# ANTI-FRAUD POLICY

PayNox EOOD

ID number: 208071994

Legal address: Bulgaria, City of Burgas, 19 Marahydyk St., fl. 2, office 1

# Table of Contents

# INTRODUCTION

Fraud poses a significant threat to financial institutions, including cryptocurrency exchanges, leading to financial losses, regulatory penalties, and reputational damage. This Anti-Fraud Policy establishes a comprehensive framework to prevent, detect, and respond to fraudulent activities, ensuring compliance with legal and regulatory requirements.

The policy applies to all customers, employees, contractors, and third-party service providers interacting with the platform. It outlines the measures taken to safeguard the platform from fraudulent transactions, identity theft, and insider threats while maintaining a secure and transparent financial ecosystem.

By implementing robust fraud detection tools, strict customer due diligence (CDD) procedures, and a risk-based approach, this policy helps mitigate fraud risks, ensuring the integrity of our platform and protecting users from financial crime.

# DEFINITIONS

To ensure clarity and consistency, the following key terms are defined:

Fraud: Any intentional act of deception, misrepresentation, or omission carried out to gain an unlawful financial or personal advantage.

Identity Fraud: The use of stolen, fake, or falsified personal information to create or access accounts.

Account Takeover (ATO): Unauthorized access to a user's account through hacking, phishing, or credential theft, often used for fraudulent transactions.

Transaction Fraud: Unauthorized or deceptive transactions, including chargeback abuse, fake payments, and money laundering.

Crypto Fraud: The misuse of cryptocurrency to disguise illicit activities, such as using mixers, tumblers, chain-hopping, or privacy coins to obscure fund origins.

Insider Fraud: Fraud committed by employees, contractors, or vendors, including misusing company resources, insider trading, or collusion with external parties.

Risk-Based Approach: A compliance strategy that prioritizes fraud prevention efforts based on the level of risk posed by customers, transactions, and jurisdictions.

Sanctions Screening: The process of checking individuals and entities against global watchlists (e.g., OFAC, UN, FATF) to ensure compliance with sanctions regulations.

Whistleblower: An employee or third party who reports fraudulent activities or compliance violations through confidential reporting mechanisms.

## PURPOSE

The purpose of this Anti-Fraud Policy is to establish a robust framework for preventing, detecting, and responding to fraudulent activities within the organization. By implementing strict controls, advanced monitoring systems, and clear reporting mechanisms, this policy aims to:

Protect the Integrity of the Platform – Ensure the security and transparency of all transactions by preventing fraudulent activities such as identity theft, money laundering, and unauthorized access.

Ensure Regulatory Compliance – Adhere to global financial regulations, including AML/CFT laws, sanctions screening requirements, and fraud prevention standards.

Safeguard Customers and Stakeholders – Protect users, employees, and business partners from financial losses, reputational damage, and security risks caused by fraudulent activities.

Promote a Fraud-Resistant Culture – Educate employees, customers, and third parties on fraud risks and encourage ethical behavior and accountability.

Enhance Risk Management – Utilize a risk-based approach to identify and mitigate fraud risks effectively while ensuring proactive compliance monitoring.

By enforcing this policy, the organization strengthens its ability to detect and prevent fraud, ensuring a secure and compliant financial ecosystem.

## SCOPE

This Anti-Fraud Policy applies to all individuals and entities involved in the operations of the organization, covering a wide range of activities to ensure fraud prevention and compliance.

This policy applies to:

- All personnel working for or on behalf of the organization must adhere to fraud prevention measures.
- Individuals or entities using the platform for cryptocurrency transactions must comply with anti-fraud policies.
- External partners, payment processors, and technology providers must align with the organization’s fraud prevention standards.

The policy covers:

- Verification processes to prevent identity fraud and financial crimes.
- Real-time tracking of activities to identify suspicious behavior, including unauthorized access, money laundering, and chargeback fraud.

- Safeguards against internal fraud, including misuse of company assets, insider trading, and unauthorized fund transfers.
- Implementation of Two-Factor Authentication (2FA), encryption, and blockchain analytics to prevent hacking and account takeovers.
- Clear procedures for reporting, investigating, and escalating fraud incidents.

This policy applies to all financial activities, transactions, and operational processes within the organization, ensuring a secure, compliant, and fraud-resistant environment.

