JOINT REGULATORY GUIDANCE ON COMPLYING WITH AML/CFT VERIFICATION REQUIREMENTS

IN LIGHT OF COVID-19 MEASURES

CENTRAL BANK OF TRINIDAD & TOBAGO

'2020

CENTRAL BANK OF TRINIDAD & TOBAGO

JOINT REGULATORY GUIDANCE ON COMPLYING WITH AML/CFT VERIFICATION REQUIREMENTS IN LIGHT OF COVID-19 MEASURES

Trinidad and Tobago and the world in general, has faced an unprecedented set of circumstances linked to the coronavirus (COVID-19) pandemic, particularly during this period of social distancing, self-isolation and other disruptions to everyday business. We recognise that this may pose challenges to traditional mechanisms for compliance with customer due diligence obligations and in particular, obligations for the verification of identity under the anti-money laundering and counter-terrorism financing and proliferation financing (hereinafter "AML") regime. The Central Bank of Trinidad and Tobago ("Central Bank"), the Trinidad and Tobago Securities and Exchange Commission ("TTSEC") and the Financial Intelligence Unit of Trinidad and Tobago ("FIU") (collectively referred to as "the Authorities") are committed to working constructively with you throughout this disruptive period. During the COVID-19 social distancing restrictions, it is anticipated that financial institutions and listed businesses ("reporting entities") may still need to establish new business relationships or conduct occasional activities or transactions for new customers. However, we expect that the volume of new business relationships established during this period will be lower than normal.

We emphasize the importance of continuing to provide essential financial services by using the flexibility built into the risk-based approach for AML compliance, to address the challenges posed by the COVID-19 social distancing restrictions. During this period, we expect reporting entities to continue to comply with the customer due diligence and verification of identity requirements as outlined in the Financial Obligations Regulations (2010) (as amended), and in particular Regulations 11, 12, 15, 16, 24 and 25. Please note that Regulation 15(5) also allows for appropriate measures to be implemented to address the risks of non-face-to-face interactions and transactions. Further, reporting entities are reminded that Regulations 14(2) and 14(5) allow for flexibility in instances of lower risk and for the application of simplified due diligence measures. Additionally, Part II – Section 6.3.1 of the **Central Bank's AML/CFT Guideline** ("Central Bank's Guideline") provides guidance on the application of simplified due diligence measures, including adjusting the timing of verification in certain circumstances. See also guidelines 53-58 of the TTSEC's AML/CFT Guidelines for the Securities Sector ("TTSEC's Guidelines").

Ultimately, reporting entities should continue to gather sufficient information to form a general understanding of the customer's identity so that it remains possible to assess the money laundering, terrorism and proliferation financing ("ML/TF/PF") risks.

Having regard to the foregoing, we 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/PF risk. We expect 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 to new and emerging ML/TF/PF risks at this time.

JOINT REGULATORY GUIDANCE ON COMPLYING WITH AML/CFT VERIFICATION REQUIREMENTS IN LIGHT OF COVID-19 MEASURES

The Authorities recognise that reporting entities may need to temporarily amend their AML compliance programmes to implement alternative processes to verify customers' identity, but face challenges in making formal amendments during this period. In these circumstances, we expect that reporting entities will keep a record of approved changes in policies and procedures made due to the COVID-19 pandemic.

ON-BOARDING NEW CUSTOMERS

The following are some considerations for the acceptance of electronic or digital identification where a person's identity cannot immediately be verified face-to-face during the COVID-19 period. These measures are not exhaustive and are not intended to be used as a checklist. Reporting entities are urged to consider the ML/TF/PF risks on a case-by-case basis:

1. Applying simplified due diligence measures where lower risks are identified, for example, where accounts are created specifically to facilitate government payments for economic relief to individuals or businesses.

2. Delaying physical verification of documents where non face-to-face business relationships are established and imposing limitations or restrictions on account usage until identity can be verified with original documents. For example, impose restrictions on wire transfers, loan facilities, or by implementing transaction limits. Reporting entities may accept digital copies of documents as an interim measure, until the original documents can be physically verified when it is practical to do so before the relaxation of restrictions.

3. Accepting scanned documentation sent by e-mail, preferably as a PDF. Consider requiring that these scanned copies be accompanied by some form of declaration, for example, "I certify that this document is a true copy of the original" and for identification documents a declaration stating: "I certify that the photograph is a true likeness of my facial features".

4. Accepting recently expired government-issued identification to verify the identity of individuals. Please note that the Miscellaneous Provisions [2019 Novel Coronavirus (2019-nCoV)] Act, 2020 allow for the continuation of the validity of driving permits, taxi driver licences, badges, certificates or other documents issued by the Licensing Authority, where those documents expire during the period March 27, 2020 to July 31, 2020 until 31st August, 2020 or for a longer period as necessary. Notwithstanding, reporting entities are still required to take reasonable measures to determine the authenticity of all government-issued identification documents.

