AML POLICY

FOR CASH DEPOSITS AND CASH WITHDRAWS

Anti-Money-Laundering Policy of November 21, 2024

Introduction: company **737 Exchange Ltd.** is having its office at: Ground Floor, The Sotheby Building, Rodney Village, Rodney Bay, Gros-Islet, Saint Lucia. The Company Registration number is 2024 - 00695

Objective of the AML Policy: We seek to offer the highest security to all of our users and customers. Therefore, we have created a three-step account verification to ensure their identities. This procedure helps us prove that the details of the person registered are correct, and the deposit methods used are not stolen or used by someone else. Moreover, it creates the general framework for the fight against money laundering. We also take into account the fact that depending on the nationality, origin, and the way of payment and withdrawal, different safety measurements must be taken.

737 Exchange Ltd. also puts reasonable measures to control and limit ML risk, including dedicating the appropriate means.

737 Exchange Ltd. is committed to high standards of anti-money laundering (AML) according to the EU guidelines and compliance and requires management and employees to enforce these standards in preventing the use of its services for money laundering purposes.

The AML program of 737 Exchange Ltd. is designed to be compliant with :

EU: “Directive 2015/849 of the European Parliament and of The Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering.”

EU: “Regulation 2015/847 on information accompanying transfers of funds.”

EU: Various regulations imposing sanctions or restrictive measures against persons and embargo on certain goods and technology, including all dual-use goods.

BE: “Law of 18 September 2017 on the prevention of money laundering limitation of the use of cash.”

DEFINITION OF MONEY LAUNDERING

Money laundering is understood as:

The conversion or transfer of property, especially money, knowing that such property is derived from criminal activity or from taking part in such activity, for the purpose of concealing or disguising the illegal origin of the property or helping any person who is involved in the commission of such an activity to evade the legal consequences of that person or companies action;

The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or an act of participation in such activity;

The acquisition, possession, or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from assisting in such activity;

Participation in, association to commit, attempts to commit and aid, abet, facilitate, and counsel the commission of any of the actions referred to in points before.

Money laundering shall be regarded as such even when the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

ORGANIZATION OF THE AML FOR 737 Exchange Ltd.

In accordance with the AML legislation, 737 Exchange Ltd. has appointed the "highest level" for the prevention of ML: the full management of 737 Exchange Ltd. is in charge.

Furthermore, an AMLCO (Anti Money Laundering Compliance Officer) is in charge of enforcing the AML policy and procedures within the system.

The AMLCO is placed under the direct responsibility of the general management.

AML POLICY CHANGES AND IMPLEMENTATION REQUIREMENTS

Each major change of 737 Exchange Ltd. AML policy is subject to approval by the general management of 737 Exchange Ltd. and the AMLCO.

THREE-STEP VERIFICATION

Step one verification:

Step one verification must be done by every user themselves upon the registration on the website operated by 737 Exchange Ltd. During this process, the user fills out the requested fields with information such as 1) email address, 2) first name, last name, gender, birth date, 3) country, zip code, city, state/province, phone number, currency, and address.

Step two verification:

Step two verification must be done by every user who has deposited over $2000 (two thousand dollars) or requested their first cashout. Until step two verification is done, the related cash-out or deposit transaction will be placed on hold.

Step two verification requires the scan copy or photo of the user's ID documents, taken by the user and sent to the Company. Only an official ID can be used for ID verification. Depending on the country, the variety of accepted IDs may be different. The user needs to go through a deposit method confirmation too if the step-one-verification data is correct. The deposit method confirmation will be checked by two different data banks to ensure the given information matches the one provided on the first step of verification. If a mismatch of the information occurred, the user/customer is required to send in confirmation of their current residence: a recent utility bill, bank statement, or any other government-issued document under their registered name.

Step three verification:

Step three verification must be done by every user who has deposited over $5000 (five thousand dollars) or cashed out over $5000 (five thousand dollars). Until step three verification is done, the related cash-out or deposit transaction will be placed on hold. Step three verification requires users to reveal a source of wealth.

CUSTOMER IDENTIFICATION AND VERIFICATION (KYC)

The formal identification of customers on entry into commercial relations is vital, both for the regulations relating to money laundering and the KYC policy.

In order to complete the KYC procedure, we ask our users to upload a set of valid, unexpired identification documents, which includes a valid proof of identity (ID, passport, or driver's license), proof of residence (a recent utility bill, bank statement, or any other government-issued document under the registered name), and a clear copy of the card(s) used for funding the account (as a deposit confirmation method). In addition, those users who want to request a cashout are asked to add a wire instruction from the bank (if they want to receive the funds via the Bank Wire) or a screenshot of the BTC Wallet (if they want to receive the funds via the crypto payment method).

Please note that the company employee can conduct additional checks if the situation requires so.

SOURCE OF FUNDS

If a player deposits over $5000 (five thousand dollars), according to the above-mentioned information, we may ask for the source of wealth (SOW).

Examples of SOW are:

Ownership of business

Employment

Inheritance

Investment

Family

It is critical that the origin and legitimacy of that wealth are clearly understood. Please note that the company employee reserves the right to conduct additional checks and ask for additional documents if the situation requires so.

If the user deposits the amount of funds equivalent to $5000 either in one or multiple transactions, their account will be frozen until all the above-mentioned steps are successfully completed. The user will be notified via email.

