



# **FINANCIAL CRIME MODULE**

<b>MODULE</b>	<b>FC (Financial Crime)</b>
<b>CHAPTER</b>	<b>Table of Contents</b>

		Date Last Changed
FC-A.1	Purpose	01/2022
FC-A.2	Module History	10/2023
<b>FC-B</b>	<b>Scope of Application</b>	
FC-B.1	License Categories	04/2006
FC-B.2	Overseas Subsidiaries and Branches	01/2018
<b>FC-C</b>	<b>Risk Based Approach</b>	
FC-C.1	Risk Based Approach	01/2022
FC-C.2	Risk Assessment	01/2023
<b>FC-1</b>	<b>Customer Due Diligence</b>	
FC-1.1	General Requirements	10/2023
FC-1.2	Face-to-face Business	01/2022
FC-1.3	Enhanced Customer Due Diligence: General Requirements	01/2022
FC-1.4	Enhanced Customer Due Diligence: Non face-to-face Business and New Technologies	01/2022
FC-1.5	Enhanced Customer Due Diligence: Politically Exposed Persons (PEPs)	01/2022
FC-1.6	Enhanced CDD for Charities, Clubs and Societies	01/2022
FC-1.7	Enhanced CDD: 'Pooled Funds'	10/2014
FC-1.8	Introduced Business from Professional Intermediaries	01/2018
FC-1.9	Shell Banks	10/2019
FC-1.10	Simplified Customer Due Diligence	01/2022
FC-1.11	Reliance on Third Parties for Customer Due Diligence	10/2023
<b>FC-2</b>	<b>AML / CFT Systems and Controls</b>	
FC-2.1	General Requirements	04/2020
FC-2.2	On-going Customer Due Diligence and Transaction Monitoring	01/2022
<b>FC-3</b>	<b>Money Laundering Reporting Officer (MLRO)</b>	
FC-3.1	Appointment of MLRO	10/2019
FC-3.2	Responsibilities of the MLRO	01/2020
FC-3.3	Compliance Monitoring	01/2022
<b>FC-4</b>	<b>Suspicious Transaction Reporting</b>	
FC-4.1	Internal Reporting	04/2006
FC-4.2	External Reporting	10/2019
FC-4.3	Contacting the Relevant Authorities	10/2019
<b>FC-5</b>	<b>Staff Training and Recruitment</b>	
FC-5.1	General Requirements	01/2022

<b>MODULE</b>	<b>FC (Financial Crime)</b>
<b>CHAPTER</b>	<b>Table of Contents (continued)</b>

**Date Last  
Changed**

<b>FC-6</b>	<b>Record-keeping</b>	
FC-6.1	General Requirements	01/2019
<b>FC-7</b>	<b>NCCT Measures and Terrorist Financing</b>	
FC-7.1	Special Measures for 'NCCTs'	10/2014
FC-7.2	Terrorist Financing	01/2023
FC-7.3	Designated Persons and Entities	04/2006
<b>FC-8</b>	<b>Enforcement Measures</b>	
FC-8.1	Regulatory Penalties	04/2006
<b>FC-9</b>	<b>AML / CFT Guidance and Best Practice</b>	
FC-9.1	Guidance Provided by International Bodies	10/2014
<b>FC-10</b>	<b>Fraud</b>	
FC-10.1	General Requirements	01/2016
<b>FC-11</b>	<b>Crypto-assets</b>	
FC-11.1	Transfers of Crypto-assets and Wire Transfers	XX/2024

## **APPENDICES (included in Volume 4 (Investment Business), Part B)**

### **CBB Reporting Forms**

<i>Form Name</i>	<i>Subject</i>	
STR	<del>Suspicious Transaction Reporting Form</del> [Deleted in July 2016]	07/2016
MLRO	[This form is deleted 07/2010]	

### **Supplementary Information**

<i>Item Number</i>	<i>Subject</i>	
FC-(i)	Decree Law No. 4 (2001)	04/2006
FC-(i)(a)	Decree Law No. 54 (2006)	07/2007
FC-(i)(b)	Decree Law No.58 (2006)	07/2007
FC-(ii)	UN Security Council Resolution 1373 (2001)	04/2006
FC-(iii)	UN Security Council Resolution 1267 (1999)	04/2006
FC-(iv)	Examples of Suspicious Transactions	04/2006
FC-(v)	Guidance Notes	04/2006

<b>MODULE</b>	<b>FC: Financial Crime</b>
<b>CHAPTER</b>	<b>FC-11: Crypto-assets</b>

## FC-11.1 Transfers of Crypto-assets and Wire Transfers

**FC-11.1.1** This section is applicable to investment firm licensees who undertake regulated investment services involving transfers of crypto-assets. The CBB considers transactions involving transfer of crypto-assets as functionally analogous to wire transfer.

**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.

### *Crypto-asset Transfers to be considered as Cross Border Wire Transfer*

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

<b>MODULE</b>	<b>FC: Financial Crime</b>
<b>CHAPTER</b>	<b>FC-11: Crypto-assets</b>

## FC-11.1 Transfers of Crypto-assets and Wire Transfers (continued)

### *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 and/or wire transfer of funds they make on behalf of their customers.

