CAREY OLSEN

BVI AML amendments to keep pace with developments in the digital world

Service area / Corporate
Location / British Virgin Islands
Date / August 2018

FinTech. ICOs. Blockchain.

It is increasingly rare for a dialogue within the financial services industry to take place without reference to one of these words (or similar, related concepts).

Acknowledging this sudden and continued growth in the use of innovative digital products across the globe, the British Virgin Islands (the "BVI") introduced amendments to the Anti Money Laundering and Terrorist Financing Code of Practice 2008 (the "**AML Code**") on 1 August 2018, which help to support the use of digital services for AML purposes in this new digital era. These amendments were, to a certain extent, to be expected, based on the jurisdiction's historic ability to provide innovative regulatory frameworks within which new financial services products can thrive, whilst adhering to its responsibility in the fight against money laundering, terrorist financing and proliferation financing.

The Anti-Money Laundering and Terrorist Financing (Amendment) (No. 2) Code (the "Code")

The Code applies to persons (the "**Entities**") licenced or registered to carry out any 'relevant business' (as such term is defined in the Anti-Money Laundering Regulations, 2008 and which includes, among other matters, banking business, insurance business and the business of company management), and also to non-financial businesses (designated as such in the Non-Financial Business (Designation) Notice, 2008).

Any Entity that falls within the ambit of the Code is now able to take advantage of the following three key changes to the BVIs AML regime.

Digital verification

The AML Code requires that any identifying information obtained by an Entity during the process of identification must be verified, by checking reliable, independent source documentation, data or information to confirm that the customer/applicant for business (the "Applicant") is who they say they are.

The Code now explicitly permits the use of electronic or digital means in order to carry out this verification exercise. Accordingly, in addition to the traditional methods of reliance on physical paper form information, the use of digital, electrical, magnetic, optical, electromagnetic, biometric and photonic methods may also now be used in order to conduct verification.

As with physical verification, it remains the responsibility of the Entity to adopt qualitative checks in order to properly assess the strength of the information sourced and received. Relevant factors to be considered will include:

- the security of the electronic/digital data or source;
- the method used in collecting, storing and maintaining the information;
- the level of privacy attached to the electronic/digital data source; and
- whether the electronic/digital data or source is reviewed and updated regularly.

Reliance on third party platforms

Under the Code, an Entity may now also engage, and rely on the data of, a third party (such as a Blockchain provider) to carry out the verification of an Applicant's identity, provided

that the Entity is satisfied that the information obtained and stored by that third party is sufficiently extensive, accurate and reliable.

The third party itself must:

- be independently established, operate independently and be independent of the Applicant;
- use and access a range of positive and negative information sources;
- access a wide range of alert data sources;
- have transparent processes that enable an Entity to know what checks have been carried out, what the results of those checks were and to determine the level of satisfaction provided by the checks; and
- not have been convicted of a criminal offence or sanctioned for a breach of data or providing misleading data.

An Entity relying on the electronic/digital and other data of a third party organisation must record its satisfaction that the above conditions are met. It must also engage in a cyclical monitoring process to keep track of any changes to the above conditions and to ensure the third party's continued compliance with these conditions.

Non face-to-face transactions

Due to the speed at which transactions take place, and the global reach of these transactions, in this new digital era, it is becoming increasingly common for transactions to take place, and for business relationships to be established, without any face-to-face contact. Recognising and facilitating this, the Code no longer requires that every Applicant is automatically treated as high risk due only to the fact that there has been no face-to-face contact.

Other factors may now also be taken into account, including the nature and characteristics of the product or service requested, the assessed money laundering or terrorist financing risk presented by the Applicant, and the likelihood as to whether face-to-face contact has been deliberately avoided by the Applicant.

Conclusion

Whilst further amendments to existing regulation in the BVI (including the AML Code), and the implementation of new laws and regulations, will be required in order to fully embrace and regulate the growth of FinTech, Blockchain and the ICO industry in the BVI, the changes brought about by the Code provide a helpful indication of the BVIs forward thinking and technologically supportive approach in developing its anti-money laundering policies.

FIND US

Carey Olsen
Rodus Building
PO Box 3093
Road Town
Tortola, VG1110
British Virgin Islands

T +1 284 394 4030
F +1 284 494 4155
E bvi@careyolsen.com

FOLLOW US

Visit our corporate team at careyolsen.com