AIX Anti-Money Laundering (AML) Market Notice[1]: Compliance and Procedures applicable to Members

1. Members' Policy

AIX Members[2] have an obligation to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities ("AML") by complying with requirements hereunder and all applicable AML laws and regulations in jurisdictions they operate.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

AIX Members shall have AML policies, procedures and internal controls designed to ensure compliance with all applicable regulations and rules and must be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in Members' business.

AIX Member shall certify regularly to AIX Regulation & Compliance that it has implemented its anti-money laundering program and that it will perform (or its agent will perform) specified requirements of the customer identification program and suspicious transaction reporting.

2. AML Compliance Person Designation and Duties

AIX Members must designate a senior staff person as their Money Laundering Reporting Officer (MLRO), with full responsibility for the Member's AML program. The MLRO must be qualified by experience, knowledge and training. The duties of the MLRO will include monitoring the Member's compliance with AML obligations, overseeing communication and training for employees. The MLRO will also ensure that the Member keeps and maintains all of the required AML records and will ensure that Suspicious Activity Reports (SARs) are

[1] Published via Market Notice No. 2020.03.17_01 dated 17.03.2020

[2] For the purpose of this Notice, "AIX Member" or "Member" shall mean broker/dealer admitted as a Member of AIX and/or as a Participant of AIX CSD.

filed with a respective financial intelligence unit ("FIU")[3] when appropriate. The MLRO is vested with full responsibility and authority to enforce the Member's AML program.

Member firms will provide AIX Regulation & Compliance with contact information for the MLRO, including: (1) name; (2) title; (3) mailing address; (4) email address; (5) telephone number; and (6) facsimile number and will keep AIX informed of any change in this information and will review, and if necessary update, this information upon request of AIX.

3. Risk-based approach and Customer Identification Program

AIX Member should identify, assess, and understand the money laundering and terrorist financing risks emerging from launch of new product, service or relationship with client. Based on that assessment, AIX Member should apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified.

AIX Members are required to have and follow reasonable procedures to document and verify the identity of their customers who open new accounts. These procedures must address the types of information the Member will collect from the customer and how it will verify the customer's identity. These procedures must enable the Member to form a reasonable belief that it knows the true identity of its customers.

The Member's customer identification program (CIP) must be in writing and be part of the Member's AML compliance program.

a. Identification of Customer

Based on the risk, and to the extent reasonable and practicable, AIX Members will ensure that they have a reasonable belief that they know the true identity of their customers by using risk-based procedures to verify and document the accuracy of the information they get about their customers.

AIX Members will verify customer identity through documentary means. Appropriate documents for verifying the identity of customers include the following:

- For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as passport; and

- For a person other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or a trust instrument.

The risk that members may not know the customer's true identity may be heightened for certain types of accounts, such as an account opened in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction that has been designated by FATCA as a primary money laundering jurisdiction, a terrorist concern,

[3] Financial intelligence unit (FIU) is a national centre for the receipt and analysis of suspicious transaction reports and other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis.

or has been designated as a non-cooperative country or territory. AIX Members will identify customers that pose a heightened risk of not being properly identified.

b. Lack of Verification

When AIX Members cannot form a reasonable belief that they know the true identity of a customer or customer due diligence cannot be completed to satisfaction of AIX Member, they will do the following: (1) not open an account; (2) impose terms under which a customer may conduct transactions while an attempt to verify the customer's identity is made; (3) close an account after attempts to verify customer's identity fail; and (4) determine whether it is necessary to file a Suspicious Account Report (SAR) in accordance with applicable laws and regulations.

c. Recordkeeping

AIX Members will document the verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. They will keep records containing a description of any document that they relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date.

d. Reliance on Another Financial Institution for Identity Verification

AIX Members may, under the following circumstances, rely on the performance by another financial institution (including an affiliate) of some or all of the elements of their CIP with respect to any customer that is opening an account or has established an account or similar business relationship with the other financial institution to provide or engage in services, dealings or other financial transactions:

- when such reliance is reasonable under the circumstances;
- when the other financial institution is subject to a rule implementing the anti-money laundering compliance program requirements and is regulated in a jurisdiction which has comparable AML standards; and
- when the other financial institution has entered into a contract with the AIX Member requiring it to certify regularly to the AIX Member that it has implemented its anti-money laundering program and that it will perform (or its agent will perform) specified requirements of the customer identification program.

The AIX Member will not be held responsible for the failure of the other financial institution to fulfill adequately its CIP responsibilities, provided that the AIX Member can establish that its reliance was reasonable and it has obtained the requisite contracts and certifications.