EXAMPLES OF INTERIM VERIFICATION CHECKS

After customers have provided digital copies of identification documents, additional verification measures may include:

a. using secure video-calling services to compare the physical likeness of a customer with scanned or photographed copies of identification documents;

b. requiring the customer to provide a clear, front-view photo of themselves or 'selfie' that can be compared with the scanned or photographed copies of identification documents;

c. interviewing the customer via video or telephone calls to ask questions about their identification, their reason for requesting the financial service or other questions to ascertain whether the customer is who they claim to be and the nature and purpose of the business relationship;

d. conducting an independent search of the Companies Registry to validate documentation submitted by companies or utilizing the Ministry of Works and Transport's Driver's Permit Verification System to verify driver's permits;

e. seeking third party verification of identity to corroborate information provided by the customer or by placing reliance on the due diligence carried out by others, such as intermediaries or the customer's primary bank account provider, where appropriate agreements are in place to provide access to such information;

f. where possible, gathering and analyzing additional data to verify the evidence provided by the customer, such as geolocations and IP addresses or by verifying phone numbers, or by sending codes to the customer to validate access to accounts;

g. requiring that the first deposit to the account (if opened), be made by electronic transfer from the customer's account at their existing bank for source of funds verification.

Reporting entities are reminded of their reporting obligations to identify and report designated persons under the Anti-Terrorism Act, Chap. 12:07 ("ATA") and the Economic Sanctions Orders, 2018. Additionally, where there is doubt about the authenticity of identification documents, the transaction should not be completed and a suspicious activity report must be filed with the FIU. Account agreements should include clauses that provide for the contract to be nullified if documentation proves to be incorrect/falsified/misrepresented. Physical verification of the original identification documents must be done as soon as practicable when it is safe to do so.

ONGOING DUE DILIGENCE

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

For customers to whom simplified due diligence measures were applied during this time, reporting entities must ensure that there are processes and controls to detect and review changes in the risk profile of the customer and to apply the appropriate due diligence measures, in such instances.

REMAINING VIGILANT TO NEW AND EMERGING ML/TF/PF RISKS

As most economies are facing a downturn, financial flows are likely to diminish. However, experience from past crises suggests that in many cases, illicit finance will continue to flow. As criminals are highly adaptive, new techniques and channels of laundering money are likely to emerge. For example, there are international reports of increased levels of cyber-crime; COVID-19-related frauds and medical scams targeting vulnerable people and companies; fraudulent fundraising campaigns; criminals exploiting vulnerabilities due to remote working arrangements, to bypass customer due diligence controls; fraudulent investment opportunities; phishing schemes that prey on COVID-19 related fears; insider trading; and criminal networks selling rationed goods at a higher price. The FIU has also published a Scam Alert for the attention of reporting entities.

During this time, Non-Profit Organisations ("NPOs") will be engaged in charitable services to ensure social relief is provided for those in need and affected by COVID-19. Reporting entities are reminded that not all NPOs are high risk and some carry little to no risk for terrorist financing. [See Part II Section 7.3 of the Central Bank's Guideline and guidelines 45-52 of the TTSEC's Guideline] The intent is that NPOs utilize legitimate and transparent channels and that their services benefit those in need. Therefore, a risk based approach must be applied to ensure that financial transactions conducted with NPOs, are for legitimate activities and such transactions are not unnecessarily delayed, disrupted or discouraged. Reporting entities should also be alert 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 entities should take risk-sensitive measures to establish the legitimate origin of unexpected financial flows, where these financial 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 customers include cash-intensive businesses in the retail and service

sectors, and any companies in sectors affected by the economic downturn which continue to maintain pre-COVID-19 financial flows, notwithstanding restrictions on non-essential services and economic activity.

REPORTING OBLIGATIONS

Reporting entities are therefore encouraged to remain vigilant during this time, as criminals will attempt to profit from the COVID-19 pandemic by exploiting persons in urgent need of care and the goodwill of the general public. Reporting entities are reminded to continue monitoring transactions and pay particular attention to unusual or suspicious patterns in customers' behaviour and financial flows, identifying risk indicators and implementing processes and controls to prevent the misuse of the aforementioned assistance packages for ML/TF/PF purposes.

Reporting entities are also reminded of their obligations to report suspicious activities and transactions in accordance with Section 55A (1) of the Proceeds of Crime Act, Chap.11:27, Section 22C (3) of the ATA and Regulation 9 (2) of the Economic Sanction Orders, 2018. Reports are to be filed with the FIU immediately or within fourteen (14) days from the date the transaction was deemed suspicious.

In closing, the Authorities continue to work closely with each other and our international regulatory partners throughout this period, to ensure the stability of the financial sector and the continued protection of consumers.

We will continue to monitor and keep these measures under review especially as new issues arise and we look forward to our continued partnership with reporting entities and industry associations, as we navigate the COVID-19 impact.

CONTACT US:
Should you have any queries in respect of this Guidance please contact:
Central Bank: aml@central-bank.org.tt
TTSEC: aml@ttsec.org.tt
FIU: fiucompliance@gov.tt

CENTRAL BANK OF
TRINIDAD & TOBAGO