FEBRUARY, 2020

Amendments to the Anti-Money Laundering Regulations

On 5th February 2020 the Anti-Money Laundering (Amendment) Regulations, 2020 were published.

The principal changes which will from 5 August 2020 have an effect on the operations of financial services providers are:

(1) the removal of the concept of the equivalent jurisdiction as a factor when determining whether simplified due diligence could be applied when verifying the identity of a customer and/or on the acceptance of certain types of payments. Going forward, each financial services provider, or third party service providers acting on their behalf, will need to make and document an assessment of a low level of risk in order for these concessions to be available;

(2) the development of the requirements for financial services providers to conduct risk assessments of a country or geographic area.

CIMA issues various amendments to the AML Guidance Notes

In response to the report of the Caribbean Financial Action Task Force mutual evaluation report, published in March 2019 and the follow-up review in 2020, the Cayman Islands Monetary Authority ("CIMA") has published a number of amendments to the Guidance Notes on the Prevention and Detection of Money Laundering and Terrorist Financing in the Cayman Islands (the "Guidance"). The amendments addressed the following areas:

1. Targeted Financial Sanctions;
2. Assessing Risks and Applying a Risk-Based Approach;
3. Ongoing Monitoring; and
4. Virtual Asset Service Providers

For further information on any of the issues discussed in this article please contact:

Matt Mulry
DD:+1 345 814 4054
matt.mulry@dilloneustace.ie

Jonathan Law
DD:+1 345 814 4057
jonathan.law@dilloneustace.ie

A summary of the amendments to the Guidance is set out below. The full text of the amendments is available in the CIMA website (www.cima.ky).

Targeted Financial Sanctions

The purpose of the amendments to the Guidance is to (1) add specific definitions and to include a general discussion of the concepts related to targeted financial sanctions; (2) highlight the relevant sanctioning bodies and applicable sanctions within the Cayman Islands; (3) identify the authorities responsible for the targeted financial sanctions regime in the Cayman Islands; (4) set out the responsibilities of financial service providers ("FSPs") in achieving compliance with the Guidance; (5) set out the obligations of FSPs to monitor the consolidated list maintained by the United Kingdom Office of Financial Sanctions Implementation ("OFSI") as well as domestic designations made by the Governor of the Cayman Islands; and (6) to set out the reporting obligations of FSPs to the competent authorities.

The amendments are extensive and address the general obligation of FSPs to develop a comprehensive programme (including staff training) to comply with the applicable measures and to monitor business relationships and assess one-off transactions for the purposes of allowing for the identification of assets subject to applicable targeted financial sanctions.

FSPs are required to regularly monitor the sanctions in place including local designations made by the Governor. FSPs should review their client lists against the lists of designated persons/entities and the consolidated list maintained by the OFSI. Further, FSPs must take steps to freeze funds or economic resources belonging to, owned, held or controlled by designated persons or entities and report to the Governor, through the Financial Reporting Authority ("FRA"), the details of any frozen funds or economic resources or actions taken in compliance with the prohibition requirements of the relevant UN Security Council measure, including attempted transactions. FSPs must report to the Governor, through the FRA, if they know or have reasonable cause to suspect that a person is a designated person or has committed a criminal offence.

FSPs must put in place procedures to screen new and existing customers, including where the information changes during the course of the business relationship and must ensure that payments are not indirectly made to or for the benefit of a designated person. FSPs are reminded of the legal obligation not to transfer or make funds or economic resources available directly or indirectly to a designated person or entity and the freezing of assets extends to all funds or assets that are owned, held or controlled by the designated person.

The amendments to the Guidance address the actions to be taken by FSPs where screening results in 'false positives' and the reporting obligations of FSPs in respect of search results, attempted transactions, incoming transfers of funds or assets and any other information which may suggest that freezing measures are being circumvented. The amendments to the Guidance also address the actions to be taken by FSPs in relation to the unfreezing of assets and the circumstances under which an exemption or licence to deal with the frozen funds or assets can be sought.

Assessing Risks and Applying a Risk-Based Approach

The purpose of the amendments to the Guidance is to enforce the message that FSPs are to apply a risk based approach to their anti-money laundering, terrorist financing and proliferation financing ("ML/TF/PF") controls and procedures. FSPs are to consider all relevant risk factors, determine a risk level and implement appropriate mitigation measures. FSPs are required to assess and understand their business risks, understand who their customers are, what they do, where they operate and the expected levels of activity. In conducting a risk assessment FSPs should look to all relevant resources such as the Cayman Islands National Risk Assessment, reports from the FRA and other law enforcement agencies, circulars from CIMA, industry and international associations and other credible sources. Risk assessments should be reviewed to ensure ongoing relevance.

When identifying risk, FSPs should adopt and document policies and procedures that are appropriate to their size, business and complexity. FSPs should identify risk with regards to their products, services, delivery channels, customers and geographic locations. A risk classification should be applied (high, medium or low) and appropriate mitigation measures applied. FSPs should determine the risk weight to be applied given the individual or a combination of risk factors. The risk assessment should be documented and kept up to date and be available to the relevant Supervisory Authority.

