AMENDMENTS № 5 TO AIFC ANTI-MONEY LAUNDERING, COUNTER-TERRORIST FINANCING AND SANCTIONS RULES

Approval Date: 10 September 2023

Commencement Date: 1 January 2024

Astana, Kazakhstan

In this document, underlining indicates a new text and strikethrough indicates a removed text.

Amendments to the AIFC AML, Counter-Terrorist Financing and Sanctions Rules

(…)

6. CUSTOMER DUE DILIGENCE
6.1. Conducting Customer Due Diligence
6.1.1. Obligation to conduct Customer Due Diligence

A Relevant Person must:
(a) conduct CDD under AML 6.3.1 for each of its customers including when the customer is carrying out occasional transactions the value of which singularly or in several linked operations (whether at the time or later), equal or exceed USD 15,000; and
(a-a) conduct CDD under AML 6.3.1 for each of its customers including when the customer is carrying out occasional transactions with Digital Assets the value of which singularly or in several linked operations (whether at the time or later), equal or exceed USD 1,000; and
(b) in addition to (a) and (a-a), conduct EDD under AML 7.1.1 in respect of:
(i) each customer it has assigned as high risk;
(ii) business relationships and transactions with persons from countries with high geographical risk factors.

(…)

11-1. TRANSFER OF DIGITIAL ASSETS
11-1.1. Digital Asset transfer
(1) If a Digital Asset Service Provider transfers Digital Assets to another Digital Asset Service Provider:
(a) the originating Digital Asset Service Provider must:
(i) obtain and hold required and accurate originator information and required beneficiary information on the transfer; and
(ii) immediately and securely submit the information in (i) to the beneficiary Digital Asset Service Provider or any other relevant institution as so required by law.
(2) The information in (1) should be stored in a manner such that it cannot be altered and so that it is readily available to AFSA on AFSA's request.
(3) For the purposes of 1(a), an originating Digital Asset Service Provider must ensure that all transfers of Digital Assets with value equal to or more than USD1,000 involving natural persons are accompanied by:
(a) the name of the originator;
(b) the originator's digital asset wallet address or account number or (in the absence of an account) unique transaction reference number;
(c) the originator's physical address, or national identity number, or customer identification, or date and place of birth;
(d) the name of the beneficiary; and
(e) the beneficiary's digital asset wallet address or account number or (in the absence of an account) unique transaction reference number.
(4) For the purposes of 1(a), an originating Digital Asset Service Provider must ensure that all transfers of Digital Assets with value equal of less than USD 1,000 involving natural persons are accompanied by:
(a) the name of the originator;
(b) the originator's digital asset wallet address or account number or (in the absence of an account) unique transaction reference number;
(c) the name of the beneficiary; and
(d) the beneficiary's digital asset wallet address or account number or (in the absence of an account) unique transaction reference number.

(5) For the purposes of 1(a), an originating Digital Asset Service Provider must ensure that all all transfers of Digital Assets with value equal to or more than USD 1,000 involving Body Corporates are accompanied by:
(a) the registered corporate name or trading name of the originator;
(b) the originator's digital asset wallet address or account number or (in the absence of an account) unique transaction reference number;
(c) either of the following:
(i) the customer identification number; or
(ii) the registered office address or primary place of business;
(d) the following beneficiary information:
(i) the name of the beneficiary; and
(ii) beneficiary's digital asset wallet address account number or (in the absence of an account) unique transaction reference number.
(6) For the purposes of 1(a), an originating Digital Asset Service Provider must ensure that all transfers of Digital Assets with value equal of less than USD 1,000 involving Body Corporates are accompanied by:
(a) the name of the originator;
(b) the originator's account number or (in the absence of an account) unique transaction reference number;
(d) the following required beneficiary information;
(i) the name of the beneficiary; and
(ii) beneficiary's account number or (in the absence of an account) unique transaction reference number.
(7) The Digital Asset Service Provider should not execute a transaction if it does not comply with requirements set out in (3), (4), (5) or (6), as applicable, and should return the relevant amounts back to the originator. The Digital Asset Service Provider should have appropriate risk-based policies and procedures to determine when to execute, reject or suspend a transfer lacking the required information while at all times complying with these requirements.
(8) In determining the value of a transfer, Digital Asset Service Providers must take a reasonable and justified approach. If multiple transfers from the same originator appear to be linked, they will be aggregated for the purpose of calculating the transfer's value.
(9) An intermediary Digital Asset Service Provider who participates in transfers of Digital Assets must:
(a) take reasonable measures, consistent with current guidance, to identify transfers of Digital Assets that lack the required originator or beneficiary information;
(b) adopt risk-based policies and procedures to determine when to execute, reject or suspend a transfer lacking the required information; and
(c) keep records for at least 6 years after the completion of the transaction to which it relates.
(10) If several transfers from a single originator are bundled in a batch file for transmission to beneficiaries, they may be exempted from the requirements in respect of originator information, provided that they include the originator's account number or unique transaction reference number, and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

