Compliance Policy, Anti-Money Laundering (AML), and Counter-Terrorist Financing (CTF) Prevention

FF Soluções Digitais e Financeiras LTDA - FFS
CNPJ: 05.980.434/0001-19

São Paulo, August 8, 2023
Version 2.0.1

Index

1. Introduction

1.1 Purpose of the Manual

The purpose of this manual is to establish guidelines, policies, and procedures for the effective implementation of an Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) program specifically tailored for cryptocurrency intermediation activities. It aims to ensure compliance with Brazilian regulations and applicable international standards, promoting transparency, integrity, and security in operations, as well as protecting FFS (referred to as the company in this manual) against risks associated with money laundering and terrorist financing.

The main objectives of this Manual are:

- Establish a robust compliance program to ensure compliance with national and international laws related to AML and CFT, as well as specific standards related to cryptocurrency intermediation;

- Identify, assess, and mitigate money laundering and terrorist financing risks associated with cryptocurrency operations, seeking to ensure the integrity of the financial system and protect the interests of clients and the company;

- Define appropriate procedures for customer identification and due diligence (KYC), including the verification of their identity and relevant information;

- Establish mechanisms for continuous monitoring of transactions involving cryptocurrencies to detect suspicious patterns and unusual operations;

- Ensure the training and awareness of company employees regarding AML and CFT issues, as well as the importance of compliance with established internal policies and controls;

- Establish an efficient communication channel with relevant authorities to report suspicious or unusual transactions, as required by current legislation;

- Promote a culture of compliance and business ethics, reinforcing the company's commitment to preventing money laundering and countering terrorism, thereby enhancing its reputation in the market.

- This Manual is an integral part of FFS's Compliance Program and must be followed by all employees involved in cryptocurrency intermediation activities, regardless of their hierarchical position. Additionally, the company's senior management is committed to periodically reviewing this Manual, ensuring its compliance with the latest regulations and industry best practices.

1.2 What is AML and CFT?

Anti-Money Laundering (AML) comprises a set of measures, procedures, and controls implemented to prevent illegally obtained funds from being legitimized through financial transactions, concealing their illicit origin. On the other hand, Combating the Financing of Terrorism (CFT) refers to actions aimed at preventing financial assets from being used to finance terrorist activities or terrorist groups.

Financial institutions, including those dealing with cryptocurrencies, play a crucial role in preventing these illicit activities, as they can be exploited by criminals to move and conceal funds. Therefore, it is essential for companies to adopt rigorous AML and CFT policies and procedures to ensure the detection and prevention of suspicious activities.

1.3 Importance of Anti-Money Laundering and Combating the Financing of Terrorism

Money laundering and terrorism financing pose significant threats to the integrity of the financial system and society at large. These practices can be used to support criminal activities and destabilize global security. The implementation of an effective AML and CFT program is crucial to protecting the company's reputation, complying with legal obligations, and contributing to the security and stability of the financial market.

1.4 Scope of the Manual

This manual applies to all cryptocurrency intermediation activities carried out by the company, covering everything from the acquisition and trading of cryptocurrencies to the provision of related services, such as custody and trading on behalf of clients. All areas of the company involved in these activities must adhere to the policies and procedures described in this document, ensuring compliance with regulatory guidelines and national and international best practices in AML and CFT. It is important for all employees and third parties involved in these operations to be aware and committed to promoting the prevention and combating of illicit practices.

1.5 Cryptocurrencies and Intermediation

Cryptocurrencies are digital assets that use cryptography and distributed ledger technology (blockchain) to ensure transaction security and data integrity. These assets function as a medium of exchange, unit of account, or store of value and can be used for various purposes, including investments, payments, and project financing.

The most well-known cryptocurrencies include Bitcoin, Ethereum, and Algorand. However, there are many other types of cryptocurrencies, including utility tokens (representing access to a product or service) and security tokens (representing ownership or stakes in companies).

Cryptocurrency intermediation is the process by which companies and financial institutions facilitate the buying, selling, exchanging, and storing of these digital assets. This activity can be carried out through various platforms and services, such as exchanges, currency houses, digital wallets, and trading platforms.

