THE ANCHOR

UNDERSTANDING ML/TF/PF RISKS AROUND VIRTUAL ASSET SERVICE PROVIDERS

CIMA recently conducted a Sectoral Risk Assessment of VASPs (the 'VASP SRA') to consider the inherent ML/TF risks that VASPs face and to help allocate its resources effectively and efficiently. The VASP SRA will also further inform policy making and supervision in the area of AML/CFT/CPF.

Risk factors in the following categories are considered for purposes of this ML/TF risk assessment:

- Nature size and complexity of the sector, including geographic factors:
- Types of customers;
- Transactions, products and services; and
- Delivery channels.

WHAT'S INSIDE

For each of the listed risk categories, risk increasing and decreasing factors were considered and to help guide the assessment of inherent ML/TF risks. The table below summarizes the ratings assigned on each risk factor in each category assessed.

Category	Risk Rating
Nature and Size	Medium-High
Customers	Medium-High
Transactions, products and service	**High**
Delivery	Medium-High
Overall	Medium-High

A detailed version of the VASP SRA will be incorporated into the wider Cayman Islands' 2021 National Risk Assessment, due for publication late summer. CIMA recognizes that VASPs evolve at a rapid pace and AML/CFT/CPF risk must be re-assessed on an ongoing basis. As VASPs are only just entering the regulatory sphere, with applications for registration with CIMA still in process, understanding of the sector will develop significantly as CIMA registers more VASPs and collects more data.

In the meantime, VASPs are reminded that pursuant to the Anti-Money Laundering Regulations, they are required to take steps to identify, assess, and understand their ML/TF risks in relation to customers, geographic areas, products, services and transactions, and delivery channels; and to align all aspects of their internal controls and procedures with their risk understanding, including customer due diligence procedures, transaction monitoring systems, and the independent audit function.

CIMA's progress against FATF follow up actions

In February 2021, the FATF determined that the Cayman Islands had made sufficient progress on 60 of the 63 Recommended Actions outlined in the 2017 Mutual Evaluation Report. Of the remaining 3, FATF determined that progress had been partly made, but that follow up actions ("FUAs") would be required in relation to sanctions, enforcement and prosecutions.

In keeping with its high level political commitment to satisfy the remaining FUAs, the Cayman Islands chose to proactively engage with the FATF through regular reporting. This resulted in CIMA being able to demonstrate tangible progress with the FUA "CIMA should apply sanctions that are effective, proportionate and dissuasive, and take administrative penalties and enforcement actions to ensure that breaches are remediated effectively and in a timely manner."

FATF subsequently issued an updated Public Statement following the June Plenary meeting acknowledging the progress of the jurisdiction as follows:

"Since February 2021, when the Cayman Islands made a high-level political commitment to work with the FATF and CFATF to strengthen the effectiveness of its AML/CFT regime, the Cayman Islands has taken steps towards improving its AML/CFT regime, including by applying sanctions that are effective, proportionate and dissuasive, and taking administrative penalties and enforcement actions against obliged entities to ensure that AML/CFT breaches are remediated.

The Cayman Islands should continue to work on implementing its action plan to address its strategic deficiencies, including by: (1) imposing adequate and effective sanctions in cases where relevant parties (including legal persons) do not file accurate, adequate and up-to-date beneficial wnership information in line with those requirements; and (2) demonstrating that they are prosecuting all types of money laundering in line with the jurisdiction's risk profile and that such prosecutions are resulting in the application of dissuasive, effective, and proportionate sanctions."

The last FUA is not due until May 2022, and so the most likely scenario is that the Cayman Islands will not be removed from the 'grey list' until the FATF plenary in October 2022. CIMA remains totally committed to strengthening the AML/CFT supervisory regime and will continue its active industry engagement and collaboration with domestic agencies to foster AML/CFT compliance.

