AML/CFT Regulatory Response to the COVID-19 Pandemic

The Central Bank of Barbados ("CBB"), Financial Services Commission ("FSC"), Ministry of International Business & Industry - International Business Unit ("IBU"), Corporate Affairs and Intellectual Property Office ("CAIPO") and the Financial Intelligence Unit ("FIU"), (collectively referred to as "the Competent Authorities") recognise the challenges faced by financial institutions as they address issues that arise as a result of the COVID-19 Pandemic. We are cognisant of the importance of continuing to provide essential financial services while operating under restricted conditions, and to ensure adherence to the established protocols. These include observing any established curfews, social distancing or self-isolation which has resulted in staff and key officers working from home and limited face-to-face contact with customers.

The following represents some of the key elements from the Financial Action Task Force ("FATF") paper "*Covid-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses, May 2020*".

INCREASED MONEY LAUNDERING/TERRORIST FINANCING (ML/TF) RISK

Internationally, the national responses to COVID-19 emergency has led, unintentionally, to new opportunities for criminals and terrorists to generate and launder illicit proceeds heightening ML/TF risks. As such, the FATF has identified the following emerging issues.

These include: Increased Fraud, Cyber Crime, Impact on Other Predicate Crime, Changing Financial Behaviours, Misdirection of Government Funds or International Financial Assistance and Increased Risks of Corruption, Increased Financial Volatility, Change in Criminal Environment and Terrorist Financing.

Potential ML/TF risks emerging from threats and vulnerabilities were identified as:

- Increased misuse of online financial services and/or virtual assets to move and conceal illicit funds;
- Exploitation of temporary changes to internal controls caused by remote working situations to bypass customer due diligence measures;
- Misuse of natural and legal persons to obtain and subsequently launder stimulus funds, taking advantage of legitimate businesses, or to hide funds via insolvency schemes; and

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

AML/CFT CONTROLS AND RESPONSES

Financial Institutions and Designated Non-Financial Business Entities and Professionals ("collectively referred to as "Entities") are reminded of the requirement to comply with the Money Laundering and Financing of Terrorism (Prevention and Control) Act ("MLFTA"), as amended, and the relevant AML/CFT Guidelines ("Guidelines").

VERIFICATION OF CUSTOMER IDENTITY

Having regard to the foregoing, the Competent Authorities encourage the use of responsible electronic and digital customer on-boarding measures, while ensuring that risk-based controls are in place to mitigate ML/TF risk. It is expected that the verification of original documents will be completed as soon as practicable after COVID-19 restrictions are lifted. It is also important for reporting entities to remain alert and vigilant to new and emerging ML/TF risks at this time.

The Competent Authorities recognise the challenges in which COVID-19 may make it difficult for entities to verify the identity of individuals using their normal processes (for example by acquiring certified copies of original documents). However, during this period, entities are expected to continue to comply with their obligations with regards to customer identity verification. It is essential to confirm that customers are who they claim to be and that the information or documentation aligns with the customer's risk profile.

The Competent Authorities' Guidelines provide for elements of customer identity verification to be carried out remotely, provided that certain appropriate safeguards are in place. Documents in electronic form are acceptable provided that entities take a risk-based approach and have suitable documented policies and procedures in place to ensure the authenticity of the electronic document(s). Entities should assess the type of electronic file and ensure that it is authentic .

There are a number of ways to verify information (both at the time of establishing the relationship or as a part of ongoing customer due diligence) whilst observing curfew, social distancing or self-isolation.

These measures include the following and are not exhaustive:

- Meeting customers through telephone or secured video conferencing (where this option is used it must be documented for each case) to ask questions about their identification, their reason for requesting the financial service or other questions to ascertain whether customers are who they claim to be and the nature and purpose of the business relationship;
- If an introducer or suitable certifier has met the customer, they must confirm to the financial institution that they have met the customer via video conferencing, including a photograph or scanned copy of the documents;
- Certification of documents through "selfie" documents, photographs or videos: Photographs should clearly show the person's face and the image on the identity document being held in the same picture to demonstrate this actually belongs to the customer. A clear scanned copy or photograph of the document itself should also be provided.
- Interviewing customers through secured videoconference to compare the physical likeness of a customer with scanned or photographed copies of identification documents;
- Statements and bills received in an e-format. Where statements or bills have been provided to the customer in an e-format, these are acceptable provided that they clearly show the customer's residential address (not just an email address). These documents should then be verified via one of the methods outlined above.
- Government issued identification received in e-format. Entities may accept recently expired government-issued identification, , in order to verify the identity[1] of an individual until relevant services resume. However, the entity is still required to determine the authenticity of the identification via one of the methods outlined above.
- Requiring that the first deposit to the account, be made by electronic transfer from the customer's account at their existing bank for source of funds verification.