Due to the digital and decentralized nature of cryptocurrencies, intermediation of these assets presents specific risks related to money laundering, terrorism financing, and financial fraud. Cryptocurrency transactions can be conducted quickly, easily cross international borders, and, in some cases, offer a certain degree of anonymity. These characteristics may attract criminals seeking to conceal or move illicit funds.

1.5.1 Key Characteristics

- Decentralization: Cryptocurrencies are not controlled by financial institutions or central governments. Instead, their issuance and validation are carried out through cryptographic protocols and consensus mechanisms involving a network of distributed computers.

- Anonymity and Pseudonymity: Cryptocurrency transactions can be conducted relatively anonymously, as users do not need to reveal their real identities. Instead, they use digital addresses (public keys) for transactions, providing a level of pseudonymity to operations.

- Security: Cryptocurrency transactions are protected by encryption, making operations secure and resistant to fraud and counterfeiting.

- Transparency: All cryptocurrency transactions are recorded in a public ledger known as the blockchain. This ledger is accessible to anyone and allows verification and tracking of transactions.

- Scarcity and Mining: Most cryptocurrencies have a limited quantity of units that can be created, giving them a scarcity characteristic. The creation of new units, in many cases, is done through the mining process, involving the solving of complex computational problems.

1.5.2 Importance of Understanding

For the effective fulfillment of AML and CFT obligations in cryptocurrency intermediation, it is crucial that all company employees understand the nature and functioning of cryptocurrencies, as well as their peculiarities compared to traditional fiat currencies. This understanding will enable the company to adopt appropriate procedures to mitigate money laundering and terrorism financing risks associated with the use of cryptocurrencies..

1.5.3 Types of Cryptocurrencies

The company deals with various types of cryptocurrencies in its intermediation operations. Below are the main types of cryptocurrencies supported by the company:

- Cryptocurrencies (e.g., Bitcoin, Ethereum, Ripple, Algorand, Cardano, etc.)
- Utility Tokens (e.g., Chainlink, BAT, CRO, etc.)
- Security Tokens (Representing real estate value)
- Stablecoins (e.g., USDT - Tether, USDC - USD Coin, DAI, etc.)
- Non-Fungible Tokens (e.g., NFTs)
- Governance Tokens (e.g., Maker, Compound, Uniswap, etc.)
- Tokens of Specific Platforms (e.g., EOS, Tezos, Tron, etc.)

1.5.4 Functioning of Cryptocurrencies and Blockchain

- Blockchain: Blockchain is a distributed ledger technology consisting of a chain of blocks containing transaction information. Each block is connected to the previous one through encryption, forming an immutable and transparent chain of data. Blockchain is the foundation of many cryptocurrencies and offers various advantages, such as security, decentralization, and transparency.

- Cryptocurrency Transactions: Cryptocurrency transactions are recorded on the blockchain and are public, allowing anyone to verify the validity and history of a transaction. Each transaction is digitally signed to ensure the authenticity and security of operations.

- Public and Private Keys: To conduct cryptocurrency transactions, users use a pair of cryptographic keys: a public key and a private key. The public key, also known as the wallet

address, is shared with others so they can send cryptocurrencies to the user. The private key, on the other hand, is kept secret and is used to digitally sign transactions and authorize the sending of cryptocurrencies.

- Mining: In many cryptocurrencies, such as Bitcoin, the process of validating transactions and creating new blocks is carried out by miners. Miners are network participants who use computational power to solve complex mathematical problems. When a miner solves a problem, they can create a new block and receive cryptocurrency rewards for their work.

- Consensus: Blockchain technology uses consensus mechanisms to ensure that all network participants agree on the correct version of the ledger. Different cryptocurrencies use different consensus algorithms, such as Proof of Work (PoW) used by Bitcoin, Proof of Stake (PoS) used by Ethereum, among others.

- Smart Contracts: Smart contracts are self-executing programs stored on the blockchain and automatically executed when certain conditions are met. They enable the creation of digital agreements and contracts without the need for intermediaries, making transactions faster and more efficient.

1.6 Principles and International Standards

1.6.1 Financial Action Task Force (FATF)

The Financial Action Task Force (FATF), established in 1989 by G7 countries, is an intergovernmental organization aiming to combat money laundering and terrorism financing. FATF develops and promotes policies and international standards to strengthen the integrity of the global financial system and protect it against exploitation by criminals and terrorists.