The amount of risk that an FSP is prepared to accept should be determined. This risk tolerance should be based upon legal, regulatory and reputational consequences of a compliance failure. In establishing the risk tolerance of an FSP, senior management should identify the risks that they are willing, and not willing, to accept and consider whether it has the capacity to manage the risks that are accepted. FSPs should implement appropriate risk mitigation policies and procedures that will allow them to effectively mitigate the identified risks. The nature of the policies will be determined by a number of factors including the size and complexity of the FSPs business, location of its operations, customer type and activity, volume and size of transactions.

FSPs should have systems in place to monitor their controls and also to identify new and emerging risks associated with new products, technologies or business activity.

Ongoing Monitoring

FSPs are required to understand the purpose and intended nature of the business which it has with a customer. Ongoing monitoring is considered essential for FSPs to maintain that understanding of the customer and business relationship. FSPs are required to conduct ongoing monitoring on the business relationship. Such monitoring includes ensuring that documents and information collected from the customer are up to date and the assigned level of risk remains accurate. Transactions should also be reviewed to ensure that they are consistent with the customer's profile, business and source of wealth. Such review of transactions should take place in respect of transactions initiated by the FSP or taking place through them.

FSPs should develop and implement policies and procedures relating to ongoing monitoring. Separate measures should be implemented for anti-money laundering, terrorist financing and proliferation financing. They should document measures for keeping collected documents and information up to date and particular attention should be paid to higher risk categories of customers and relationships. A periodic review should take place in line with a customer's assigned level of risk and the policies and procedures should outline the remedial actions required in the event of a trigger event arising. Such trigger events could include a material change to the ownership structure of a customer, the identification of a politically exposed person, adverse information from media or other sources or a request for new product service. FSPs must be able to identify all customer transactions and monitor these as a key part of identify any ML/TF/PF risks. The transaction monitoring procedures should be clearly documented, implemented by well trained staff and reviewed.

Unusual transaction should be detected by the monitoring process, if an alert is generated the FSP should establish a review process which may include gathering additional due diligence or making a suspicious activity report to the FRA.

FSPs should be able to demonstrate a periodic review of all customers with an appropriate degree of frequency given the level of risk assessment of respective customer profiles.

Virtual Asset Service Providers

The Proceeds of Crime Law ("PCL") defines "*virtual asset*" as "*a digital representation of value that can be digitally traded or transferred and be used for payment or investment purposes*". The PCL defines "*virtual asset service*" as "*the business of conducting one or more of the following activities or operations for or on behalf of a person – (a) exchanging between virtual assets and fiat currencies; (b) exchanging between one or more other forms of convertible virtual assets; (c) transferring virtual assets; (d) safekeeping or administering virtual assets or instruments enabling control over virtual assets; and (e) participating in and providing financial services related to an issuer's offer or sale of a virtual asset*".

The sector specific guidance issued by CIMA is intended to provide practical assistance to FSPs which are virtual asset service providers in complying with their ML/TF/PF obligations. Virtual assets as a result of their characteristics naturally have a high ML/TF/PF risk associated with them. FSPs engaging in virtual asset services are required to carry out a comprehensive and detailed risk assessment associated with the relevant technology, product or business practice associated with virtual assets. In carrying out such a risk assessments, FSPs are required to consider a range of unique factors related to virtual assets including those virtual assets that move value in and out of fiat currency; decentralized business models; the use of encryption technology which undermines the ability to identify beneficial owners; the use of online platform trading exchanges; and the nature and scope of the product, payment or delivery channel.

The sector specific guidance emphasizes that FSPs providing virtual asset services are required to fully comply with their obligations to collect, review and update due diligence information, conduct ongoing monitoring of customers and business relationships, and to maintain and update records. The FSPs obligations to comply with targeted financial sanctions and to ensure that internal and external reporting

procedures are in place are clearly set out. Guidance is provided on indicators of suspicious activity relating to both virtual assets and initial coin offerings and information which is required to be retained in relation to virtual asset transfers in or from within Cayman are also specified.
CIMA.

DILLON EUSTACE

Dublin
33 Sir John Rogerson's Quay, Dublin 2, Ireland. Tel: +353 1 667 0022 Fax: +353 1 667 0042.

Cayman Islands
Landmark Square, West Bay Road, PO Box 775, Grand Cayman KY1-9006, Cayman Islands. Tel: +1 345 949 0022 Fax: +1 345 945 0042.

New York
245 Park Avenue, 39th Floor, New York, NY 10167, U.S.A. Tel: +1 212 792 4166 Fax: +1 212 792 4167.

Tokyo
12th Floor, Yurakucho Itocia Building, 2-7-1 Yurakucho, Chiyoda-ku, Tokyo 100-0006, Japan. Tel: +813 6860 4885 Fax: +813 6860 4501.