MORE2SAVE TECHNOLOGIES ApS
Usserød Kongevej 157
2970 Hørsholm, Denmark
Reg.: 39789841

AML KYC Policy

Effective from November 2nd of 2020

1. INTRODUCTION

This Policy is provided to you to help you understand, as a potential or actual client of More2Save Technologies ApS, a company with registration number 39789841, registered at Usserød Kongevej 157, 2970 Hørsholm, Denmark, (the "Company" or "us") the basic principles that the companies employ to discharge its regulatory duties relating to customer identification and verification and the measures that the Company takes regarding the prevention of money laundering and terrorist financing on its Platform.

This Policy forms an integral part of the Client Agreement and other terms and policies that govern your relationship with us. As a pre-requisite of opening and maintaining a trading account with us, you must agree to and accept and consent to the terms of the Client Agreement. By doing so, you also agree to the terms of this Policy.

You must ensure that you have read and understood the contents of this Policy before you commence any operations on your Cartex wallet account (hereafter the "Cartex account").

This Policy lays down the Company's framework and procedures for:

(i) preventing the Company and its Platform from being used, intentionally or unintentionally, by criminal elements for money laundering or financing of terrorist activities;

(ii) enabling the Company to know/understand the Users of its Platform and their background and source of funds;

(iii) properly identify and verify the identity of Users. This Policy can be modified or altered by the Company at any time with or without notice.

2. LEGAL FRAMEWORK

The Company is required to comply with the provisions of the Money Laundering and Terrorist Financing Prevention Act of Estonia dated 26 October 2017 (the "Law") and the Directive 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (the "Directive") as may be amended from time to time.
In accordance with the Law, we are obliged to set out policies and procedures for preventing money laundering activities.

Those procedures, which are implemented by the Company include, inter alia:

(i) identification and due diligence procedures of the Users through the implementation of a risk-based approach;

(ii) record-keeping procedures in relation to the Users' identity and their transactions at the Platform;

(iii) internal reporting procedures to the Company's Money Laundering Reporting Officer appointed to receive and consider information or suspicion that a User is engaged in money laundering activities;

(iv) appropriate procedures of internal control, risk management, with the purpose of preventing money laundering activities; and

(v) examination of transactions that due to their nature are considered vulnerable to money laundering, and especially for complicated or unusually large transactions and transactions that are taken place without an obvious financial or legal purpose;

3. RISK-BASED APPROACH

3.1 Risk-Based Approach in User Verification

The Company applies appropriate measures and procedures, on a risk-based approach, so as to focus its effort in those areas where the risk of money laundering and terrorist financing appears to be higher. A risk-based approach is adopted by the Company during the verification of the Users' identity, the collection of information for the construction of their economic profile and monitoring of their transactions and activities at their Cartex accounts. Taking into consideration the assessed risk, the company determines the type and extent of measures it adopts, to manage and mitigate the identified risks.

User acceptance procedure is prepared following a detailed assessment of the risks faced by the Company from the Users and/or their transactions and/or their countries of origin or operations and/or any other factors the Company may identify as significant from time to time. The Company identifies the Users prior to or during to commencing a business relationship.

The Company, in accordance with the Law, conducts the verification of the identity of the Users and the beneficial owners (if the User is a body corporate) during the establishment of the business relationship. The verification of Users' information may be made via the submission of documents or electronically, or by other means in the Company's sole discretion.

3.2 Timing of User Identification

The Company performs identification of the Users prior the establishment of the business relationship and proceeds with verification of the potential Users' identity prior or during the establishment of a business relationship to prevent interruption of the normal conduct of business and where there is limited risk of money laundering or terrorist financing occurring. In the case of the latter, the due diligence procedure shall be completed as soon as practicable after the initial contact. Where, in the Company's opinion, the risk of money laundering and terrorist financing cannot be determined as low, enhanced User due diligence shall be completed prior to the establishment of a business relationship. Each User is required to complete the Company's KYC procedures by submitting the relevant KYC documentation or pass electronic verification.