FATF's recommendations are widely recognized as the international standard for implementing effective AML/CFT measures. These recommendations are based on three fundamental pillars:

- Risk identification and assessment: Countries and financial institutions must identify and assess money laundering and terrorism financing risks in their respective jurisdictions and sectors to develop effective strategies to mitigate these risks.

- Implementation of preventive measures: Financial institutions and entities subject to AML/CFT laws must implement appropriate policies and procedures to identify, verify, and monitor their clients, as well as detect and report suspicious activities to competent authorities.

- Establishment of a robust legal and regulatory framework: Countries must adopt laws, regulations, and other measures to criminalize money laundering and terrorism financing, establish effective sanctions for these crimes, and ensure cooperation between national and international authorities.

In June 2019, FATF issued specific guidelines for the regulation and supervision of activities related to cryptocurrencies, including the intermediation of these assets. These guidelines state that companies involved in cryptocurrency intermediation must be subject to the same AML/CFT obligations as other financial institutions, such as banks and brokerages.

1.6.2 FATF Standards for Cryptocurrencies

In response to the growth and development of the cryptocurrency market and the recognition of associated risks with money laundering and terrorism financing, FATF issued specific guidelines to regulate and supervise activities involving cryptocurrencies. These guidelines aim to ensure the integrity of the global financial system and protect cryptocurrency markets from exploitation by criminals and terrorists..

Key recommendations from FATF for cryptocurrencies include:

- Definition of cryptocurrencies and Virtual Asset Service Providers (VASPs): FATF defines cryptocurrencies as digital or virtual assets that use cryptography and distributed ledger technology (blockchain) to ensure transaction security and data integrity. Virtual Asset Service Providers (VASPs) are companies or individuals engaging in intermediary activities, such as buying, selling, exchanging, transferring, and storing cryptocurrencies.

- Regulation and supervision of VASPs: Countries must implement a legal and regulatory framework to license, register, and supervise VASPs, ensuring these entities comply with AML/CFT requirements. This includes applying the same preventive measures required for traditional financial institutions, such as Know Your Customer (KYC) procedures, transaction monitoring, and reporting suspicious activities.

- Implementation of AML/CFT measures for VASPs: VASPs must adopt effective AML/CFT policies and procedures, including customer identification and verification, risk assessment and management, continuous transaction monitoring, and reporting suspicious activities to competent authorities.

- International cooperation and information exchange: Countries must ensure cooperation between national and international authorities to combat money laundering and terrorism

financing in the cryptocurrency sector. This includes exchanging information about VASPs and their clients, as well as mutual assistance in investigations and legal proceedings.

- Sanctions and punitive measures: Countries must establish effective and proportionate sanctions for VASPs that fail to comply with AML/CFT requirements, including fines, suspension or revocation of licenses, and, in severe cases, criminal actions.

1.6.3 International Cooperation

International cooperation is a key element in the fight against money laundering and terrorism financing, especially in the context of cryptocurrencies, which can be rapidly transacted and easily cross borders. Collaboration between countries, regulatory authorities, law enforcement agencies, and financial institutions is essential to share information, identify emerging trends, and develop effective strategies to combat these crimes.

Key aspects of international cooperation in the field of AML/CFT include:

- Exchange of information between authorities: National authorities must establish effective mechanisms to share relevant information about money laundering, terrorism financing, and other illicit activities related to cryptocurrencies. This may include creating focal points, contact networks, and information-sharing platforms to facilitate cooperation and coordination among authorities..

- Legal mutual assistance and extradition: Countries must implement treaties and bilateral or multilateral agreements allowing legal mutual assistance and the extradition of criminals involved in money laundering and terrorism financing. This may include cooperation in investigation, evidence collection, asset confiscation, and prosecution of cases related to cryptocurrencies.

- Capacity building and training: International cooperation should also involve the sharing of knowledge, experiences, and best practices in the field of AML/CFT. This may include conducting training programs, workshops, and seminars to strengthen the skills and competencies of authorities, financial institutions, and other relevant actors in the fight against money laundering and terrorism financing.

- Adherence to and implementation of international standards: Countries must adhere to and implement international standards established by the Financial Action Task Force (FATF) and other relevant organizations, such as the World Bank and the International Monetary Fund (IMF), to ensure consistency and effectiveness of AML/CFT measures globally.