RISK MANAGEMENT

ADDITIONAL MEASUREMENTS

In addition, an AI is overseen by the AML compliance officer, who will look for any unusual behavior and report it right away to the 737 Exchange Ltd. management.

According to a risk-based general experience, the human employees will recheck all checks done by the AI or other employees and may redo or do additional checks according to the situation.

In addition, a data scientist, supported by modern electronic analytic systems, will look for unusual behavior like depositing and withdrawing without betting sessions, attempts to use a different bank

account for deposit or cashout, nationality, or gaming activity changes, as well as carry out checks whether an account is used by its original owner.

Moreover, to successfully complete a cashout, a user has to use the same payment method as was used for an initial deposit in order to prevent any money laundering.

Enterprise-wide risk assessment

As part of its risk-based approach, 737 Exchange Ltd. has conducted an AML "Enterprise-wide risk assessment" (EWRA) to identify and understand risks specific to 737 Exchange Ltd. and its business lines. The AML risk policy is determined after identifying and documenting the risks inherent to its business lines, such as the services, website offers, end-users, their transactions, delivery channels used by the bank, geographic locations of the bank's operations, customers, and transactions, as well as other qualitative and emerging risks.

The identification of AML risk categories is based on 737 Exchange Ltd. understanding of regulatory requirements, expectations, and industry guidance. Additional safety measures are taken to cope with the World Wide Web risks.

The EWRA is yearly reassessed.

ONGOING TRANSACTION MONITORING

AML-Compliance ensures that ongoing transaction monitoring is conducted to detect transactions that are unusual or suspicious compared to the customer profile. This transaction monitoring is conducted on three levels:

The first Line of Control:

737 Exchange Ltd. works solely with the trusted Payment Service Providers, all having effective AML policies, aiming to prevent the large majority of suspicious deposit transactions from taking place without proper execution of KYC procedures onto the potential customer.

The second Line of Control:

737 Exchange Ltd. makes its network aware so that any contact with the customer, player, or authorized representative must give rise to the exercise of due diligence on transactions on the account concerned. In particular, these include:

requests for the execution of financial transactions on the account;

requests in relation to means of payment or services on the account.

The three-step verification with adjusted risk management should continuously provide all necessary information about all customers of 737 Exchange Ltd. Furthermore, all transactions must be overseen by employees, overwatched by the AMLCO, who is, in turn, overwatched by the general management.

The specific transactions submitted to the customer support manager, possibly through their Compliance Manager, must also be subject to due diligence. Determination of the unusual nature of one or more transactions essentially depends on a subjective assessment in relation to the completed KYC process, the

user's financial behavior, and the transaction counterparty. These checks are done by an automated system, while an employee cross-checks them for additional security.

The transactions observed on customer accounts for which it is difficult to understand the lawful activities and origin of funds must therefore rapidly be considered atypical (as they are not directly justifiable).

Any 737 Exchange Ltd. staff member must inform the AML division of any atypical transactions they observe and cannot attribute to a lawful activity or known customer's source of income.

The third Line of Control:

As the last line of defense against AML, 737 Exchange Ltd. will do manual checks on all suspicious and higher-risk users in order to fully prevent money laundering.

Please note that in case fraud or money laundering is found, the authorities will be informed.

REPORTING OF SUSPICIOUS TRANSACTIONS AT 737 Exchange Ltd.

In its internal procedures, 737 Exchange Ltd. describes in precise terms, for the attention of its staff members, when it is necessary to report suspicious transactions and how to proceed with such reporting.

Reports of atypical transactions are analyzed within the AML team in accordance with the precise methodology fully described in the internal procedures.

Depending on the result of this examination and based on the information gathered, the AML team:

will decide whether it is necessary or not to send a report to the FIU, in accordance with the legal obligations provided in the Law of 18 September 2017;

will decide whether or not it is necessary to terminate the business relations with the customer.

PROCEDURES

The AML rules, including minimum KYC standards, will be translated into operational guidance or procedures that are available on the intranet site of 737 Exchange Ltd.

Record keeping

Records of data obtained for the purpose of identification must be kept for at least ten years after the business relationship has ended.

Records of all transaction data must be kept for at least ten years following the carrying-out of the transactions or the end of the business relationship.

This data will be encrypted and stored safely offline and online.

Training

737 Exchange Ltd. human employees will make manual controls on a risk-based approval for which they get special training.

Its usage reflects the training and awareness program:

a mandatory AML training program in accordance with the latest regulatory evolutions for all employees who are in touch with finances;

academic AML learning sessions for all new employees.

The content of this training program is established in accordance with the kind of business and the posts the employees hold. These sessions are conducted by an AML-specialist working in the 737 Exchange Ltd. AML team.

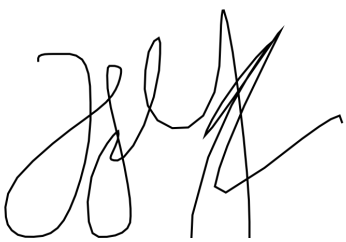
Auditing

Internal audit regularly establishes missions and reports about AML activities.

DATA SECURITY

All data given by any user/customer will be kept secure and will not be sold or given to third parties unless otherwise stated in Privacy Policy. Only if forced by law or in order to prevent money laundering, the data may be shared with the AML-authority of the affected state.

737 Exchange Ltd. will follow all guidelines and rules of the data protection directive (officially Directive 95/46/EC).



Rostyslav Zhmura