21 April 2020

ADVISORY

RE: Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") Compliance During COVID-19

The Cayman Islands Monetary Authority ("the Authority" or "CIMA") recognises that this is a challenging time for our regulated entities. The coronavirus pandemic ("COVID-19") has led to operational resilience being tested, with staff working from home in shifting market conditions.

CIMA is committed to supporting regulated entities observing curfew, social distancing or self-isolation. This Advisory has been prepared by CIMA to help regulated entities maintain appropriate standards of AML/CFT systems and controls while adapting to new and changing circumstances.

This is not a legal document and should not be relied upon in respect of points of law. Reference for that purpose should be made to the appropriate statutory provisions.

The importance of AML/CFT systems and controls

The COVID-19 emergency has led to a heightened risk of money laundering ("ML"). The Financial Action Task Force ("FATF") has identified significant emerging risks. These include criminals advertising and trafficking in counterfeit medicines, offering fraudulent investment opportunities, engaging in phishing schemes that prey on virus-related fears, committing malicious or fraudulent cybercrimes, fundraising for fake charities, investment and product scams, and insider trading in relation to COVID-19. Like criminals, terrorists may also exploit these opportunities to raise funds.

Specific threats and vulnerabilities are:

- Increased use of online schemes and/or virtual assets as a layering method to launder proceeds;
- Exploitation of temporary changes to internal controls caused by remote working situations to bypass customer due diligence measures;
- Potential increases in transactions not in line with customers' profiles, increased use of the informal economy to provide financing as traditional gatekeepers are locked down, and increases in bulk-cash movements;
- Misuse of legal persons to obtain and subsequently launder stimulus funds fraudulently, taking advantage of legitimate businesses, or to hide funds via insolvency; and
- Criminals and terrorists using the economic impact of COVID-19 to move into new cash-intensive and high-liquidity lines of business, including for the laundering of proceeds. For instance, real estate or troubled businesses, which can be used to generate cash and mask illicit proceeds.

Verification of Customer Identity

CIMA recognises that COVID-19 may make it difficult for regulated entities to verify the identity of individuals using their normal processes (for example by acquiring certified copies of original documents). However, during this period, CIMA expects regulated entities to continue to comply

with their obligations with regards to customer identity verification. It is essential to confirm that the customer is who they claim to be and that the information or documents fit in with the customer's risk profile.

CIMA's Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands ("Guidance Notes") 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 the regulated entity takes a risk-based approach and has suitable documented policies and procedures in place to ensure the authenticity of the electronic document(s). Regulated entities should check the type of electronic file and ensure that it is tamper resistant.

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

These include:

- Meeting customers through video conferencing (where this option is used it must be documented for each case). If an introducer or suitable certifier has met the customer, they must confirm to the regulated entity 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.
- Statements and bills received in an e-format. Where statements of bills have been provided to the customer in an e-format they 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. Regulated entities can accept recently expired government-issued identification, i.e., after March 1st, 2020, in order to verify the identity of an individual. However, the regulated entity is still required to determine the authenticity of the identification via one of the methods outlined above.

Where a regulated entity has adopted a deviated verification method as indicated above, it should complete the verification using normal processes as soon as practicable.

CIMA expects regulated 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., limited transfers or withdrawals until verifications are completed using normal practices.

The Cayman Islands Registrar of Companies has also confirmed that it will accept affidavits or other documents that have been notarised/certified online or utilising audio-video technology.

Risk Assessments

Regulated entities should remain vigilant and ensure that Institutional Risk Assessments are updated to reflect heightened ML/TF risks due to COVID-19. Ongoing monitoring should be used to assess the transaction profiles of customers. Regulated entities should consider whether to recalibrate transactional monitoring software to reflect emerging risks. Unusual transactions may be a result of ML or TF, but they could also be COVID-19 related.

Updated policies, procedures and documentation

It is important that regulated entities document the steps that they are taking to mitigate the ML/TF/PF/Sanction risks as a result of the COVID-19 crisis including the risk assessments. Where a regulated entity is deviating from their normal compliance practices and procedures, it should document the reasons for such variations and the evidence of returning to the normal compliance practices after the conclusion of this crisis.

Training

CIMA strongly encourages regulated entities to provide AML/CFT/CPF/Sanctions related training to their staff via online platform such as webinars and other online learning modules. In cases where face to face AML/CFT/CPF/Sanctions training to staff was postponed/cancelled due to COVID-19, CIMA would expect to see the documentation that the regulated entity had organised or booked courses.

Signatures

CIMA expects regulated entities to consider whether an electronic signature is acceptable legally and by the counterparty and consider virtual arrangements for witnessing such signatures where relevant.

Supervision and inspections

CIMA will continue its AML/CFT activities during this period on a risk-based approach. New AML/CFT inspections are commencing on a remote basis and off-site supervisory activities will continue. Regulated entities should continue to interact with CIMA. Delays and extensions to deadlines, including for submitting documents, will be considered on a case by case basis.

Reporting

Regulated entities must continue to effectively manage ML/TF risks, taking into account emerging risks presented by the COVID-19 pandemic. Regulated entities must report suspicious activities and comply with Sanctions obligations as required by the relevant laws.

Further guidance

To understand the emerging ML/TF risks, regulated entities should refer to the guidance or position papers issued on the COVID-19 by international standard setting bodies such as the FATF.

To understand the requirements of customer verification, regulated entities should refer to CIMA's Guidance Notes.

For digital record keeping, regulated entities may refer to the Statement of Guidance on the 'Nature, accessibility and retention of records' issued by the Authority.

Regulated entities are urged to seek CIMA's assistance where required. All queries should be forwarded to ContactAMLCFT@cima.ky.

- END -