- Participation in international forums and initiatives: Countries should actively participate in forums and international initiatives related to AML/CFT, such as the International Conference on Anti-Money Laundering and Asset Recovery, the Global Initiative for Financial Transparency, and the Global Partnership against Money Laundering. This participation allows the exchange of ideas, identification of common challenges, and the development of cooperative solutions to address global threats of money laundering and terrorism financing.

References

- Financial Action Task Force on Money Laundering and Terrorist Financing (GAFI/FATF) - www.fatf-gafi.org
- Central Bank of Brazil (BCB) - Financial Stability Department - www.bcb.gov.br/estabilidadefinanceira
- Financial Activities Control Council (COAF) - www.gov.br/coaf
- Brazilian Federation of Banks (Febraban) - www.febraban.org.br
- International Compliance Association (ICA) - www.int-comp.org
- Brazilian Cryptoeconomics Association (ABCripto) www.abcripto.com.br
- Brazilian Legislation Portal - http://www4.planalto.gov.br/legislacao/
- Regulation Normative Instruction RFB N° 1888/2019
- GOMES, R. C.; SAADI, R. A. Organized Crime – Money Laundering. Brasília: National Police Academy, 2008.
- ROMANTINI, G. L. Institutional Development of Money Laundering Combat in Brazil since Law 9613/98.
- UNODC – UNITED NATIONS OFFICE ON DRUGS AND CRIME. Money Laundering Globalization.
- BIO, S. R.; CORNACHIONE JUNIOR, E. B. Information Systems – A Managerial Approach. 2nd ed. São Paulo: Atlas, 2008.

2. Regulatory Framework

2.1 Applicable Brazilian Legislation

The intermediation of crypto-assets in Brazil is subject to a specific set of regulations aimed at protecting the financial system and combating crimes such as money laundering and the financing of terrorism. The main applicable Brazilian laws and regulations include:

2.1.1 Law No. 9,613/1998 - Money Laundering Law

Establishes money laundering crimes and mandates reporting to competent authorities regarding suspicious transactions.

2.1.2 Law No. 12,683/2012

Amends provisions of the Money Laundering Law and establishes additional measures for the prevention and combating of terrorism financing.

2.1.3 CVM Instruction No. 617/2019

Regulates public offerings of distribution of securities, including crypto-assets, and establishes transparency and compliance requirements for related activities.

2.1.4 CVM Instruction No. 497/2011

Addresses the constitution, administration, operation, and disclosure of information regarding investment funds, including those investing in crypto-assets.

2.1.5 CVM Instruction No. 555/2014

Regulates private equity investment funds (FIP), which may invest in assets such as crypto-assets.

2.1.6 Normative Instruction RFB No. 1888/2019

Institutes and regulates the obligation to provide information on operations conducted with crypto-assets to the Special Secretariat of the Federal Revenue of Brazil (RFB).

2.2 Relevant International Standards

In addition to national legislation, it is important to consider relevant international standards that establish global guidelines for preventing money laundering and combating the financing of terrorism. Some of the main standards include:

2.2.1 FATF Recommendations (Financial Action Task Force)

FATF is an international organization that defines recommendations for combating money laundering, terrorism financing, and the proliferation of weapons of mass destruction. FATF recommendations are widely adopted by various countries.

2.2.2 European Union Directives (EU)

For companies conducting business with the EU or EU citizens, it is relevant to observe European directives on money laundering prevention, which also align with FATF recommendations.

2.3 Regulatory Bodies and Supervisory Entities

In Brazil, the intermediation of crypto-assets is regulated and supervised by specific entities. Some of the main ones are:

2.3.1 Brazilian Securities and Exchange Commission (CVM)

Responsible for regulating, supervising, and overseeing activities related to securities, including investment funds involving crypto-assets.

2.3.2 Central Bank of Brazil (BCB)

BCB acts in the control and supervision of the financial system, and its regulations are important for institutions operating with crypto-assets.

2.3.3 Financial Activities Control Council (COAF)

COAF is responsible for receiving, examining, and identifying suspicious occurrences of illicit activities and reporting them to the competent authorities.

2.3.4 Brazilian Federal Revenue (RFB)

The Brazilian Federal Revenue (RFB) plays a crucial role in the supervision and taxation of operations involving crypto-assets.

