P2P Global Network AML & KYC Policy

Nextchange Limited (the "Company") has established an Anti-Money Laundering and Know Your Customer Policy (hereinafter - the "AML & KYC Policy"), in an attempt to maintain the best compliance practices in conjunction with applicable laws and regulations relating to anti-money laundering in all countries where we operate.

AML & KYC Policy covers the following areas:

- Internal Controls
- Compliance Officer
- Training
- Customer Verification Procedures
- Monitoring of Transactions
- AML Program Audit

Internal Controls

P2P have designed a structured system of internal controls in order to comply with applicable AML & KYC laws and regulations, some of which are outlined in this Policy including, but not limited to, our Customer Verification Procedures, filling Suspicious Activity Reports ("SARs"), as well as other requirements and audits.

Compliance Officer

The Compliance Officer is the person, duly authorised by the Company, whose responsibility is to develop and enforce the effective implementation of the AML & KYC Policy. The Compliance Officer is required to report any violations of the AML & KYC procedures and is responsible for collecting and filing SARs.

Training

All employees receive a full AML & KYC 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. New employees receive relevant training within thirty (30) days of their start date. Training program is updated regularly to reflect current laws and regulations.

Customer Verification Procedures

The Company establishes its own customer verification procedures within the standards of AML & KYC frameworks. In order to open an account, customer's identity and place of residence need to be verified and checked against sanctions and watch lists, including the Office of Foreign Assets Control ("OFAC") and Politically Exposed Persons list ("PEP").

In addition, certain groups of assets are limited to investors with "qualified" status only.

In order to open an account for an individual customer, the following information needs to be verified:

- Email address;
- Mobile phone number;
- Full name;
- Date of birth;
- Proof of identity (government identity card, driver's license, passport);
- Citizenship;
- Proof of residential address (utility bills, bank statement, official government letter); and
- Additional information or documentation if requested.

Monitoring of Transactions

The Company uses customer transaction monitoring as a risk-assessment and suspicious activity detection tool. If a transaction is inconsistent with a customer's known personal activities or personal habits, this transaction may be considered suspicious. Data and transaction monitoring tools are used to identify 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 onsite. SAR filing is confidential and only the Company's employees involved in the investigation and reporting process will be aware of its existence.

All records are retained for eight (8) years and are available upon official request by an authorised examiner, regulator, or law enforcement agency.

AML Program Audit

The Compliance Officer is responsible for conducting AML & KYC audit at least annually. In addition, annual independent test of the AML & KYC procedures is done by a third party. In order to achieve segregation of duties, the Compliance Officer is not responsible for such independent test.