Cayman Attorneys Regulation Authority

27 April 2020

ADVISORY NOTICE

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

The Cayman Attorneys Regulation Authority ("CARA") knows that the Coronavirus Pandemic ("COVID-19") is an incredibly worrying and stressful time for everyone. We understand that many law firms and attorneys-at-law face uncertainty and difficult business conditions with operational resilience being tested, with staff working remotely in shifting market conditions at home and abroad.

CARA is committed to supporting regulated firms and sole practitioners observing curfew, social distancing or self-isolation.

CARA has seen the advisory note prepared by the Cayman Islands Monetary Authority ("CIMA") dated 21 April 2020 and concurs with that advice.

This Advisory Notice has been prepared by CARA to help regulated firms maintain appropriate standards of Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation financing (collectively referred to as "AML") 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. CARA provides this document as part of its outreach and guidance role.

The importance of AML/CFT/CPF systems and controls

The COVID-19 emergency has led to a heightened risk of money laundering, including terrorist and proliferation financing. Legal practices and practitioners should be aware that criminals will continue to operate throughout this time and look to take advantage of the pandemic.

The Financial Action Task Force ("FATF"), the global money laundering and terrorist financing watchdog, 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:

- 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;

- 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; and

- Increased use of online schemes and/or virtual assets as a layering method to launder proceeds.

As the AML supervisor for firms of attorneys-at-law conducting relevant financial business, we understand the particular challenges currently facing legal practices and practitioners. This includes the difficulties associated with undertaking customer due diligence ("CDD"), including appropriate levels of identification and verification, especially where clients cannot be met face-to-face.

Please note that firms of attorneys-at-law are still required to comply with their statutory requirements at all times in relation to the Anti-Money Laundering Regulations, The Proceeds of Crime Law, The Terrorism Law (2018), The Proliferation Financing (Prohibition) Law (2017 Revision) and relevant Targeted Financial Sanctions applicable in the Cayman Islands.

CARA is not able to waive or otherwise relax any of these requirements. However, in line with a risk-based approach, the Anti-Money Laundering Regulations ("AMLRs") provide flexibility in the application of their requirements. There exist options for practices seeking to comply while also observing requirements such as curfews imposed in the Islands and social-distancing.

Verification of Customer Identity

Verifying the identity of a client is often undertaken in person, on the premises of the legal practice or their delegate or relied upon service provider, using suitable identification documents. This can provide a strong level of assurance as to the proper identity of the client, but under the current COVID-19 measures in the Cayman Islands, this is no longer possible in the current circumstances. Firms of attorneys-at-law should consider what risks this may create.

CARA recognises that COVID-19 may make it difficult for regulated firms to verify the identity of individuals using their normal processes (for example by acquiring certified copies of original documents). However, during this period, CARA 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. The inability to conduct in-person verification does not mean that CDD cannot be completed; it means that alternative methods must be used that provide the necessary assurance that the person is indeed who they say they are.

Our guidance notes regarding assessing the Money Laundering & Terrorist Financing risks for lawyers may be of assistance.

CARA reminds firms of attorneys-at-law that they should be adopting a risk-based approach, taking into consideration their practice-wide risk assessment, policies and procedures (where necessary updating them) and the circumstances of individual clients/matters.

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. Such methods may include (but are not limited to) using the following independently or in combination:

- '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.

- Digital Identity and Verification Services that meet the requirements under the AMLRs. Such services must be capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact the person with that identity whilst being secure from fraud and misuse.

- Gathering and analysing additional data to triangulate the evidence provided by the client, such as geo-location, IP addresses, verifiable telephone numbers.

- Certification of documents through "selfie" documents, photographs and/or videos (live or recorded): 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.

If a deviated verification method is used, the responsibility to make sure the verification of identity is undertaken correctly remains with the relevant practitioner and practice. If you are relying on persons outside the firm to conduct CDD, you should ensure that you understand how they have adapted their CDD procedures to the current circumstances. Such decisions should be fully documented.

Further, 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. A full record and evidence of the deviated processes should be kept, e.g. the use of video calls or 'selfie' verification, why certain methods were chosen and why you were satisfied that identity had been verified.

If a digital identification verification service is used, you must consider whether it provides the assurance needed. In order to make this judgement, you may have regard to the Financial Action Task Force (FATF) guidance on Digital Identity, particularly;

- You must understand what the service actually does and any limits on the service provided.

- You must take a risk-based approach to relying on the service including understanding the assurance level provided and that it is appropriate to the risk in each matter it is to be used.

- You must use anti-fraud and other cyber security processes to support the service.

- Consider whether the service has attained any accreditation or certification from any of the bodies listed by FATF in Appendix D of the Digital Identity Guidance.

CARA expects regulated entities to take a risk-based approach when establishing new relationships and impose restrictions where the associated Money Laundering, Terrorist Financing or Proliferation Financing may be higher – for example, imposing transaction limitations until verifications are completed using normal practices. The above methods alone may not be appropriate or sufficient for high risk matters or clients. In such situations, further verification (including source of wealth or funds) will likely be required.

