Anti-Money Laundering and Countering the Financing of Terrorism Compliance / Know your Customer Policy (AML / KYC Policy)

Last amended: 31.10.2024

1. Preamble

Xcards releases this mandatory document - Anti-Money Laundering and Countering the Financing of Terrorism Compliance / Know Your Customer Policy - which sets out the standards required for Xcards to effectively minimize or completely eliminate illicit activities in the provision of its services to its customers. This objective should be achieved by implementing and complying with the FATF Standards for Virtual Assets as a matter of priority.

Among the most crucial preventive measures Xcards carries out are:

- Know your customer procedure (KYC);
- Record keeping and – suspicious transactions/activities monitoring and reporting.

To prevent fraudulent activity, Xcards performs monitoring of Customers' activity within its system using both numerous automated mechanisms and IT solutions and manual checks.

The best practices to be implemented by Xcards in its internal scrutiny procedures shall contribute the belief that virtual asset technologies and businesses can continue to grow and innovate in a responsible way, and in its turn, it will contribute to creation of a level playing field.

Xcards also implements sanction measures applied by the Republic of Seychelles in relation to quite a wide group of natural persons and legal entities. That means permanent checks whether a customer is subject to international sanctions or not, respectively fulfilment of other procedures as described in Xcards internal binding documents.

2. Know Your Customer Procedure

Xcards shall apply know your customer procedure measures in respect of customers and conduct ongoing monitoring of business relationships.

In order to establish the identity of its customers, Xcards shall obtain sufficient data (documents, supporting information) from the (prospective) customer and verify this data with independent sources. Customers who, in the opinion of Xcards, pose a higher risk may be subject to a more thorough investigation, which may lead to request for additional information and take a longer period of time to verify the identity of such Customer.

Xcards reserves the right to re-identify a customer where it deems this procedure appropriate and in this regard request additional data or renew previously provided information.

The Customer agrees to cooperate with all Xcards requests in connection with using services to verify identity and status as a legal person. The Customer may use an Unverified Account with the limitations specified in the Terms and Conditions or upgrade to the Verified Account through Verification by providing necessary additional information and documents as specified, but not limited herein.

If documents are in a foreign language, Xcards may require that the documents be translated into the language understandable for Xcards. The Customer shall bear the costs concerning the formalization, translation, certification of the documents and other related costs and they are not subject to reimbursement by Xcards.

For Customer's Verification, Xcards requests the following documents/information:

- Proof of identity (passport, driver's license, national identity card);
- Proof of address (tenancy agreement, utility bills, telephone bills, bank statements, etc.);
- Phone number verified by receiving a code via SMS;
- Other documents/information at Xcards' own discretion depending on the nature of Transfer Order and/or other operations/activity.

Xcards reserves the right to request to have a call with a video to make sure that the documents are provided by the passport holder or to have additional photo/video verification.

Based on the risk, and to the extent reasonable and practicable, Xcards will ensure that Xcards has a reasonable belief that Xcards knows the true identity of Customer by using Verification and documents provided by the Customer. Xcards will analyze the information Xcards obtains to determine whether the information is sufficient to form a reasonable belief that Xcards knows the true identity of the Customer (e.g., whether the information is logical or contains inconsistencies). Despite any provisions, the Customer confirms that he is solely responsible for the accuracy of any information provided.

3. Suspicious transactions/activities monitoring and reporting

Xcards shall conduct ongoing monitoring (check) of a business relationship.

In accordance with a Section 46(2) of the AML/CFT Act "ongoing monitoring" of a business relationship means the following;

- Scrutinizing transactions undertaken throughout the relationship to ensure that the transactions are consistent with a Xcards knowledge of the customer, the business and risk profile and the source of funds of the customer;
- Keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up to date.

Following its AML Policy and the applicable legal acts, Xcards, when necessary, will report to the respective authorities of the activities that may be considered as money laundering and terrorist financing. Xcards will not disclose any information about such report to have been made and will not address any questions in relation to that.

The requirement to report suspicious transactions applies to all types of transactions or activities.

4. Ongoing monitoring

Xcards reserves the right to continuously monitor, on a risk-sensitive basis, the business relationship with a Customer by:

- Periodically reviewing documents, data, and information obtained to ensure they are up to date (through third parties).
- Conducting appropriate scrutiny of Transactions and activities carried out by Customers to ensure they are consistent with Xcards' knowledge of the Customer's business and risk profile, and verifying that such Transactions and activities align with Xcards' understanding of the Customer's source of funds and wealth.

To continuously monitor the business relationship with a Customer, Xcards may conduct file reviews to ensure that information held about the Customer is up to date and that identification documents are still valid. Additionally, Xcards may more frequently monitor transactional activity to identify any red flags or unusual activity.

AML online check services are based on the AML Global Watchlist, which includes global AML risk data sources such as sanction lists (e.g., OFAC, UN, HMT, EU, DFAT), law enforcement lists (e.g., Interpol, country-specific government and state agencies, police forces), and international governing regulatory bodies (financial and securities commissions).

5. Record keeping and reporting

If Xcards suspects that a Customer is involved in money laundering, terrorist financing, or other illegal activities, it shall report any relevant knowledge or suspicion to governmental and regulatory authorities. Xcards will not notify any Customers of such suspicious transaction reports. Employees and Xcards may be held liable for tipping off Customers, which is a criminal offense punishable by a fine and/or imprisonment.

Xcards shall retain data collected for AML/KYC purposes throughout the business relationship for a period of five (5) years from the date of transaction. Registration or another interaction between the Customer and Xcards completion, or for such other minimal period as required by applicable law.