MONEY LAUNDERING & TERRORIST FINANCING RISKS AND PRACTICES DURING COVID-19

GUIDANCE FOR FINANCIAL INSTITUTIONS

MAY 2020

I. PURPOSE, SCOPE, AND APPLICABILITY

- This guidance paper produced by the Central Bank of Bahrain ("CBB") should be read in conjunction with local and international standards relevant to prevention of money laundering and terrorist financing. The paper is applicable to all licensees regulated and supervised by the CBB.

- This guidance paper is based on the ***COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses*** published by the Financial Action Task Force ("FATF") in May 2020, as part of a coordinated and timely response to the impact of the COVID-19 crisis on global anti-money laundering ("AML") and counter terrorist financing ("CFT") efforts, and the application of the FATF Standards in this context.

- This guidance paper provides a summary of the challenges, good practices and policy responses to new money laundering and terrorist financing threats and vulnerabilities arising from the COVID-19 crisis. Additionally, all financial institutions are urged to read the FATF guidance paper [1]comprehensively.

[1] https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf

II. INTRODUCTION

The COVID-19 pandemic has generated various government responses, ranging from social assistance and tax relief initiatives, to enforced confinement measures and travel restrictions. While unintended, these measures may provide new opportunities for criminals and terrorists to generate and launder illicit proceeds.

At a global level, criminals are taking advantage of the COVID-19 pandemic to carry out financial fraud and exploitation scams, including advertising and trafficking in counterfeit medicines, offering fraudulent investment opportunities, and engaging in phishing schemes that prey on virus-related fears. Malicious or fraudulent cybercrimes, fundraising for fake charities, and various medical scams targeting innocent victims are likely to increase, with criminals attempting to profit from the pandemic by exploiting people in urgent need of care and the goodwill of the general public and spreading misinformation about COVID-19. National authorities and international bodies are alerting citizens and businesses of these scams, which include impostor, investment and product scams, as well as insider trading in relation to COVID-19. Like criminals, terrorists may also exploit these opportunities to raise funds.

Criminals and terrorists may seek to circumvent national AML/CFT systems and controls while they assume resources are focused elsewhere. Financial institutions ("FIs") and other businesses should remain vigilant to emerging Money Laundering ("ML") and Terrorist Financing ("TF") risks and ensure that they continue to mitigate these risks effectively and are able to detect and report suspicious activity, as the mitigation of financial crime risk and effective control measures remains a vital priority for the CBB and the Kingdom of Bahrain ("Bahrain").

III. THREATS AND VULNERABILITIES

- **Threats**: The United Nations has warned that threats related to terrorism remain and that terrorist groups may see opportunities for increased terrorist and terrorist financing activity while globally governments' attention is focused on COVID-19. As international humanitarian and aid responses to COVID-19 increase, there is a risk of funds being diverted to support terrorists and terrorist groups. In addition, the FATF paper states that reporting from FATF members, observers, and open sources indicates that new threats have evidently stemmed from COVID-19-related crime and impacts on ML/TF risks internationally. Such threats include the following:

  - ***Fraudulent Activities:*** Criminals have attempted to profit from the COVID-19 pandemic through increased fraudulent activities. The primary fraudulent activities include, but are not limited to, impersonation of officials, counterfeiting (including essential goods such as medical supplies and medicines), fundraising for fake charities, and fraudulent investment scams.

  - ***Cyber Crimes:*** There has been a sharp rise in social engineering attacks, specifically phishing emails and mobile messages through spam campaigns. These attacks use links to fraudulent websites or malicious attachments to obtain personal payment information. Reports also indicate that cybercriminals are using different methods to insert ransomware on personal computers and mobile devices. For example, some cybercriminals are using malicious websites and mobile applications that appear to share COVID-19- related information to gain and lock access to victims' devices until payment is received.

  - ***Impact on Other Predicate Crimes:*** Criminals may take advantage of the pandemic to exploit vulnerable groups through means such as human trafficking, exploitation of workers, and online child exploitation.

- **Vulnerabilities**: With the ever-increasing risks associated with COVID-19, other contextual factors and ML vulnerabilities are becoming exceedingly evident globally. The FATF paper also indicate that such vulnerabilities include, but are not limited to, the following:

  - ***Changing Financial Behaviors:*** Reporting indicates significant changes in financial behaviors and patterns in light of COVID-19. Many bank offices and branches are closed due to public health and "lockdown" measures. Customers are therefore carrying out more transactions remotely. This has potentially led to increased online banking activities, including customer onboarding and identity verification. In addition, certain population segments (e.g. the elderly and low-income groups) may be less familiar with using online banking platforms, and therefore more susceptible to fraud.

- ***Misdirection of Government Funds or International Financial Assistance and Increased Risks of Corruption:*** Many governments are providing stimulus funds to mitigate the economic impact related to COVID-19. Reports entail that criminals may try to fraudulently claim or misdirect such funds. Methods in which criminals may achieve this include exploiting stimulus measures and misappropriating international financial assistance, thus increasing the risk of corruption.