## CORE PRINCIPLES

The following core principles guide the organization's approach to fraud prevention, detection, and response:

- Fraudulent activities will not be tolerated under any circumstances.
- Any individual or entity found engaging in fraud will face strict disciplinary actions, legal consequences, and possible account restrictions or termination.
- Fraud prevention efforts are prioritized based on risk levels, with enhanced scrutiny on high-risk users, transactions, and jurisdictions.
- Continuous risk assessments ensure that fraud detection measures evolve with emerging threats.
- Advanced AI-driven fraud detection systems monitor transactions and user behavior in real time.
- Strong Know Your Customer (KYC) and Customer Due Diligence (CDD) protocols prevent identity fraud and unauthorized access.
- Blockchain analytics tools are used to track and flag suspicious cryptocurrency transactions.
- The organization adheres to global Anti-Money Laundering (AML), Counter-Terrorist Financing (CFT), and sanctions screening regulations.
- Compliance teams regularly update fraud prevention measures to align with OFAC, FATF, EU, and other regulatory bodies.
- Employees, customers, and third parties are encouraged to report suspected fraud through secure and anonymous channels.
- Whistleblowers are protected from retaliation to foster a culture of transparency and accountability.
- Regular employee training programs enhance fraud awareness and detection skills.
- Internal audits and compliance reviews ensure the effectiveness of fraud prevention controls.

By upholding these core principles, the organization maintains a secure, transparent, and fraud-resistant platform while ensuring regulatory compliance and customer protection.

## CUSTOMER FRAUD

To identify, prevent, and mitigate fraudulent activities committed by customers, ensuring the integrity of the platform and compliance with regulatory standards.

Use of stolen, fake, or synthetic identities to create accounts.

Misrepresentation of personal or business information during Know Your Customer (KYC) verification.

Unauthorized access to customer accounts through hacking, phishing, or credential theft.

Exploitation of weak security measures to manipulate transactions or withdraw funds.

Unauthorized payments or chargeback abuse to exploit refund policies.

Wash trading and price manipulation to create artificial market activity.

Use of privacy coins, mixers, tumblers, or chain-hopping to obscure transaction origins.

Deposits and withdrawals structured to evade transaction monitoring thresholds.

Participation in Ponzi schemes, scams, or fraudulent Initial Coin Offerings (ICOs).

Customers pretending to be legitimate users or support agents to deceive others.

Fraudulent claims of lost access or unauthorized transactions to recover funds illegitimately.

*Strict KYC & Customer Due Diligence (CDD):*

- Multi-level identity verification with AI-powered fraud detection.
- Screening against sanctions lists and Politically Exposed Persons (PEP) databases.

*Advanced Transaction Monitoring & Risk Scoring:*

- Real-time blockchain analytics to detect high-risk transactions.
- AI-based fraud detection to flag suspicious patterns.

*Strong Account Security Measures:*

- Mandatory Two-Factor Authentication (2FA).
- Behavioral biometrics to detect anomalous login activities.

*Automated Fraud Alerts & Reporting Mechanisms:*

- Immediate account restrictions for suspicious activities.
- Secure and anonymous fraud reporting channels for users and employees.

*Consequences of Customer Fraud*

- Immediate account suspension or termination for verified fraud cases.
- Freezing of funds linked to fraudulent activities.
- Regulatory reporting to authorities (e.g., FinCEN, FATF, OFAC).
- Permanent bans from the platform for repeated violations.

By implementing these fraud detection and prevention measures, the organization ensures a secure, compliant, and trustworthy financial ecosystem.

## INTERNAL AND EMPLOYEE FRAUD

To prevent, detect, and address fraudulent activities committed by employees or insiders, ensuring the organization's integrity and compliance.

Insider Trading: Misuse of confidential company or customer data for personal gain.

Bribery & Corruption: Accepting kickbacks, unauthorized incentives, or engaging in unethical practices.

Misuse of Funds: Unauthorized transfers, fund misallocation, or asset theft.

Data Manipulation & Misrepresentation: Altering records, reports, or compliance documents for fraudulent purposes.

Collusion with External Parties: Assisting external fraudsters in bypassing security measures.

Fraud Prevention Measures

Strict Access Controls: Limited and role-based system access.