11-1.2. Digital Asset Transfers to or from self-hosted digital wallets

(1) In case of a transfer of a Digital Asset made to or received from a self-hosted digital wallet, the Digital Asset Service Provider of the originator or beneficiary must obtain and hold information referred to in 11-1.1.(3), (4), (5) or (6) from Clients and ensure that the transfer of Digital Assets can be individually identified.

(2) If a Digital Asset transfer exceeds USD 1,000 or there is a suspicion of money laundering or terrorist financing of a transfer to a self-hosted digital wallet, the Digital Asset Service Provider of the originator or beneficiary must take adequate measures on a risk-sensitive basis to mitigate and manage the money laundering and terrorist financing risks associated with the transfer.

Guidance on risk mitigating measures on transfers to or from self-hosted digital wallets

A Digital Asset Service Provider should undertake the following non-exhaustive measures to ensure compliance with AML 11-1.2 (2):
(a) to conduct enhanced monitoring of Digital Asset transfers with self-hosted digital wallets;
(b) to accept Digital Asset transfers from or to self-hosted digital wallets only where the Digital Asset Service Provider has them assessed to be reliable, having regard to the screening results of the Digital Asset transactions and the associated digital wallets and the assessment results on the ownership or control of the self-hosted digital wallet by the originator or beneficiary; and
(c) to impose transaction limits or prohibition.

Note: Chapter 11-1. comes into operation 12 months after the commencement date of the AIFC Rules on Digital Asset Activities.

11-2. DIGITAL ASSET TRANSFER COUNTERPARTY DUE DILIGENCE AND ADDITIONAL MEASURES

11-2.1. General requirements

(1) If a Digital Asset Service Provider conducts a Digital Asset transfer referred to in Chapter 11-1, the Digital Asset Service Provider will be exposed to money laundering and terrorist financing risks associated with the institution which may be the ordering institution, intermediary institution or beneficiary institution involved in the Digital asset transfer ("Digital Asset transfer counterparty").
(2) To avoid sending or receiving a Digital Asset to or from illicit actors or designated parties that had not been subject to appropriate CDD and screening measures of a Digital Asset transfer counterparty and to ensure compliance with the Travel Rule, a Digital Asset Service Provider must conduct due diligence on the Digital Asset transfer counterparty. A Digital Asset Service Provider should identify and assess the money laundering and terrorist financing risks associated with the Digital Asset transfer to or from the Digital Asset transfer counterparty and apply the appropriate risk-based anti-money laundering and countering financing terrorism measures.
(3) A Digital Asset Service Provider must conduct due diligence measures on a Digital Asset transfer counterparty before conducting a Digital Asset transfer or making the transferred Digital Assets available to the recipient.
(4) A Digital Asset Service Provider does not need to undertake the Digital Asset transfer counterparty due diligence process for every individual Digital Asset transfer when dealing with Digital Asset transfer counterparties that it has already conducted counterparty due diligence on previously, unless there is a suspicion of money laundering and terrorist financing.
(5) A Digital Asset Service Provider must undertake reviews of the Digital Asset transfer counterparty due diligence records on a regular basis or upon trigger events (e.g., when it becomes aware of a suspicious transaction or other information such as negative news from credible media, public information that the counterparty has been subject to any targeted financial sanction, money laundering and terrorist financing investigation or regulatory action).
(6) Based on the Digital Asset transfer counterparty due diligence results, a Digital Asset Service Provider must determine if it should continue to conduct Digital Asset transfers with, and submit the required information to, a Digital Asset transfer counterparty, and the extent of anti-money laundering and countering financing terrorism measures that it should apply in relation to a Digital Asset transfer with the Digital Asset transfer counterparty on a risk-sensitive basis.

