MAPLES GROUP

UPDATE

Revised AML Guidance Notes on e-KYC and Remote CDD / Ongoing Monitoring

On 30 August 2023, revised Guidance Notes on the Prevention and Detection of Money Laundering ("ML"), Terrorist Financing ("TF"), and Proliferation Financing in the Cayman Islands (August 2023) (the "Revised GNs") were published in the Cayman Islands Gazette.

The Revised GNs have been consolidated with Guidance Notes (Amendment) (No. 1) – Virtual Asset Service Providers (February 2021) and Guidance Notes (Amendment) (No. 2) – Securitisation (May 2021).

Importantly, the Revised GNs incorporate changes to facilitate the use of e-KYC and Remote Customer Due Diligence ("CDD") / Ongoing Monitoring. The amendments support FATF-issued guidance on digital identification and provide for remote onboarding of clients and the use of e-KYC and digital ID technologies on an ongoing basis, where appropriate based on the risk assessment of clients.

These measures were the subject of a Cayman Island Monetary Authority ("CIMA") Private Sector Consultation Paper in December 2022 and build on an earlier advisory issued by CIMA in 2020 during COVID-19 that suggested regulated entities could utilise virtual means of verification of client identity to satisfy CDD requirements.

On 11 August 2023, CIMA also issued a Summary of Private Sector Consultation and Feedback Statement with respect to the foregoing (the "Consultation Feedback") which includes some useful discussion.

Changes of General Application

As part of the update to the Revised GNs, CIMA made two small but potentially important changes of general application:

1) For verification of corporate legal entities, the Revised GNs now include the following:

"…*When verifying customers that are corporate legal persons, regulated entities may use publicly available sources, including company registries*."

2) More broadly, and with the relevant new wording in emphasis:

"CDD documents, ***including government issued identification, received*** *in electronic form are acceptable provided that the FSP takes a RBA [risk-based approach] and has suitable documented policies and procedures in place to ensure the authenticity of the electronic document(s)."*

Both items suggest that obtaining certified copies may be of diminished relevance provided that information received can be (in the case of the former) corroborated against public sources and (in the case of the latter) relied upon as not being fakes.

We discuss this further in the context of e-KYC.

Very broadly, regulated entities will need to both (i) holistically assess the use of new digital ID system / technology solutions for CDD purposes and (ii) with respect to each given customer, consider the suitability of such solutions whether for purposes of onboarding, remediation, or ongoing monitoring.

Use of Technology for CDD Purposes by Regulated Entities

According to the Revised GNs, Cayman Islands regulated entities should have robust documented policies and procedures in place to ensure a consistent and adequate approach to relying on new digital ID system / technology solutions for CDD purposes. These may include (but are not limited to):

(a) A tiered CDD approach that leverages the new technology solutions with various assurance levels;
(b) Policies for the secure electronic collection and retention of records by the new technology solutions;
(c) A process for enabling authorities to obtain from the new technology solutions the underlying identity information and evidence needed for identification and verification of individuals;
(d) Anti-fraud and cybersecurity processes to support e-KYC / digital ID proofing and / or authentication for AML / CFT efforts resulting from the new technology solutions;
(e) Back-up plans for possible instances where the new technology solution fails;
(f) A description of risk indicators that would prompt a financial service provider ("FSP") to refrain from utilising new digital ID system / technology solutions; and
(g) Procedures for the regular, ongoing and independent review of the new systems and processes effectiveness.

Risk Assessments

Regulated entities will need to carry out a formal risk assessment of e-KYC / digital ID technologies. The risk assessment should include documented consideration of how the proposed system works, the level of assurance that it provides, and any particular risks associated with it such as the accuracy of the underlying information and / or technology, appropriateness of the application for the relevant client base, timeliness of the applications' updates, i.e. sanctions lists, evaluation of the resilience and cyber security measures of the application, storage of personal information, etc.

The Revised GNs provide that customer identification and verification procedures that rely on reliable independent e-KYC / digital ID systems with appropriate risk mitigation measures in place, which meet ISO / IEC technical global standards for digital ID systems may present a standard level of risk, and may even be lower-risk where higher assurance levels are implemented and / or appropriate ML / TF risk control measures, such as product functionality limits, are present.

Video Conferencing and Selfies

The Revised GNs provide that *"video-conferencing …is not considered face-to-face"*.

The relevance of this is that by not being a 'face-to-face' meeting, additional checks are required.

In relation to verification of natural persons through 'selfie' documents, photographs or videos, the Revised GNs provide:

"Photographs should be in colour and clearly show the person's face, holding the identity document in the same photograph to demonstrate it actually belongs to the customer. A clear scanned copy in colour or photograph of the identity document itself should also be provided."

For corporate legal persons or legal arrangements (trusts, foundations), video-conferencing may be used to *"identify natural persons such as directors and officers, ultimate beneficial owners, settlors or grantors, trustees, protectors, enforcers or those appointed to act on behalf of the customer"*.

To corroborate constitutional documents, regulated entities should seek to verify constitutional documents presented during a video conference against public sources, in accordance with the general guidance.

Importantly, there is also a requirement that accessible records be maintained. On this the Consultation Feedback provides that:

"The FATF Guidance states that regulated entities should ensure that they have access to, or have a process for enabling authorities to obtain, the underlying identity information and evidence or digital information needed for identification and verification of individuals. It does not prescribe how this should be done. Digital records specifying the types of identity evidence used for specific evidence, including data source, date / time and means of accessing it may support this requirement."

For further guidance, FSPs may refer to the Statement of Guidance on Nature, Accessibility and Retention of Records issued by CIMA, where applicable.

Further Assistance

If you need additional advice relating to your ongoing regulatory compliance obligations, please contact us. We would be delighted to assist.

Cayman Islands

Chris Capewell
+1 345 814 5666
chris.capewell@maples.com

Patrick Head
+1 345 814 5377
patrick.head@maples.com

Tim Dawson
+1 345 814 5525
tim.dawson@maples.com

Martin Livingston
+64 21 321 353
martin.livingston@maples.com

Jo Ottaway
+1 345 814 5511
jo.ottaway@maples.com

September 2023