Transaction & Activity Monitoring: AI-driven tools to detect suspicious behavior.

Whistleblower Protection: Secure, anonymous reporting channels for fraud concerns.

Regular Audits & Compliance Reviews: Routine checks to prevent financial misconduct.

Mandatory Employee Training: Awareness programs on fraud risks and ethical conduct.

Consequences of Internal Fraud

Immediate termination for fraudulent activities.

Legal action for financial or regulatory violations.

Regulatory reporting to relevant authorities.

By enforcing these measures, the organization ensures a transparent, ethical, and fraud-resistant workplace.

## THIRD-PARTY AND VENDOR FRAUD

To prevent and address fraudulent activities by third-party service providers, vendors, and business partners, ensuring compliance and protecting company assets.

Types of Third-Party & Vendor Fraud

- Contract Fraud: False invoicing, overbilling, or misrepresenting services.
- Collusion & Kickbacks: Unethical agreements between employees and vendors for personal gain.
- Service Manipulation: Delivering substandard or incomplete services while charging full fees.
- Misuse of Company Data: Unauthorized access, sharing, or exploitation of sensitive information.

Fraud Prevention Measures

- Vendor Due Diligence (VDD): Background checks before onboarding vendors.
- Contract Audits & Compliance Reviews: Regular monitoring of vendor agreements and transactions.
- Automated Fraud Detection: AI-based monitoring for suspicious payment patterns.
- Whistleblower & Reporting Channels: Secure reporting mechanisms for fraud concerns.

*Consequences of Vendor Fraud*

- Termination of contracts and blacklisting of fraudulent vendors.
- Legal action for financial misconduct or regulatory violations.
- Reporting to authorities for severe breaches.

By enforcing strict controls, the organization ensures transparent and fraud-resistant vendor relationships.

## FRAUD PREVENTION MEASURES

To effectively combat fraudulent activities, the organization implements a multi-layered fraud prevention strategy that integrates advanced technology, strict security protocols, and regulatory compliance. At the core of this strategy is Customer Due Diligence (CDD) and Know Your Customer (KYC) procedures, ensuring that all users

undergo thorough identity verification. AI-powered tools and global sanctions screening help detect high-risk individuals and prevent unauthorized access to the platform.

Real-time transaction monitoring and risk scoring play a crucial role in identifying suspicious activities. The organization utilizes AI-driven analytics and blockchain tracking tools to detect anomalies, such as rapid fund movements, structured transactions, or connections to illicit activities. Automated alerts flag high-risk transactions, allowing for swift investigation and response.

To enhance security, the platform enforces strong account protection measures, including mandatory Two-Factor Authentication (2FA) and behavioral biometrics to detect unauthorized access attempts. Encryption and advanced cybersecurity protocols further safeguard user data, reducing the risk of breaches and fraud.

Internally, employee fraud prevention is reinforced through strict role-based access controls, ensuring that sensitive information is only accessible to authorized personnel. Regular audits and compliance reviews help detect insider fraud, while mandatory fraud awareness training ensures employees remain vigilant against fraudulent activities.

Third-party risks are also addressed through vendor due diligence and ongoing contract audits. Before onboarding any vendor, the organization conducts background checks and ensures compliance with fraud prevention standards. Service agreements include strict terms to prevent false invoicing, overbilling, or data misuse.

The organization fosters a transparent reporting culture by maintaining secure whistleblower channels for employees and customers to report fraud anonymously. All reports undergo a structured internal review process, and whistleblowers are protected from retaliation

To stay ahead of emerging fraud threats, the organization continuously updates its fraud prevention framework in line with global Anti-Money Laundering (AML), Counter-Terrorist Financing (CFT), and sanctions screening regulations. Collaboration with regulatory authorities and law enforcement agencies ensures compliance and enhances the platform's ability to combat financial crime effectively.

By integrating these fraud prevention measures, the organization ensures a secure, compliant, and fraud-resistant environment for all users.

## REPORTING AND ESCALATION

The organization maintains a structured and transparent reporting and escalation process to ensure that fraudulent activities are identified, investigated, and addressed

promptly. This framework enables employees, customers, and third parties to report suspicious activities securely while ensuring proper escalation for swift action.