3. Risk Profiles

3.1 Identification of Customer Profiles

The proper identification of customer profiles is a crucial element in preventing money laundering and terrorist financing. In this regard, the company establishes procedures for collecting information and analyzing each client, identifying their characteristics, and the purpose of transactions. Customer profile classification can be based on criteria such as transaction volume, nature of activities, source of funds, and the region of origin or destination of transactions.

3.2 High-Risk Customers

Recognizing high-risk customers is a crucial aspect of an effective AML and CFT program. Customers with specific characteristics, such as politically exposed persons (PEPs), offshore companies, or those in high-risk jurisdictions.

3.3 Risk Factors for Crypto-Asset Activities

Operations involving crypto-assets have unique aspects and specific risks for AML and CFT. Price volatility, ease of fund transfer, and potential anonymity offered by some cryptocurrencies can facilitate money laundering and terrorist financing. Therefore, the company must identify and assess these risk factors to develop appropriate strategies and controls.

3.4 Continuous Monitoring of Risk Profiles

An efficient AML and CFT program requires continuous monitoring of customer risk profiles throughout the business relationship. This involves implementing systems and technologies that enable the detection of unusual behavioral patterns or suspicious transactions. Continuous monitoring is essential to identify potentially illicit activities, trigger appropriate investigations, and report suspicious transactions to the relevant authorities as needed.

3.5 Definition of Operational Limits

To mitigate the risk of money laundering, the company establishes limits for transactions involving crypto-assets, especially those with High-Risk customers or considered atypical operations. These limits help prevent unjustified or disproportionate financial movements.

3.5.1 Individual below US$ 10,000.00 per month or equivalent in local currency

Background check, verification against sanctions lists such as OFAC, active registration with the federal revenue service, submission of documents, self-assessment, and proof of address.

3.5.2 Individual above US$ 10,000.00 per month or equivalent in local currency

The same as item 3.5.1 + income tax declaration or proof of financial capacity.

3.5.3 Legal Entity below US$ 65,000.00 per month or equivalent in local currency

Background check, verification against sanctions lists such as OFAC, active registration with the federal revenue service, articles of association, submission of documents from partners, self-assessment, and proof of address.

3.5.4 Legal Entity above US$ 65,000.00 per month or equivalent in local currency

The same as item 3.5.3 + revenue declaration, balance sheet / income tax declaration.

3.5.5 Legal Entity as a digital account, payment institution/company selling crypto on its app or platform

The same as item 3.5.4, and we limit to US$ 10,000.00 per month per CPF (SSN) (of its customers) submitted with the request in our request book, a digital assets intermediation contract where it commits to following the same practices as outlined in this manual. All CPFs (SSNs) undergo our background check, verification against sanctions lists such as OFAC, active registration with the federal revenue service, and date of birth.

4. Know Your Customer (KYC), Know Your Employee (KYE), Know Your Partner (KYP), Know Your Supplier (KYS), and Know Your Wallet (KYW).

4.1 Know Your Customer (KYC)

The Know Your Customer (KYC) process is an essential component of the Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Prevention program. It involves the collection, verification, and continuous updating of information about the company's customers to understand their identity, the source of funds, and the purpose of transactions. KYC plays a

crucial role in risk mitigation and combating illicit activities, allowing the identification of high-risk customers and the detection of suspicious transactions.

The customer information collection process, also known as Know Your Customer (KYC), involves obtaining detailed data about the customer's identity, including name, address, date of birth, identification number, among others. Additionally, it is important to gather information about the nature of the customer's activities and the source of funds used in crypto-asset transactions. This information enables the company to assess the customer's risk profile and determine whether they fall into high-risk categories that require additional due diligence measures.

We adopt different levels of verification and document requests as per item 3.5 Definition of Operational Limits.

The entire onboarding process must go through our platform.

4.1.1 Politically Exposed Person (PEP)

An individual who holds or has held high-level political positions or has a close relationship with such individuals, posing additional risks due to the potential for political influence. The company does not engage with this customer profile.