There is a potential that affidavits or other documents can be notarised/certified online or utilising audio-video technology. These should be used with caution and consideration should be had to the points raised above regarding verification of identity.

Firms should ensure that staff working from home have access to the necessary CDD documentation to be able to properly consider the risks of any client or matter.

If a firm is using digital or video photography to support CDD or obtaining other personal information, thought should be had to obtaining consent from the data subject for the capture and storage of this information, with due regard to data protection requirements.

If personal or sensitive information is requested by email or other electronic means in support of CDD, due consideration should be made to the associated information security risks. Firms should consider and record the necessary steps to mitigate such risks, for example encryption or password-protection.

Risk Assessments

Regulated entities should remain vigilant and ensure that business Risk Assessments are updated to reflect heightened Money Laundering, Terrorist Financing or Proliferation Financing risks due to COVID-19. Ongoing monitoring should be used to assess the transaction profiles of customers. Unusual transactions may be a result of Money Laundering, Terrorist Financing or Proliferation Financing, but they could also be COVID-19 related.

As well as changes to how we live our lives, COVID-19 is also changing the economy globally. An economic downturn may make legal practices more susceptible to financial difficulties or other pressures, which creates risk and potential weaknesses for criminals to exploit. As we all continue during this period of uncertainty, practitioners and practices should be particularly alert to the following risks in new or prospective customers:

- Being asked to work with unusual types of client or on unusual types of matter.
- Resistance from a client regarding compliance with due diligence checks, for example, clients pressuring attorneys to forego necessary due diligence checks or to ‘speed up’ the process.
- Being ask to, and becoming involved in, work that is outside of the practice or practitioner’s normal area of experience and/or expertise, without full understanding of the money laundering, terrorist financing and proliferation financing risks associated with the new area of work.

- Any attempt to gain access to your client account where not accompanied by the provision of legal services.
- Transactions where the business rationale for the transaction is not clear.

Supervised Firms should always ensure that they are comfortable as to their understanding of the matter, including its purpose and why it is happening in the particular way it is happening.

CARA expects Supervised Firms to consider whether their risk-assessments need to be updated in respect of COVID-19. Supervised Firms may find it useful to consult our guidance regarding AML Risk Assessments for Attorneys when updating their risk-assessments in consideration of the COVID-19 pandemic.

Updated policies, procedures and documentation

It is important that regulated entities document the steps that they are taking to mitigate the Money Laundering, Terrorist Financing, Proliferation Financing or Sanctions 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 evidence the returning to the normal compliance practices after the conclusion of this crisis.

CARA expects Supervised Firms to consider whether their policies, controls and procedures remain appropriate and whether they need adjustment to reflect what the firm is doing. If processes change then the firm should consider updating relevant policies.

Training

CARA strongly encourages regulated entities to provide Money Laundering, Terrorist Financing, Proliferation Financing and Sanctions related training to their staff via online platform such as webinars and other online learning modules. This can also be done in-house by meeting platforms such as Zoom or Microsoft Teams.

In cases where face to face Money Laundering, Terrorist Financing, Proliferation Financing and/or Sanctions training to staff was postponed or cancelled due to COVID-19, CARA would expect to see the documentation evidencing that the regulated entity had organised or booked courses and if appropriate, reasons why such training could not be provided using technology during lockdown.

Signatures

CARA expects Supervised Firms 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

CARA will continue its activities during this period, on a risk-based approach.

Our 'onsite' inspections are continuing on a remote basis, using phone and video conferencing as appropriate. Desk-based supervisory activities continue. Regulated entities should continue to interact with CARA. 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 Money Laundering, Terrorist Financing, Proliferation Financing and Sanctions risks, taking into account emerging risks presented by the COVID-19 pandemic. Regulated entities **must** still report suspicious activities to the FRA and comply with Sanctions obligations as required by the relevant laws.

Further guidance

Supervised Firms are urged to visit the Guidance Section on our website for further information regarding their obligations.

It is not for CARA to provide specific legal advice and/or confirmation on the application of the AMLRs. You are required to satisfy yourself on your legal/regulatory obligations under the AMLRs and that you have complied with them.

If you have questions about whether a specific identification method is allowable or any other aspect of the above, you should contact us. If necessary, you should obtain independent legal advice from an experienced and more specialist legal practitioner.

Our staff are still working full time, although our physical office is closed. If assistance is required, Supervised Firms are urged to seek CARA's assistance where required. All queries should be forwarded to info@cara.ky and our staff will get back to you as soon as practicable.

CARA will take a proportionate approach to difficulties as a result of COVID-19: this includes our approach to enforcement. If we identify breaches of the AMLRs that have taken place during this uncertain time, we will consider any mitigating circumstances, as outlined in our Enforcement Policy. This means that we will focus on serious misconduct, with a clear distinction between people who are trying to do the right thing, and those who are not. Again, our advice to firms is that they should fully document any problems.

Whilst care has been taken to ensure this Advisory Note is accurate, up-to-date and useful, CARA repeats that this is not a legal document and the Authority will not accept any legal liability in relation to this note. We will continue to work with our supervised population to raise AML standards through this challenging time.