Entities should consider whether an electronic signature is legally acceptable, including by the counterparty, and consider virtual arrangements for witnessing such signatures where relevant.

[1] Note that the first directive came into effect from March 28, 2020 (Refer to the Emergency Management (Covid-19) Curfew Directive, 2020).

Where an entity has adopted a different verification method as indicated above, it should be documented in all cases and the verification completed using normal processes as soon as practicable.

The Competent Authorities expect entities to take a risk-based approach when establishing new relationships and impose restrictions where the associated ML/TF risks may be higher. For example, imposing transaction limitations, i.e., number of transfers or withdrawals until verification is completed using normal practices.

ONGOING DUE DILIGENCE

In respect of ongoing due diligence, based on the current circumstances, there may be legitimate reasons for customers not providing updated information. As such, the usual processes for dealing with these situations, including exiting the customer relationship, may not be appropriate at this time[2].

Entities may consider applying simplified or reduced due diligence measures where lower risks are identified, including to facilitate relief programmes and to facilitate contactless payment solutions. Where this approach is taken, entities should ensure that enough information is provided to support effective customer monitoring.

Consideration can also be given to a tiered CDD approach by entities, which may include customers having access to different account functionalities depending on the extent of the identification/verification being conducted, with strict pre-set thresholds defined for various account levels. In addition, entities may allow limited account services (e.g. caps on daily/monthly withdrawals, deposit limits) based on the level of CDD conducted and the customer risk profile.

Entities should ensure that there are processes and controls to detect and review changes in the risk profile of the customer. Where there are changes, appropriate due diligence measures should be applied.

NON-PROFIT ORGANISATIONS ("NPOs")

During this time, NPOs will be engaged in charitable services to ensure social relief is provided for those in need and affected by COVID-19. Financial institutions are reminded that not all NPOs are high risk and some carry little to no risk for terrorist financing. The intent is that NPOs utilize legitimate

[2] See measures that can be implemented set out in the 2017 FATF Guidance on AML/CFT Measures and Financial Inclusion, with a Supplement on Customer Due Diligence.

and transparent channels and that their services benefit those in need. Therefore, a risk-based approach should continue to be applied to ensure that financial transactions conducted with NPOs are for legitimate activities and therefore continued vigilance is required. At the same time, however, financial institutions should also ensure that such transactions are not unnecessarily delayed, disrupted or discouraged. Financial institutions should also be vigilant to criminals who may seek to profit from the Government's COVID-19 relief programmes by setting up companies or NPOs to receive social assistance funds, or by taking advantage of legitimate businesses to obtain and subsequently launder economic stimulus funds.

REPORTING OBLIGATIONS

Entities should continue to effectively manage ML/TF risks, taking into account emerging risks presented by the COVID-19 pandemic. The obligations to report suspicious activities and transactions are laid out Section 23 of the MLFTA and corresponding sections of the Guidelines. Entities should report suspicious activities and comply with United Nations sanctions obligations as required. Reports are to be filed with the Financial Intelligence Unit ("FIU") promptly from the date the transaction or circumstances was deemed suspicious.

Given the health risks posed by the transmission of COVID-19, the submission of suspicious transaction/activity reports (STRs) **via email is encouraged**. In the event, that a regulated entity is unable to submit a STR via email, the Report can be delivered directly to the FIU where on arrival, the relevant delivery protocols will be communicated.

ONGOING MONITORING

Entities should consider the impact of the changing financial environment which may trigger an update to customer risk profiles. Consequently, entities are reminded to continue monitoring transactions and pay particular attention to unusual or suspicious patterns in customer behaviour and financial flows, identifying risk indicators and implementing processes and controls to prevent the misuse of their institutions.

TRAINING AND AWARENESS

Entities should continue to provide training to staff especially during this period and in light of any emerging ML/TF risk. Training should be facilitated online or virtually, as far as possible, however should it become necessary for face-to-face training, entities should observe the established COVID-19 safety protocols.

The Competent Authorities will continue to engage entities from time to time on the application of AML/CFT measures and related matters emanating from the impact of COVID-19 on their operations and, where necessary, provide guidance. However, entities are encouraged to:

- Advise the Competent Authorities where the COVID-19 restrictions prohibit the implementation of the MLFTA or Guidelines
- Inform the Competent Authorities of any evolving ML/FT risks or threats as a result of COVID-19 adjustments

CONTACT US

Queries should be sent to:

- Central Bank of Barbados - supervision@centralbank.org.bb
- Financial Services Commission – CBenskin-Murray@fsc.gov.bb
- International Business Unit – compliance.mibi@barbados.gov.bb
- Corporate Affairs and Intellectual Property Office – caipo.general@barbados.gov.bb
- Financial Intelligence Unit - adminfiu@barbados.gov.bb