

## Risk Appetite Statement

Date: 24.01.2022

### Introduction

Founded in 2018, Finrax offers cross-border frictionless crypto payment processing, allowing business entities to receive payments in cryptocurrencies for their services. Our Clients can receive deposits in cryptocurrencies without having to worry about volatility, hidden fees or accounting and reconciliation. We solve the hurdles around volatility or slow blockchain transactions and abstract our Clients from the intrinsic complexity associated with the blockchain so that they can run their business the traditional way. We become their bridge between the crypto and the fiat worlds.

Finrax is licensed and adheres to the AML/KYC requirements prescribed by the AML Act and FATF recommendations. Each business entity with whom Finrax does business needs to pass enhanced due diligence procedures before any business operations.

This Statement sets out Finrax's risk appetite and tolerance approach, which is periodically reviewed by the Board of Directors based on a periodic compliance risk assessment that determines the company's compliance, risk tolerance and strategy against money laundering, terrorist financing, sanctions and other related financial crime risks. All strategic plans and business plans for functional areas must comply with this Statement.

### Overview of risk appetite

Finrax manages these compliance risks through detailed processes that emphasize the importance of regulatory standards, professionalism, the maintenance of high-quality personnel and accountability to stakeholders.

Finrax maintains policies designed in full compliance with local and global sanctions laws, AML laws & data protection laws imposed by the Estonian FIU, the international FATF and other relevant authorities. Finrax's anti-money laundering policy highlights our risk assessment process and risk appetite statement.

Finrax has an active and preventive anti-money laundering policy to help stop money laundering attempts and takes appropriate action. Finrax takes a proactive anti-money laundering approach through customer profiling and segmentation to add more analytical information to its monitoring and control process in its periodic risk assessments.

Due to the new trends and changing global compliance environment, Finrax not only manages sanctions, money laundering and terrorist financing risks but also takes into account other risks related to financial crime, such as corruption and bribery risks in its operations.

Finrax is a virtual currency service provider and as such the level of risk for money laundering in this sector is medium and the level of risk for terrorist-financing remains high according to Estonia's 2020 National Risk Assessment Report.

The acceptable levels of risk for Finrax have been described in detail in the supplements to this Statement. Finrax's risk appetite is high with the relevant risks alleviated in accordance with the AML Policy and this Risk Appetite Statement.

### **Monitoring & Reporting**

This Statement is supplemented by the "Customer Risk Assessment Matrix" and "Company Risk Assessment Matrix" in which all risk tolerances are reported to the Compliance Committee and any deviations outside of tolerances are reported to the Board of Directors. Reporting systems are maintained to ensure that risk appetite is effectively incorporated into management decisions. Feedback on the implementation of Finrax's Risk Appetite Statement is provided through the Compliance Committee.

As part of Finrax's AML policy, the Client's activity is monitored for unusual or suspicious patterns, trends or distant transactions that do not match the pre-defined regular behavior. Transactions are often monitored using software that balances activity against a threshold of what is considered "normal and expected". Finrax relies on an internal anti-money laundering control system and utilizes independent 3rd party software. Monitoring is automatic and/or manual by receiving alerts generated by an internal rule-based monitoring system in real-time.

When an illicit transaction is detected, Finrax stops the processing of the said transaction and an internal suspicious activity report (SAR) is created and reviewed by our Compliance Committee. We then request additional documents and information around the case and when necessary the MLRO reports such cases to the regulator.

### **Internal controls**

Finrax's policies, procedures, systems and personnel are designed to prevent the materialization of money laundering risks or to ensure the prompt identification of risk factors. Risk management at Finrax is designed to ensure an effective risk management process in all operations. Risk management is an integral part of all aspects of Finrax's business and is the responsibility of all employees. Managers have a special responsibility to assess their risk environment, put in place the appropriate controls and monitor the effectiveness of these controls. The risk management culture and internal controls emphasize appropriate behavior, analysis and risk management in all business processes.

### **Unacceptable Levels of Risk**

Finrax does not knowingly do business with anyone engaged in criminal activity. In addition, Finrax will not enter into business relationships with prohibited parties, including:

- Exact matches on Sanctions lists
- Exact adverse media matches exposing illegal activities
- Parties that are not transparent in trying to meet the requirements of the AML Policy
- Parties that are not collaborative in providing all the necessary information as required in the AML Policy
- Parties that do not hold the license required to conduct regulated activities
- Parties involved in deceptive marketing practices

The MLRO will work with senior management and the board of directors to conduct a comprehensive review of all relevant customer information to determine the appropriate course of action.