- ***Increased Financial Volatility:*** Recent financial and economic volatility reflects uncertainties associated with COVID-19. In this context, opportunistic criminals may shift their activities to exploit new vulnerabilities by taking advantage of the economic downturn, large value shifts in securities markets, and utilizing virtual assets. In addition, financial service providers in the securities market are transferring or liquidating assets in response to COVID-19- related uncertainties. These large value shifts in markets can potentially increase the risk of illicit financial market activities, such as insider trading that seeks to profit from large value swings.

IV. EMERGING ML/TF RISKS

- FIs must be familiar with the methods in which criminals and terrorists are exploiting the pandemic and how their AML/CFT compliance processes might need to be altered in order to manage the elevated risk. The potential ML/TF risks emerging from the aforementioned threats and vulnerabilities could include:

  - Criminals finding ways to bypass CDD measures by exploiting temporary challenges in internal controls caused by remote working situations, in order to conceal and launder funds;

  - Increased misuse of online financial services and virtual assets to move and conceal illicit funds;

  - Misuse of financial aid and insolvency schemes as a means for natural and legal persons to conceal and launder illicit proceeds;

  - As individuals move money out of the banking system due to financial instability, this may lead to an increased use of the unregulated financial sector, creating additional opportunities for criminals to launder illicit funds;

  - Misuse and misappropriation of domestic and international financial aid and emergency funding by avoiding standard procurement procedures, resulting in increased corruption and consequent ML risks; and

  - Criminals and terrorists exploiting COVID-19 and the associated economic downturn to move into new cash-intensive and high-liquidity lines of business in developing countries, both for the laundering of proceeds and to fund their operations, as well as fraudulently claiming to be charities to raise funds online.

V. POTENTIAL AML/CFT RESPONSES

- In line with Bahrain's efforts to vigilantly combat COVID-19, the CBB aims to work alongside FIs to mitigate risks arisen from the pandemic, whilst simultaneously ensuring that criminals and terrorists do not misuse the financial sector for the purpose of ML/TF. As many AML/CFT private sector employees are now working remotely, FIs are required to adapt their AML/CFT processes to stay in line with the requirements stipulated in the Financial Crime ("FC") Module of the CBB Rulebook during such a time. Potential responses to COVID-19 applicable by licensees are as follows:

  - **Risk-Based Approach:** Licensees are reminded of the importance of continuing to provide essential financial services while also mitigating ML/TF risks by using the full range of tools at their disposal. FIs are encouraged to develop a comprehensive risk assessment to assess the ML/TF risks associated with COVID-19. The risk assessment must be based on relevant factors, commensurate with the nature, type, complexity and size of the licensee's business. Consequently, the assessment must identify sufficient control measures to be implemented, proportionate to the identified risks in order to mitigate them effectively and efficiently.

  - **Transaction Monitoring:** Due to the unconventional circumstances brought about by COVID-19, licensees might observe a sudden change in its customers' pattern of activity such as abnormal or unusual flows of funds. This signifies an AML/CFT compliance challenge as it makes it more difficult for compliance teams to differentiate between legitimate and potentially illegitimate activities. Increased ongoing account monitoring is essential in ensuring that customer transactions and patterns of activity are reviewed to detect suspicious activity. Moreover, it is also prudent to reassess the transaction monitoring rules and alert indicators to ascertain these programs are capable of capturing emerging typologies. Moreover, FIs should be aware of higher-risk transactions, such as activity that has no apparent lawful purpose, funds transfers to and from higher-risk jurisdictions, and currency-intensive transactions. It is vital that FIs utilize opportunities to update information on customers in order to maintain a high standard of monitoring.

  - **Suspicious Transaction Reporting ("STRs"):** In the case where an alert was triggered by the monitoring system, or a staff member suspects that a customer is engaged in ML/TF, or if the transaction or the customer's conduct otherwise appears unusual or suspicious, licensees are reminded of their obligation to investigate the transaction/activity and file a suspicious transaction report immediately in accordance with the requirements stipulated in the FC Module. It is imperative to exercise vigilance in the current environment in order to respond to the changed risk environment for criminal activity.

- **Digital Onboarding (non face-to-face):** In the case where conducting face-to-face customer onboarding becomes exceedingly challenging, licensees may implement digital onboarding subject to CBB approval. However, such a request must be subsequent to a thorough risk assessment, and confirming that all the requirements commensurate to the FC Module are comprehensively met (including methods in which the licensee aims to identify and verify the customer). Digital onboarding processes must be embedded with technical controls to verify the customer and the identity documentation. Biometric authentication must be implemented alongside with liveness checks, facial recognition, and three-dimensional face matching techniques.

- **Awareness:** FIs are encouraged to engage with their customers in order to raise awareness on the emerging fraudulent activities and cybercrimes, such as phishing emails and mobile messages through spam campaigns, initiated by criminals disguising as the licensee. In addition, licensees must ensure that their staff members are made adequately aware of the rising COVID-19 ML/TF risks, in order to effectively identify and avoid the possible misuse of licensees for such purposes.

VI. CONCLUSION

It remains important to continue to put in place and maintain effective systems and controls to ensure that the Kingdom's financial system is not abused for money laundering or terrorist financing purposes. Licensees are strictly reminded that financial crime remains unacceptable, even in times of crisis such as the COVID-19 outbreak. Licensees must ensure ongoing compliance with their AML/CFT obligations as set forth in the FC Module of the CBB Rulebook.