Guidance

Digital Asset transfer counterparty due diligence may involve the following non-exhaustive procedures:
(a) determining whether a Digital Asset transfer is or will be with a Digital Asset transfer counterparty or a self-hosted digital wallet;
(b) where applicable, identifying the Digital Asset transfer counterparty (e.g., by making a reference to a list of licensed or registered Digital Asset Service Providers or financial institutions in different jurisdictions); and
(c) assessing whether a Digital Asset transfer counterparty is an eligible counterparty to deal with and to send the required information to.

11-2.2. Digital Asset transfer counterparty due diligence measures

A Digital Asset Service Provider must apply the following Digital Asset transfer counterparty due diligence measures before it conducts a Digital Asset transfer with a Digital Asset transfer counterparty:

(a) determining if the respondent entity is licensed or registered;

(b) collecting sufficient information about the Digital Asset transfer counterparty to enable it to understand fully the nature of the Digital Asset transfer counterparty's business;

(c) understanding the nature and expected volume and value of a Digital Asset transfer with the Digital Asset transfer counterparty;

(d) determining from publicly available information the reputation of the Digital Asset transfer counterparty and the quality and effectiveness of the anti-money laundering and countering financing terrorism regulation and supervision over the Digital Asset transfer counterparty by authorities in the relevant jurisdiction;

(e) assessing the anti-money laundering and countering financing terrorism controls of a Digital Asset transfer counterparty and ensure that they are adequate and effective;

(f) assessing whether the Digital Asset transfer counterparty is subject to the Travel Rule similar to that imposed under Chapter 11-1 in the jurisdiction in which the Digital Asset transfer counterparty operates or is incorporated;

(g) assessing the adequacy and effectiveness of the anti-money laundering and countering financing terrorism controls that the Digital Asset transfer counterparty has put in place for ensuring compliance with the Travel Rule;

(h) assessing whether the Digital Asset transfer counterparty can protect the confidentiality and integrity of personal data (e.g., the required originator and recipient information), taking into account the adequacy and robustness of data privacy and security controls of the Digital Asset transfer counterparty; and

(j) obtaining approval from its senior management.

Guidance:

(1) While a relationship with a Digital Asset transfer counterparty is different from a cross-border correspondent relationship referred to in Chapter 10, there are similarities in the due diligence approach which can be of assistance to a Digital Asset Service Provider. By virtue of this, the Digital Asset Service Provider should conduct due diligence measures in Chapter 10, with reference to the requirements set out in AML 10.2.

(2) When assessing money laundering and terrorist financing risks posed by a Digital Asset transfer counterparty, a Digital Asset Service Provider should take into account the relevant factors that may indicate a higher money laundering and terrorist financing risk. Examples of such risk are where a Digital Asset transfer counterparty:

(i) operates or is incorporated in a jurisdiction posing a higher risk or with a weak anti-money laundering and countering financing terrorism regime;

(ii) is not (or yet to be) licensed or registered and supervised for anti-money laundering and countering financing terrorism purposes in the jurisdiction in which it operates or is incorporated by the relevant authorities;

(iii) does not have in place adequate and effective anti-money laundering and countering financing terrorism systems, including measures for ensuring compliance with the Travel Rule;

(iv) does not implement adequate measures or safeguards for protecting the confidentiality and integrity of personal data; or

(v) is associated with money laundering and terrorist financing or other illicit activities.

Note: Chapter 11-2. comes into operation 12 months after the commencement date of the AIFC Rules on Digital Asset Activities.