AML/CFT Policy

The Anti-Money Laundering, Countering Financing of Terrorism and Know Your Customer Policy (hereinafter - the "AML/CFT Policy") of Microexchange.store is designated to prevent and mitigate possible risks of Microexchange.store being involved in any kind of illegal activity.

Money laundering is defined as

1. the conversion or transfer of property derived from criminal activity or property obtained instead of such property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's actions;
2. the acquisition, possession or use of property derived from criminal activity or property obtained instead of such property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation therein;
3. the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property derived from criminal activity or property obtained instead of such property, knowing that such property is derived from criminal activity or from an act of participation in such an activity.

Money laundering also means participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the activities referred to above.

Terrorist financing is defined as the financing and supporting of an act of terrorism and commissioning thereof as well as the financing and supporting of travel for the purpose of terrorism

Both international and local laws and regulations require Microexchange.store to implement effective internal procedures and mechanisms to prevent money laundering, terrorist financing, drug and human trafficking, proliferation of weapons of mass destruction, corruption and bribery and to take action in case of any form of suspicious activity from its Users.

AML/CFT Policy covers the following matters

- internal controls
- training of personal;
- verification procedures;
- monitoring, risk assessment and risk-based approach;

Internal Controls

We have designed a structured system of internal controls in order to comply with applicable Anti-Money Laundering, Countering Financing of Terrorism (hereinafter - the "AML/CFT") laws and regulations, including, but not limited to:

- establishing customer's identity and verifying the information provided;
- establishing special regime for dealing with customers which are politically exposed persons (PEP);
- the identification of unusual activity and facilitating the reporting of suspicious activity (SAR);

- record keeping of customer documentation and transactional history.

Training

All employees receive a full AML/CFT training, along with a job-specific guidance. Training is conducted at least once every twelve (12) months to ensure that trainees are informed and act in compliance with all applicable laws and regulations. Employees pass additional training if necessary (if new law or regulation is adopted, if required by law, etc.) New employees pass relevant training before commencing to work. Training program is updated regularly to reflect current laws and regulations.

Verification Procedures

Microexchange.store establishes its own customer verification procedures within the standards of AML/CFT frameworks.

Microexchange.store carries out due diligence and KYC checks before entering business relations with customer, client, contractor.

In the process of due diligence and KYC and in order to open an account, person's identity, information about a person provided and documents submitted have to be verified and checked against sanctions and watch lists, including PEP list. Microexchange.store uses special tools, structured system of verification and check for that.

Regarding legal entities (their owners/shareholders/beneficiaries, etc.), Microexchange.store carries out special enhanced due diligence, KYC, compliance procedures.

Microexchange.store ensures specific enhanced identification, KYC, due diligence, compliance procedure for customers referenced as PEP, whatever their place of residence.

Monitoring, risk assessment and risk-based approach

Microexchange.store carries out customer's transactions monitoring, risk-assessment and suspicious activity detection. For that purpose it uses specially developed system, including using a high-performance tools.

Microexchange.store uses risk-based approach to combating/preventing money laundry and/or financing terrorism.

To assist in determining the level of AML/CFT due diligence to be exercised with regard to the customer, a compliance risk profile is calculated first of all on entry into relations (Low, Medium, High), and is then recalculated routinely.

AML/CFT compliance ensures that an ongoing transaction monitoring is conducted to detect transactions which are unusual or suspicious compared to the customer profile.

Determination of the unusual nature of one or more transactions essentially depends on a subjective assessment, in relation to the knowledge of the customer (KYC), their financial behaviour and the transaction counterparty.

If a transaction is inconsistent with a customer's known personal usual activities or personal habits, this transaction may be considered suspicious. Data and transaction monitoring tools are used to identify unusual/uncommon patterns of customer's activity. After review and investigation, it is Compliance Officer's decision whether to file a SAR or not.

Once a SAR is filed with a relevant agency, a copy of filing documentation is maintained. SAR filing is confidential and only the Microexchange.store's employees involved in the investigation and reporting process will be aware of its existence.

All records are retained for no less than (5) years and are available upon official request by an authorized examiner, regulator, or law enforcement agency.

Any Microexchange.store staff member must inform the Compliance Officer of any atypical transactions which they observe and cannot attribute to a lawful activity or source of income known of the customer.