FC-11.1 Transfers of Crypto-assets

FC-11.1.1 This section is applicable to investment firm licensees who undertake regulated investment services involving transfers of crypto-assets.

FC-11.1.2 Licensees must use technology solutions and other systems to adequately meet anti-money laundering, financial crime and know-your-customer requirements.

FC-11.1.3 Licensees must develop, implement and maintain effective transaction monitoring systems to determine the origin of a crypto-asset and to monitor its destination, and to apply strong transaction monitoring measures which enable the licensees to have complete granular data centric information about the transactions done by a client.

FC-11.1.4 Licensees must be vigilant and establish internal processes and indicators to identify crypto-assets that may have been tainted i.e. used for an illegal purpose (for example, certain clients or use of "mixer" and "tumbler" services).

Suspicious Wallet Addresses

FC-11.1.5 Licensees must establish and implement policies for identification of wallet addresses that are suspected of ML/TF (suspicious wallet addresses). Licensees must not establish or continue business relationship with or transact with suspicious wallet addresses.

FC-11.1.6 Where a Licensee identifies or becomes aware of a suspicious wallet address, it must immediately file a Suspicious Transaction Report (STR) in accordance with Chapter FC-4.

Accepted Crypto-asset Transfer to be Considered as Cross Border Transfer

FC-11.1.7 Licensees must consider all transfers of crypto-assets as cross-border transfers rather than domestic transfer.

Outward Transfers

FC-11.1.8 Licensees must include all required originator information and required beneficiary information details with the accompanying transfer of crypto-assets they make on behalf of their customers. Licensees must ensure that the information is transmitted immediately and securely.

FC-11.1 Transfers of Crypto-assets (continued)

FC-11.1.9 **For purposes of this Section, originator information refers to the information listed in Subparagraphs FC-11.1.12 (a) to (c) and beneficiary information refers to the information listed in Subparagraphs FC-11.1.12 (d) and (e).**

Inward Transfers

FC-11.1.10 **Licensees must:**

(a) Maintain records of all originator information received with an inward transfer; and

(b) Carefully scrutinize inward transfers which do not contain originator information. Licensees must presume that such transfers are 'suspicious transactions' and pass them to the MLRO for review for determination as to possible filing of STR.

FC-11.1.111 **While undertaking crypto-asset transfers, licensees must ensure that the ordering financial institution transmits the originator and beneficiary information immediately.**

Information accompanying Crypto-asset Transfers

FC-11.1.12 **Information accompanying all crypto-asset transfers must always contain:**

(a) The name of the originator;

(b) The originator account number (crypto-asset wallet) where such an account is used to process the transaction;

(c) The originator's address, or national identity number, or customer identification number, or date and place of birth;

(d) The name of the beneficiary; and

(e) The beneficiary account number (crypto-asset wallet) where such an account is used to process the transaction.

FC-11.1.13 Where a licensee undertakes a transfer of crypto-assets it is not necessary for the information referred to in Paragraph FC-11.1.11 to be attached directly to the crypto-asset transfers itself. The information can be submitted either directly or indirectly.

FC-11.1.14 **The CBB recognises that unlike traditional fiat currency wire transfers, not every crypto-asset transfer involves (or is bookended by) two institutions (crypto-asset entities or financial institution). In instances in which a crypto-asset transfer involves only one financial institution on either end of the transfer (e.g. when an ordering financial institution sends crypto-assets on behalf of its customers, the originator, to a beneficiary that is not a customer of a**

FC-11.1 Transfers of Crypto-assets (continued)

beneficiary financial institution but rather an individual user who receives the crypto-asset transfer using his/her own distributed ledger technology (DLT) software, such as an unhosted wallet), the financial institution must still ensure adherence to Paragraph FC-11.1.12 for their customer. The CBB does not expect that financial institutions, when originating a crypto-asset transfer, would submit the required information to individual users who are not financial institutions. However, financial institutions receiving a crypto-asset transfer from an entity that is not a financial institution (e.g. from an individual crypto-asset user using his/her own DLT software, such as an unhosted wallet), must obtain the required originator information from their customer.

Responsibilities of Ordering Financial Institution

FC-11.1.15 The ordering financial institution must ensure that crypto-asset transfers contain required and accurate originator information and required beneficiary information.

FC-11.1.16 The ordering financial institution must maintain all originator and beneficiary information collected in accordance with Chapter FC-6.

FC-11.1.17 The ordering financial institution must not execute the accepted crypto-asset transfer if it does not comply with the requirements of Paragraphs FC-11.1.15 and FC-11.1.16.

Responsibilities of Intermediary Financial Institutions

FC-11.1.18 For crypto-asset transfers, financial institutions processing an intermediary element of such chains of transfers must ensure that all originator and beneficiary information that accompanies a crypto-asset transfer is retained with it.

FC-11.1.19 An intermediary financial institution must take reasonable measures to identify crypto-asset transfers that lack the required originator information or required beneficiary information.

Responsibilities of Beneficiary Financial Institution

FC-11.1.20 A beneficiary financial institution must take reasonable measures to identify crypto-asset transfers that lack the required originator or the required beneficiary information. Such measures may include post-event monitoring or real-time monitoring where feasible.

FC-11.1 Transfers of Crypto-assets (continued)

FC-11.1.21 For crypto-asset transfers, a beneficiary financial institution must verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with Chapter FC-6.

Additions to the Glossary:

Beneficiary

(As used in Module FC): refers to the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested crypto-asset transfer.

Beneficiary financial institution

Refers to the financial institution which receives the crypto-asset transfer from the ordering financial institution directly or through an intermediary financial institution and makes the funds available to the beneficiary.

Ordering financial institution

Refers to the financial institution which initiates the crypto-asset transfer and transfers the funds upon receiving the request for a crypto-asset transfer on behalf of the originator.

Originator

Refers to the account holder who allows the crypto-asset transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the crypto-asset transfer.