All fraud-related concerns can be reported through designated internal channels, including confidential reporting systems, whistleblower hotlines, or direct escalation to compliance officers. Customers and external parties can submit fraud reports via secure online forms, email, or customer support channels. Reports must include relevant details such as the nature of the suspicious activity, involved parties, and supporting evidence where applicable.

Once a fraud report is received, the compliance and fraud investigation teams conduct an initial risk assessment to determine the severity and potential impact. Low-risk cases may be handled internally through enhanced monitoring and user verification, while high-risk incidents—such as large-scale fraud, identity theft, or regulatory violations—are escalated to senior management and relevant legal authorities.

For internal fraud involving employees or vendors, the organization follows a strict internal review process, ensuring that investigations remain confidential while adhering to labor laws and corporate policies. If necessary, access to sensitive systems may be restricted during the investigation to prevent further risks.

Regulatory compliance is a key component of fraud reporting. Any fraudulent activity that meets reporting thresholds under AML, CFT, or financial crime regulations is promptly reported to the relevant authorities, such as OFAC, FinCEN, FATF, or local law enforcement. In cases of severe fraud, the organization may also cooperate with law enforcement agencies for further legal action.

To maintain transparency and accountability, all fraud cases are documented, and periodic fraud risk reports are reviewed by senior leadership to assess trends, identify weaknesses, and improve fraud prevention strategies. By enforcing a robust reporting and escalation process, the organization ensures swift action against fraud while maintaining compliance with regulatory requirements.

## COMPLIANCE AND CONTINUOUS IMPROVEMENT

The organization is committed to maintaining strict regulatory compliance and continuously enhancing its fraud prevention measures to adapt to evolving risks. Compliance with global Anti-Money Laundering (AML), Counter-Terrorist Financing (CFT), and sanctions screening regulations is a fundamental aspect of fraud prevention. The organization ensures adherence to standards set by regulatory bodies such as FATF, OFAC, FinCEN, and EU AML directives, conducting regular audits and compliance reviews to detect potential vulnerabilities.

To strengthen fraud prevention, the organization employs a risk-based approach, continuously assessing fraud threats based on transaction patterns, customer profiles,

and jurisdictional risks. Advanced AI-driven monitoring systems and blockchain analytics are regularly updated to enhance detection capabilities, ensuring that new fraud techniques are identified and mitigated effectively.

Employee training and awareness programs play a crucial role in compliance efforts. Regular fraud prevention workshops, compliance training, and simulated fraud scenarios ensure that staff members remain vigilant against emerging fraud risks. Employees are required to stay informed about regulatory updates, internal policies, and reporting obligations.

The organization also promotes continuous improvement by analyzing fraud trends, conducting post-incident reviews, and incorporating feedback from fraud investigations. Lessons learned from past cases are used to refine internal policies, enhance security measures, and improve fraud detection techniques. Collaboration with regulatory authorities, industry partners, and cybersecurity experts further strengthens the organization's ability to proactively combat financial crime.

By integrating compliance and continuous improvement, the organization ensures a secure, adaptive, and fraud-resistant financial environment, safeguarding both its customers and stakeholders.

## CONCLUSION

In conclusion, the organization’s Anti-Fraud Policy is designed to establish a robust framework that prevents, detects, and addresses fraudulent activities across all levels of its operations. By adhering to global regulatory standards, leveraging advanced technologies, and fostering a culture of integrity, the organization ensures a secure, transparent, and compliant environment for its customers, employees, and partners.

The policy emphasizes a proactive approach, using risk-based assessments, automated fraud detection systems, and comprehensive employee training to safeguard against fraud. Whether it involves customer fraud, employee misconduct, or third-party vendor fraud, the organization is committed to swift detection, thorough investigation, and appropriate escalation of incidents.

Continuous improvement is at the heart of this policy, with ongoing updates to fraud prevention measures, compliance practices, and detection capabilities. Through regular audits, feedback, and collaboration with regulators and industry leaders, the organization ensures it remains adaptable in the face of evolving fraud risks.

By maintaining a zero-tolerance policy toward fraud and prioritizing transparency, accountability, and ethical behavior, the organization upholds its commitment to protecting its assets, customers, and reputation. Ultimately, this policy contributes to a secure financial ecosystem where trust and compliance are central to its operations.