### **Customer risk**

Finrax as a B2B service provider identifies risks related to:

#### Customer profile risk:

The risk level associated with a Client will be determined by their type of business, age of legal entity, group structure complexity and beneficial owners, directors, level of risk of the regulatory bodies, customer reputation, background checks and authorised signatories risk.

#### Geographical risk:

In addition, Finrax identifies the country of incorporation, countries of operations, countries of the controllers and beneficiaries, source and destination directions of money flows and Client's bank accounts locations.

These data are identified to assess the following factors of higher risk, the Client's cross-border activities and global reach (incl. transactions in high risk areas) and the level of difficulty in identifying the source of monetary assets. Geographical risk remains medium/high according to Estonia's 2020 National Risk Assessment Report.

#### Product risk:

Finrax identifies the Client's service description and policies; their AML/CTF measures and onboarding mechanisms; monitors the transaction behavior.

Product risk remains medium/high according to Estonia's 2020 National Risk Assessment Report.

#### Channel/Technology risk:

Finrax makes sure to understand the delivery channels and how funds are accumulated i.e. Internet banking, Blockchain, Fintech applications or others.

These measures are taken to alleviate the higher risks of internet-based service provision, use of cash and virtual currencies enabling anonymity, speed of transactions, possible issues with monitoring systems wherein the monitoring systems may not be able to identify

cashflow with criminal source with high enough efficiency. Channel/technology risk remains medium/high according to Estonia's 2020 National Risk Assessment Report.

Customer risk remains medium/high according to Estonia's 2020 National Risk Assessment Report.

### **Transaction risk**

Due to the nature of services Finrax is offering, and as a result of the global reach in providing a service Finrax could be unwittingly used for the furtherance of financial crime. Finrax must comply with legal requirements to deter and detect financial crime, which includes money laundering and terrorist financing. Therefore we are committed to identifying various transactional risks and applying appropriate measures, such as:

#### Transaction type

Identify if the type of transaction could be used for the purposes of money laundering and identification of the underlying nature of business being conducted.

#### Value of transaction

Identify if the value of the transaction appears to be in concordance with anticipated financial behavior of the customer.

#### Source of funds

Identify if the source of funds is clear and identifiable. Perform Know Your Transaction monitoring via 3rd party independent tools to identify if the crypto assets are connected to bad actors. Is there clear evidence on how funds have been accumulated and does it make commercial sense?

#### Destination of funds

Identify if the transactional behavior matches the money flow declared by the customer. Perform Know Your Transaction checks via 3rd party independent tools to verify if the recipient is legitimate and not connected to illicit activities in the past.

#### Purpose of relationship

Understand the relationship between the customer and its counterparties. Does it make commercial sense given the transaction sizes? Is there supplementary documentation to prove the relationship is legitimate?

Transaction risk remains medium/high according to Estonia's 2020 National Risk Assessment Report.

## **Jurisdiction risk**

By accessing and using the Finrax Website and any of Finrax Services, each Finrax customer declares that they are not on any trade or economic sanctions lists, such as the UN Security Council Sanctions list or OFAC. Finrax maintains the right to select its markets and jurisdictions of operation and may restrict or deny its services to certain countries.

In assessing the jurisdiction risk, Finrax also takes into account the relatively low level of regulation in the area of virtual currencies; the global fragmentation of global regulation in the area of virtual currencies; possible issues in co-operating with regulatory authorities of other states, particularly third states; and lack of area-specific guidelines.

Finrax cannot accept customers that are nationals or residents of a high-risk jurisdiction on the most up-to-date Financial Action Task Force (FATF) list or EU Commission's list of high-risk third countries.

The full list of unaccepted jurisdictions can be found on our website: <https://blog.finrax.com/general-inquiries/unsupported-countries>

Jurisdiction risk remains medium according to Estonia's 2020 National Risk Assessment Report.

## **Industry risk**

Industry risk remains medium/high according to Estonia's 2020 National Risk Assessment Report.

Finrax will not enter into a business relationship with companies operating in the following industries:

- Foreign Shell Banks
- Unregistered Money Service Businesses ("MSBs")
- Bearer shares
- Charities
- Drug Paraphernalia
- Weapons
- Multi-Level Marketing
- Carbon Credits
- Defence/Military
- Explosives
- High-Value Dealers
- Precious Metals
- Pawnbrokers
- Adult Content

Finrax may accept the following restricted industries, after performing Enhanced due diligence measures:

Gaming/Gambling

Forex/CFD brokerage

Payment Service Providers/Money Service Businesses

Loan and Investment companies