**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 (i.e. full name, address and account number or a unique customer identification number). 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, unless the ordering financial institution is able to promptly (i.e. within two business days) advise the licensee in writing of the originator information upon the licensee’s request. The period of 2 business days provided to ordering financial institution by the licensees to furnish the originator information is only applicable while undertaking fund transfer (traditional wire transfer) and must not be used in case of transfer of crypto-assets.

**FC-11.1.11** While undertaking crypto-asset transfers, licensees must ensure that the ordering financial institution transmits the originator and beneficiary information immediately.

<b>MODULE</b>	<b>FC: Financial Crime</b>
<b>CHAPTER</b>	<b>FC-11: Crypto-assets</b>

## FC-11.1 Transfers of Crypto-assets and Wire Transfers (continued)

### *Information accompanying Crypto-asset and Cross Border Wire Transfers*

- FC-11.1.12** Information accompanying all crypto-asset transfers as well as wire transfers must always contain:
- (a) The name of the originator;
  - (b) The originator account number (e.g. IBAN or 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 (e.g. IBAN or 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-11.1.12 to be attached directly to the crypto-asset transfers itself. The information can be submitted either directly or indirectly.

**FC-11.1.14** Licensees while undertaking transfer of crypto-assets must ensure that the required originator and beneficiary information is transmitted immediately and securely.

**FC-11.1.15** For the purposes of Paragraph FC-11.1.14, “Securely” means that the provider of the information must protect it from unauthorized disclosure as well as ensure that the integrity and availability of the required information is maintained so as to facilitate recordkeeping and the use of such information by financial institution. The term “immediately” means that the provider of the information must submit the required information simultaneously or concurrently with the transfer of the crypto-asset.

<b>MODULE</b>	<b>FC: Financial Crime</b>
<b>CHAPTER</b>	<b>FC-11: Crypto-assets</b>

## FC-11.1 Transfers of Crypto-assets and Wire Transfers (continued)

**FC-11.1.16** 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 institutions). 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 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.

### *Domestic Wire Transfers*

**FC-11.1.17** Information accompanying domestic wire transfers must also include originator information as indicated for cross-border wire transfers unless this information can be made available to the beneficiary financial institution and the CBB by other means. In this latter case, the ordering financial institution need only include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary.

**FC-11.1.18** For the purposes of Paragraph FC-11.1.17, the information should be made available by the ordering financial institution within three business days of receiving the request either from the beneficiary financial institution or from the CBB.

**FC-11.1.19** It is not necessary for the recipient institution to pass the originator information on to the beneficiary. The obligation is discharged simply by notifying the beneficiary financial institution of the originator information at the time the transfer is made.

<b>MODULE</b>	<b>FC: Financial Crime</b>
<b>CHAPTER</b>	<b>FC-11: Crypto-assets</b>

## FC-11.1 Transfers of Crypto-assets and Wire Transfers (continued)

### *Responsibilities of Ordering Financial Institution*

- FC-11.1.20** The ordering financial institution must ensure that crypto-asset transfers and wire transfers contain required and accurate originator information and required beneficiary information.
- FC-11.1.21** The ordering financial institution must maintain all originator and beneficiary information collected in accordance with Chapter FC-6.
- FC-11.1.22** The ordering financial institution must not execute the crypto-asset transfer or wire transfer if it does not comply with the requirements of Paragraphs FC-11.1.20 and FC-11.1.21.

### *Responsibilities of Intermediary Financial Institutions*

- FC-11.1.23** For crypto-asset transfers and cross-border wire 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 or wire transfer is retained with it.
- FC-11.1.24** Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record must be kept, for at least five years, by the receiving intermediary financial institution of all the information received from the ordering financial institution or another intermediary financial institution.
- FC-11.1.25** An intermediary financial institution must take reasonable measures to identify crypto-asset transfers and cross-border wire transfers that lack the required originator information or required beneficiary information.
- FC-11.1.26** An intermediary financial institution must have effective risk-based policies and procedures for determining:
- (a) When to execute, reject, or suspend a traditional wire transfer lacking required originator or required beneficiary information; and
  - (b) The appropriate follow-up action.



<b>MODULE</b>	<b>FC: Financial Crime</b>
<b>CHAPTER</b>	<b>FC-11: Crypto-assets</b>

## FC-11.1 Transfers of Crypto-assets and Wire Transfers (continued)

### *Responsibilities of Beneficiary Financial Institution*

- FC-11.1.27** A beneficiary financial institution must take reasonable measures to identify crypto-asset transfers and cross-border wire 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-11.1.28** For crypto-asset transfers and wire 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.
- FC-11.1.29** A beneficiary financial institution must have effective risk-based policies and procedures for determining:
- (a) When to execute, reject, or suspend a traditional wire transfer lacking required originator or required beneficiary information; and
  - (b) The appropriate follow-up action.