3.3 Operation of Cartex account prior to completion of verification

The Company, in its sole and absolute discretion, may enable a User to operate its Cartex account during the establishment of the business relationship when the User is deemed as being of low risk of money laundering and terrorism financing and according and further subject to a maximum deposit limit not exceeding the value of EUR 150 or equivalent in other currencies. Such Users must complete their KYC onboarding and provide all relevant verification documents to the Company within 14 days after the date of opening of the Cartex account.

Users who are permitted to use their Cartex account under this Section 3.3 are given 14 days from the day of the opening thereof to complete the Company's KYC and verification procedure. In a case where a User is unable to comply with the Company's KYC and verification requirements within the aforesaid time frame, the Company shall return the funds as part of the termination process and close the Cartex account. In this case, the relationship is to be considered void and the funds have to be returned to a bank account in the name of the depositor. Where the Company is unable to return the funds to its source of deposit, it must retain the funds in a separate bank account until the User completes the KYC and due diligence procedure to the Company's satisfaction in order to be able to withdraw the funds.

4. USER IDENTIFICATION

For ascertaining the true identity of the User, each User who is a natural person shall be required to provide the Company with at least the following information:

(i) True name as stated on the official identity card or passport;
(ii) Full residential address, including postal code;
(iii) Telephone;
(iv) Email address;
(v) Date of birth;
(vi) Nationality; and
(vii) Details of occupation of the User.

Each User who is a natural person shall provide to the Company at least the following documents during the onboarding procedure to verify the above information of the User:

(i) a valid proof of identity;
(ii) recent proof of residence, in the form of a utility bill, local tax authority bill or a bank statement (not older than 3 months);
(iii) such other documents as the Company may reasonably require to verify the User's source of wealth and occupation. Where a User is a body corporate or a company or any other type of legal entity, the Company shall require the following documents and information:
    a. full name of the legal entity;
    b. legal entity's address (place of operations);
    c. certificate of incorporation;
    d. memorandum of Articles and Association;
    e. certificate of registered address or a similar document;
    f. certificate or register of directors;
    g. certificate or register of shareholders;
    h. board resolution for the opening of the Cartex account indicating the authorized persons;
    i. proof or identity and proof of address of the authorized person if other than the shareholder;
    j. full KYC documents for the ultimate beneficial owner of the legal entity, including proof of beneficial ownership.

The Company reserves the right to demand when it deems appropriate, notarized and/or apostilled copies of any of the above documents along with English translation thereof. The Company reserves the right to take such additional measures as it deems fit when conducting User due diligence in cases where, in the Company's opinion,

there is an elevated higher risk of money laundering. When entering into the Client Agreement with the Company, the User authorizes the Company to carry out such searches and to transfer the User's information to such external databases and verification service providers (such as World Check) as the Company might deem necessary to complete its KYC and verification procedures.

5. POLITCALLY EXPOSED PERSONS

It's the Company policy not to establish a business relation nor accept as User persons who are classified as Politically Exposed Persons ("PEPs") or the immediate family members of PEPs due to the same presenting additional risks to the Company.

The Company has the right to perform checks in relation to the Users in external databases (such as World Check, etc.) in order to identify if the respective potential User is considered a PEP or is included in any sanctions list. The meaning of PEP includes the following natural persons who are or have been entrusted with prominent public functions in any country:

(i) heads of state, heads of government, ministers, and deputy or assistant ministers;

(ii) members of parliaments;

(iii) members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;

(iv) members of courts of auditors or of the boards of central banks;

(v) ambassadors and high-ranking officers in the armed forces;

(vi) members of the administrative, management or supervisory bodies of state-owned enterprises.

6. RECORD KEEPING

The Company documents our verification process, including all KYC information provided by the Users, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We keep records containing a description of any document that we relied on to verify your 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. With respect to nondocumentary verification, we retain documents that describe the methods and the results of any measures we took to verify the identity of Users. We also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We shall keep the Users' KYC documents and information, as well as information about the transactions posted on the Platform through the Users' Cartex accounts, for 10 (ten) years after the date of termination of a relationship with the relevant User