4.3 Know Your Employee (KYE)

The company's Know Your Employee (KYE) process aims to thoroughly understand its employees and assess their integrity and compliance with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) policies. This is done through comprehensive information collection, reference checks, and criminal background checks. The company also maintains a conflict of interest policy and provides periodic AML-CTF training to raise awareness among employees about their obligations. KYE is an important measure to mitigate internal risks and ensure a safe and trustworthy working environment..

4.4 Know Your Partner and Supplier (KYP and KYS)

The company's Know Your Partner (KYP) process aims to thoroughly understand its partners and suppliers and assess their integrity and compliance with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) policies. This is done through detailed information collection about partners, including their market reputation, business history, and legal compliance. The company also checks for connections with individuals or entities involved in illicit or high-risk

activities. KYP is an important measure to mitigate risks associated with business partnerships and ensure that the company is involved in legitimate and ethical transactions.

4.5 Know Your Wallet (KYW)

The company's Know Your Wallet (KYW) process is of utmost importance to ensure that the company does not receive crypto-assets from wallets associated with criminal activities, fraud, hacks, or those on blacklists.

Through KYW, the company collects detailed information about customer crypto-asset transactions, verifying the wallets used, transaction origin and destination addresses, as well as transaction history analysis. This allows the identification of suspicious patterns and unusual transactions, mitigating risks associated with transactions involving illicitly sourced crypto-assets.

Additionally, KYW involves the use of risk analysis tools and compliance with international sanctions lists and blacklists. This ensures that the company is not involved in transactions with wallets associated with sanctioned individuals or entities or engaged in illicit activities.

By diligently performing KYW, the company reinforces its commitment to compliance with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) regulations. This practice contributes to protecting the company's reputation, avoiding risks of involvement in illegal activities, and strengthening the integrity and trust of the crypto-asset market.

Furthermore, by identifying suspicious or illegitimate transactions during the KYW process, the company can report suspicious operations to relevant authorities and regulatory bodies, contributing to the overall security of the crypto-asset intermediation sector.

Therefore, KYW is a fundamental measure to ensure the ethics and legality of the company's operations, protecting it against risks of involvement in illicit activities and contributing to a safe and transparent working environment.

4.6 Customer Information Update Procedure

The procedure aims to maintain accurate customer information. The update is done annually and can be requested by compliance at any time. The company's digital platform is used, along with possible additional information via email. Confidentiality is ensured to protect data against unauthorized access. The process is vital for financial and regulatory integrity, requiring continuous collaboration from customers.

5. Transaction Monitoring

5.1 Detection of Suspicious Transactions

Transaction monitoring is a crucial step in preventing money laundering and combating terrorist financing. The company must implement suitable systems and technologies to continuously monitor operations involving crypto-assets. Detecting suspicious transactions involves analyzing unusual behavioral patterns or atypical activities that may indicate money laundering or terrorist financing. All deposits made into the company's accounts must exclusively come from the registered origin accounts of our customers, with proper verification of ownership corresponding to the registration..

5.2 Monitoring Criteria

Transaction monitoring criteria are defined based on a comprehensive and up-to-date risk analysis. The company establishes indicators and alerts that identify transactions exceeding certain value limits, occurring in high-risk regions, countries, or jurisdictions, or involving customers classified as high-risk. Additionally, transactions showing unusual patterns, such as multiple small transfers in short time intervals or large volumes of crypto-assets moved without clear justification, should also be subject to special monitoring.

5.3 Tools and Technologies Used

For effective transaction monitoring, the company employs advanced tools and technologies, including real-time data analysis systems, artificial intelligence algorithms, and machine learning. These technologies can help identify complex patterns and suspicious behaviors, enabling faster and more accurate detection of high-risk transactions. Furthermore, the integration of monitoring systems with external databases, such as sanctions lists and politically exposed persons, is also crucial to enhance monitoring effectiveness.

5.4 Investigation and Reporting of Suspicious Transactions

Upon identifying suspicious transactions, the company must conduct in-depth internal investigations to assess the veracity of the suspicions. If illicit activity is confirmed, the company must prepare detailed reports on suspicious operations and report them to the relevant authorities, as required by current legislation. Prompt and accurate communication of suspicious transactions is essential to support authorities in investigating criminal activities and combating money laundering and terrorist financing.

