.vandenabeele
@cliffordchance.com

Oliver Zwick
Senior Associate

T +352 48 50 50 476
E oliver.zwick
@cliffordchance.com