4. General Customer Due Diligence

AIX Members must obtain sufficient information about each customer to allow them to evaluate the risk presented by that customer and to detect and report suspicious activity. When they open an account for a customer, the due diligence they perform may be in addition to customer information obtained for purposes of the CIP.

Such information should include:

- the customer's business;

- the customer's anticipated account activity (both volume and type);
- the source of the customer's funds.

For accounts that are deemed to be higher risk, AIX Members will obtain the following information:

- the purpose of the account;
- the source of funds and wealth;
- the beneficial owners of the accounts;
- the customer's (or beneficial owner's) occupation or type of business;
- financial statements;
- banking references;
- domicile (where the customer's business is organized);
- description of customer's primary trade area and whether international transactions are expected to be routine;
- description of the business operations and anticipated volume of trading;
- explanations for any changes in account activity.

5. Due Diligence and Enhanced Due Diligence Requirements for Politically Exposed Persons (PEPs)

AIX Members will review public information, including information available in Internet databases, to determine whether any of their customers are PEPs. If they discover information indicating that a particular customer may be a PEP, and upon taking additional reasonable steps to confirm this information, they determine that the individual is, in fact, a PEP, they will conduct additional enhanced due diligence to detect and report transactions that may involve money laundering or the proceeds of foreign corruption.

In so doing, AIX Members will consider the risks that the funds in the account may be the proceeds of foreign corruption by determining the purpose and use of the private banking account, location of the account holder(s), source of funds in the account, type of transactions conducted through the account and jurisdictions involved in such transactions.

6. Sanctions

Sanctions screening must be completed, client business and transactions shall be checked against relevant Sanctions issued by such bodies as:

- CFM;
- United Nations Security Council;
- FATF;
- Consolidated list for financial sanctions in the European Union (EU);
- HM Treasury lists (UK);
- Office of Foreign Asset Controls – OFAC lists (US).
- Others

7. Monitoring Accounts for Suspicious Activity

AIX Members will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to their business.

8. Suspicious Transactions Reporting

a. Filing a SAR

Pursuant to Article 4 of AML Law and Resolution of the Government of Kazakhstan # 1484 dated 23.11.2012, AIX Members must file SAR with FIU for any transactions on AIX / AIX CSD conducted or attempted by, at or through their firm: (i) involving KZT 7,000,000 (or an equivalent amount in another currency) or more of funds or assets (either individually or in the aggregate), or (ii) where they know, suspect or have reason to suspect:

(1) the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade applicable law or regulation or to avoid any transaction reporting requirement under applicable law or regulation;
(2) the transaction is designed, whether through structuring or otherwise, to evade any requirements of the AML regulations;
(3) the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and after examining the background, possible purpose of the transaction and other facts, the Member knows of no reasonable explanation for the transaction; or
(4) the transaction involves the use of the Member or AIX / AIX CSD to facilitate criminal activity.

The Member's MLRO and his or her designee will be responsible for ensuring that SARs in relation to trading activity on AIX/ AIX CSD are filed as required.

They will also file a SAR and notify the appropriate law enforcement authority in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes.

AIX Members will report suspicious transactions by completing a SAR, and they will collect and maintain supporting documentation as required by the regulations. They will file a SAR within deadlines determined under applicable AML laws and regulations.

They will retain copies of any SAR filed in relation to trading activity on AIX/ AIX CSD and the original or business record equivalent of any supporting documentation for at least six years from the date of filing the SAR. They will identify and maintain supporting documentation and make such information available to FIU and any other appropriate law enforcement agencies, securities regulators, or AIX Regulation & Compliance exercising and performing self-regulatory powers and functions in relation to Financial Services, upon request. In particular, AIX Regulation & Compliance may require the Member to make such information available if such Member use omnibus structure for trading and settlement on AIX / AIX CSD.
AIX Members will not notify any person involved in the transaction that the transaction has been reported.

10. AML Recordkeeping

The AIX Member's MLRO and his or her designee will be responsible for ensuring that AML records are maintained properly for at least six years from the date on which the notification or report was made, the business relationship ends or the transaction is completed, whichever occurs last.

11. Training Programs

AIX Members must develop ongoing employee training under the leadership of the Member's MLRO and senior management. The training will occur on at least an annual basis. It will be based on the Member firm's size, its customer base, and its resources and be updated as necessary to reflect any new developments in the law.

The training will include, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties; (2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis and, where appropriate, the filing of SARs); (3) what employees' roles are in the firm's compliance efforts and how to perform them; (4) the firm's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the AML regime.