6. Suspicious Transaction Reports

6.1 Procedures for Reporting Suspicious Operations

Employees involved in transaction monitoring are trained to recognize signs of illicit activities and are aware of the procedures to follow when encountering suspicious transactions. The accurate and timely identification and reporting of suspicious operations are crucial to support authorities in the investigation and prevention of financial crimes.

6.2 Communication with Regulatory Bodies

The company must be prepared to establish effective communication with regulatory bodies and supervisory entities responsible for anti-money laundering and counter-terrorist financing prevention. This includes submitting reports on suspicious operations and promptly responding to information requests from authorities. Maintaining a collaborative and transparent relationship with regulatory bodies is essential to ensure compliance with legal obligations and demonstrate the effectiveness of the company's AML program.

6.3 Secrecy and Confidentiality

Reports on suspicious operations must be treated with the highest degree of secrecy and confidentiality. Unauthorized disclosure of this information can hinder ongoing investigations, jeopardize the safety of the company's clients and employees, and compromise the institution's reputation. Therefore, the company establishes strict measures and controls to ensure that reports on suspicious transactions are accessed only by authorized personnel and that information is shared strictly in accordance with legal and regulatory requirements.

The effective reporting of suspicious operations is a fundamental pillar in the company's AML program. By implementing clear procedures and adequately training employees, the company reinforces its commitment to combating money laundering and terrorist financing, actively collaborating with competent authorities to ensure the safety and integrity of the financial system and the crypto-asset market.

7. About Responsibilities

7.1 Responsibilities of Senior Management:

The senior management of the company has the primary responsibility to ensure the effective implementation and adherence to Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Prevention policies and procedures. This includes a commitment to a compliance culture, providing adequate resources for the AML program, and ensuring that the objectives of preventing and detecting illicit activities are achieved.

7.2 Responsibilities of the AML Department:

The AML Department is responsible for developing, implementing, and maintaining the company's AML policies and procedures. Additionally, it is responsible for conducting due diligence on customers, partners, and suppliers, monitoring transactions for suspicious activities, and reporting suspicious operations when necessary. The department must also provide regular training and awareness for all employees involved in crypto-asset intermediation activities.

7.3 Responsibilities of Employees:

All employees of the company have the responsibility to comply with established AML policies and procedures. This includes the proper collection of information from customers, partners, and suppliers, verifying their compliance with applicable regulations, and reporting any suspicious or atypical activities to the AML Department. Employees must also participate in periodic training and awareness to ensure ongoing understanding of AML policies and procedures.

7.4 Responsibilities of the Compliance and Internal Audit Department:

The Compliance and Internal Audit Department is responsible for periodically reviewing the effectiveness of the company's AML policies and procedures. This includes conducting internal audits, verifying compliance with regulations, and identifying areas for improvement. The Compliance Department is also responsible for keeping the company informed about changes in AML laws and regulations.

7.5 Responsibilities of the Legal Department:

The Legal Department is responsible for providing legal guidance related to the company's crypto-asset intermediation activities. This includes reviewing contracts, policies, and AML procedures to ensure compliance with applicable laws and regulations. The Legal Department must also assist in responding to any requests from authorities and regulatory bodies related to investigations or audits.

7.6 Responsibilities of the Human Resources Department:

The Human Resources Department is responsible for ensuring that all employees are properly informed about their obligations regarding AML policies and procedures. This includes providing adequate training and maintaining training records. The Human Resources Department is also responsible for ensuring that proper selection, hiring, and training processes are implemented to ensure that employees have the necessary skills to fulfill their responsibilities related to AML.

8. Internal Policies and Procedures.

8.1 AML Policy

The company must develop and implement a clear and comprehensive internal Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Prevention policy. This policy should reflect the company's commitment to complying with applicable national and international regulations and establish specific guidelines for crypto-asset intermediation activities. The AML policy should cover all stages of the customer and transaction lifecycle, from initial information collection to continuous monitoring and reporting of suspicious operations. Additionally, it should define the responsibilities and obligations of employees regarding AML.

8.2 Crypto-Asset Compliance Policies

Due to the specific nature of crypto-asset operations, it is important for the company to establish specific compliance policies for this market. This includes guidelines for verifying the origin and authenticity of crypto-assets, preventing fraudulent activities related to cryptocurrencies, and establishing criteria for the inclusion or exclusion of certain crypto-assets from the company's operations. Crypto-asset compliance policies should align with current regulations and be regularly reviewed and updated to adapt to changes in the regulatory and technological landscape.

