Cayman Islands: Updated AML Guidance on use of e-KYC, Digital ID, and remote onboarding and ongoing monitoring of business relationships

October 2023

In recent years, especially during the COVID-19 pandemic, onboarding clients and monitoring business relationships on remote basis have become the dominant trend.

In light of such trend, the Cayman Islands Monetary Authority ("**CIMA**") has timely amended the Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands (the "**Amended GN**") in August this year, which essentially codifies how Financial Service Providers ("**FSPs**") can use e-KYC and/or digital identification ("**ID**") systems to conduct remote onboarding and ongoing monitoring of business relationships. The Amended GN is also in line with the concepts in the previously-issued FATF guidance on how entities can use digital ID systems to conduct customer due diligence ("**CDD**").

In this Briefing, we provide a brief overview of the principal concepts and requirements for remote onboarding and ongoing monitoring of business relationships according to the Amended GN.

What is e-KYC?

- E-KYC refers to the process whereby a client's identity is verified via electronic means.

What is a digital ID system?

- A digital ID system refers to a system that covers the process of identity proofing/enrolment and authentication. Identity proofing and enrolment can be either digital or physical (documentary), or a combination, but binding, credentialing, authentication, and portability/federation must be digital.

Application of risk-based approach on remote onboarding and ongoing monitoring processes

- In general, FSPs are required to apply a risk-based approach ("**RBA**") on remote onboarding and ongoing monitoring of business relationships in order to assess money-laundering/terrorist financing ("**ML/TF**") risks.

- The decision to onboard a customer remotely, using e-KYC methods and/or digital ID technologies, will depend on the risks presented and assessed. Where applicable, FSPs are required to consider the application of tiered CDD.

- Where an FSP identifies a higher risk of ML/TF, additional verification measures are require to be adopted to ensure the accuracy of e-KYC procedures.

Application of risk-based approach on the digital ID / e-KYC systems

- In general, FSPs must consider the basic components of the technology solutions including digital ID/e-KYC systems and take an informed RBA when relying on these systems.

- In this regard, the Amended GN introduced a concept of “assurance level”, which measures the level of confidence and accuracy in the reliability and independence of a digital ID system and its components.

- When applying the RBA, FSPs are required to understand the chosen system’s assurance level and ensure that such level aligns with the assessed level of ML/TF risks of the relevant case. For instance, if it is determined that simplified due diligence is sufficient in cases of low ML/TF risk, FSPs may consider utilising digital ID systems/e-KYC processes with lower levels of assurance.

- For e-KYC/digital ID systems with appropriate risk mitigation measures in place that meet ISO/IEC technical global standards for digital ID systems, they may present a standard level of risk, and may even be of a lower risk where higher assurance levels are and/or appropriate ML/TF risk control measures are present.

- Additionally, before adopting a new digital ID/e-KYC system, an FSP should carry out formal risk assessments on such system, which include documented consideration of:

  (a) how the proposed system works;
  (b) the level of assurance that it provides; and
  (c) any particular risks associated with it, *inter alia*, accuracy of the underlying information and/or technology, appropriateness of the application for the licensee's client base (i.e. some applications are aligned to verify identification within a specific region), 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.

Customer due diligence

- For the purpose of CDD, FSPs should put in place robust documented policies and procedures on new digital ID system/technology solutions, which 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 an FSP to refrain from utilising new digital ID system/technology solutions; and
  (g) procedures for the regular, ongoing and independent review of the effectiveness of the new systems and processes used.

- It is worth noting that when verifying customers that are corporate legal persons, FSPs are allowed to use publicly available sources, including company registries.

- Government-issued identification in electronic form is also an acceptable CDD document, provided that the FSP takes a RBA and has suitable documented policies and procedures to ensure the authenticity of such electronic document(s).

Video-conferencing as a method of e-KYC

- Video-conferencing is considered to be an e-KYC mechanism, so additional checks have to be conducted in the same way as other non-face-to-face measures.

- FSPs shall implement appropriate controls during the video-conferencing process to verify the identity and authenticity of the ID documents presented.

- If an eligible introducer or suitable certifier has met the client, they must confirm to the FSP that they have met the client via video-conferencing, including a photograph of the client or scanned copy of the certified documents.

- When onboarding clients who are corporate legal persons or legal arrangements (trusts, foundations), video-conferencing may be used to identify natural persons relevant to such persons or arrangements, such as their directors and officers, ultimate beneficial owners, settlors or grantors, trustees, protectors, enforcers or those appointed to act on behalf of the client.

"Selfies"

- "Selfie" photographs may be used as a documentation for evidence of identity, provided that such photographs are in colour and clearly show the person's face, with that person holding the identity document in the same photograph to demonstrate it actually belongs to that person. A clear scanned copy in colour or photograph of the identity document shall also be provided.

Conclusion

The amendments in the Amended GN are much welcomed because it has the potential to significantly reduce uncertainties surrounding the use of e-KYC processes / digital ID systems when onboarding clients and monitoring business relationships. The changes also show CIMA's willingness to keep up with FATF's guidance and recommendations.

The ability to (i) verify clients/customers that are corporate legal persons, by using publicly available sources, including company registries, and (ii) use Government-issued identification in electronic form as acceptable CDD document (provided the FSP takes a RBA and has suitable documented policies and procedures to ensure the authenticity of such electronic document(s)) should facilitate client onboarding and assist with existing challenges in some jurisdictions in finding public notaries or appropriate certifiers of documents.

Further Assistance

This publication is not intended to be a substitute for specific legal advice or a legal opinion. If you require further advice relating to the matters discussed in this Briefing, please contact us. We would be delighted to assist.

E: gary.smith@loebsmith.com
E: robert.farrell@loebsmith.com
E. elizabeth.kenny@loebsmith.com
E: cesare.bandini@loebsmith.com
E: wendy.au@loebsmith.com
E: vivian.huang@loebsmith.com
E: faye.huang@loebsmith.com

About Loeb Smith Attorneys

Loeb Smith is an offshore corporate law firm, with offices in the British Virgin Islands, the Cayman Islands, and Hong Kong, whose Attorneys have an outstanding record of advising on the Cayman Islands' law aspects and BVI law aspects of international corporate, investment, and finance transactions. Our team delivers high quality Partner-led professional legal services at competitive rates and has an excellent track record of advising investment fund managers, in-house counsels, financial institutions, onshore counsels, banks, companies, and private clients to find successful outcomes and solutions to their day-to-day issues and complex, strategic matters.

- **Investment Funds**
- **Banking & Finance**
- **Insolvency/Restructuring**
- **Mergers & Acquisitions**
- **Capital Markets**
- **Corporate**
- **Private Equity**
- **Corporate & Liquidation**
- **Commercial Litigation**