Digital Identity and the use of E-KYC

The Authority has observed that its regulated entities are increasingly interested in the use of e-KYC (i.e. the electronic means to conduct customer identification and/or allow online and/or digital verification of the customer's identity).

The Covid-19 pandemic made identifying and verifying customers' identities through face-to-face interactions significantly more difficult. As a result, the Authority has seen an uptick in the use of automated systems to verify, validate, and authenticate CDD information, which is intended to replace the need for, inter alia, physical certification of documents.

THE LEGAL FRAMEWORK

So what is permitted in the Cayman Islands?

The Financial Action Task Force's Recommendation 10 and the Anti-Money Laundering Regulations, 2020 (as amended) ("AMLRs") require financial service providers ("FSPs") and trust and company service providers ("TCSPs") to undertake customer due diligence ("CDD") measures when, inter alia, establishing business relationships and carrying out transactions. Financial institutions should determine the extent of such measures using a risk-based approach ("RBA").

The legislation does not prescribe the method in which the CDD obligations are to be performed but requires that it be reliable and independent. Regulation 12(1)(a) of the AMLRs states that, *"A person carrying out relevant financial business shall identify a customer, whether a customer in an established business relationship or a one-off transaction, and whether natural, legal person or legal arrangement and shall verify the customer's identity using reliable, independent source documents, data or information"*.

Traditionally, this process has required the customer to visit the relevant regulated entity and submit physical paper-based evidence of their identity. The regulated entity has then performed a manual verification of this information

In Spring 2020, the Authority recognized that the COVID-19 pandemic was obstructing its regulated entities from verifying the identity of individuals using their normal processes. On April 21, 2020, the Authority issued an Advisory to help maintain appropriate standards of anti-money laundering, combatting the financing of terrorism, proliferation financing and targeted financial sanctions ("AML/CFT/CPF and Sanctions") systems and controls while adapting to new and changing circumstances.

While digital verification methods were permitted, such as videoconferencing or IDs in e-format, regulated entities were still required to determine the authenticity of the identification, and to complete the verification using normal processes as soon as it was possible to do so.

THE MOVE TOWARDS E-KYC

The Authority has been reviewing, on a case-by-case basis, the proposed use of e-KYC technology by regulated entities in order to obtain, at a minimum, an understanding of the proposed system, the intended verification and authentication process, as well as record retention, cyber security and data protection considerations.

Examples of e-KYC systems include: digital identification tools to assess whether the document submitted is authentic and current; systems to certify a document as a true copy; technology to verify the information against government databases; and packages to outsource electronic documentation verification to third parties.

Where regulated entities choose to adopt digital technology, the Authority expects these systems to ensure the accuracy of customer identification and verification, along with an ongoing assessment of the robustness of the technology application itself. Regardless of the approach used to obtain and maintain CDD information, the regulated entity must ensure that the customer's identity is verified using reliable, independent source documents, data or information, in line with the requirements of Regulation 12(1)(a) of the AMLRs.

Furthermore, in accordance with the Authority's Statement of Guidance on Nature, Accessibility and Retention of Records and the Rule and Statement of Guidance on Cybersecurity, regulated entities must maintain adequate procedures for the availability, maintenance, security, privacy and preservation of records, including those relating to customers, so that they are reasonably safeguarded against loss, unauthorized access, alteration or destruction. This includes records retained electronically or by any other medium. Cybersecurity requires regulated entities to establish, implement and maintain a documented cybersecurity framework that is designed to promptly identify, measure, assess, report, monitor and control or minimize cybersecurity risks as well as responding to and recovering from cybersecurity breaches that could have a material impact on their operations. The regulated entity must also consider data protection protocols to prevent the unlawful obtaining and disclosure of personal data pursuant to the applicable legislations.

THE E-FUTURE

The Authority is currently reviewing its Guidance Notes and other measures to assess whether further amendments are required. In the meantime, any regulated entity seeking to use (or enhance) its e-KYC is welcome to discuss this with the Authority.