8.3 Internal Control Procedures

The company must implement rigorous internal control procedures to ensure compliance with AML policies. This includes appointing an AML officer who will be the focal point for AML-related issues and conducting periodic reviews of processes and controls to ensure their effectiveness. It is also important to establish effective internal communication mechanisms to disseminate information about new regulations, identified risks, and best practices in the field of AML.

8.4 Documentation and Record-Keeping

All procedures, decisions, and measures related to AML must be properly documented and recorded. This includes transaction records, suspicious transaction reports, training records, updates to policies and procedures, among others. Maintaining comprehensive and organized documentation is essential for audit purposes, demonstrating compliance to regulatory authorities, and protecting the company in case of future investigations or disputes.

9. Audit and Review of AML Program

9.1 Internal Audits

The company must conduct periodic internal audits to assess the effectiveness and compliance of its Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Prevention program. Audits are performed by independent and objective professionals who review the company's procedures, controls, and policies related to AML. This detailed analysis helps identify any potential flaws and areas for improvement in the program, thereby promoting continuous enhancements.

9.2 Policy and Procedure Review

AML legislation and regulations are constantly evolving, as is the crypto-asset market landscape. For this reason, it is crucial for the company to regularly review its AML policies and procedures to ensure they comply with the latest legal requirements and are effective in mitigating risks. The review should be conducted by experts and take into account the evolution of best practices and recommendations from regulatory authorities.

9.3 Simulation Tests (Crisis Simulation)

In addition to audits and reviews, the company can also conduct crisis simulation tests to assess the responsiveness of the AML program in emergency situations. These tests simulate money laundering or terrorist financing scenarios, allowing the company to evaluate how its teams react and respond to such situations. The results of the tests are used to identify potential vulnerabilities in the program and enhance crisis response procedures.

9.4 Continuous Improvements

Based on the results of audits, reviews, and simulation tests, the company should implement continuous improvements to its AML program. These improvements may include updating policies and procedures, enhancing transaction monitoring systems, conducting additional training for the team, among other measures. The goal is to constantly refine the program and ensure that it remains effective and compliant with applicable regulations.

10. Conclusion and Commitment to AML

10.1 Company Commitment

Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) are issues of utmost importance for the company, its clients, and the entire financial system. In this manual, we have presented the best Brazilian and international practices related to AML, especially tailored for crypto-asset intermediation activities. By following these guidelines, the company reinforces its commitment to the integrity, transparency, and security of operations in the crypto-asset market.

10.2 Responsibility of All

The effectiveness of the AML program depends on the commitment of all employees of the company. Each team member plays a crucial role in identifying and preventing illicit activities. It is the responsibility of everyone to be aware of the established policies and procedures, and to rigorously fulfill their obligations regarding AML.

10.3 Continuous Improvements

AML and CFT are dynamic areas that are constantly evolving to adapt to changes in financial markets and emerging threats. For this reason, the company is committed to conducting regular reviews and continuous improvements to its AML program. This will ensure that practices and controls are up-to-date and capable of mitigating the latest risks.

10.4 Collaboration with Authorities

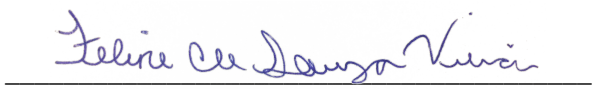
The company also reaffirms its commitment to fully collaborate with regulatory authorities and supervisory entities whenever necessary. Reporting suspicious transactions and transparent communication with competent bodies are essential to strengthen the security of the crypto-asset market and contribute to the prevention and combating of illicit activities.

10.5 Protection of Customers and the Company

By implementing a robust AML program, the company seeks to protect not only its own interests but also those of its clients. Preventing money laundering and combating the financing of terrorism are essential pillars to ensure the trust and security of clients in their crypto-asset operations.

10.6 Appreciation

Finally, the company expresses gratitude to all employees who contributed to the development of this manual and acknowledges the importance of collective effort in building a safer and more transparent financial environment. The ongoing commitment to AML is a reflection of the company's dedication to ethics, compliance, and responsibility in business.



Felipe de Souza Vieira

São Paulo, August 8, 2023