PayBitoPro

Firm's Fraud Policy

(UAE)

Created by:	Avisek Banerjee
Approved by:	Soumendu Roy
Documentation Version:	4.5
Submission Date:	14th Jan, 2025

CONTENTS

INTRODUCTION

In today's fast-evolving financial landscape—particularly within the digital asset and crypto markets—payments fraud remains one of the most significant and persistent threats to organizations of all sizes and across every industry sector. The complexity of payment infrastructures, the emergence of novel financial technologies, and the increasing sophistication of fraud schemes have amplified the risks facing treasury operations, compliance teams, and digital financial service providers.

At PayBitoPro, the integrity and security of our payment and transaction systems are paramount. Fraudulent activity can result in serious financial losses, reputational damage, regulatory penalties, and erosion of customer trust. Therefore, implementing a comprehensive, dynamic, and enforceable fraud policy is critical not only for mitigating financial risk but also for preserving the credibility of our platforms and protecting our stakeholders.

This policy has been developed with input from industry benchmarks and modeled in part after effective frameworks utilized by multinational financial institutions, with reference to standards provided by the Association for Financial Professionals (AFP). It aims to serve as a practical and strategic tool for safeguarding against fraud, reinforcing a company-wide culture of vigilance, accountability, and regulatory compliance.

1. PURPOSE

Fraud undermines the integrity, trust, and stability of financial systems, including cryptoasset platforms such as PayBitoPro. This policy outlines PayBitoPro's commitment to proactively prevent, detect, report, and respond to all forms of fraud, including those overlapping with money laundering and terrorism financing. All employees, customers, vendors, and stakeholders are expected to uphold these standards and report any suspected fraud.

2. POLICY

PayBitoPro adopts a zero-tolerance approach toward fraud, bribery, corruption, and dishonest conduct. The organization will:

a. Investigate all reported suspicions or evidence of fraud or corruption.

b. Take disciplinary, legal, and regulatory action where appropriate.

c. Enforce internal controls and compliance programs that mitigate fraud risk.

d. Comply with applicable laws including the Proceeds of Crime Act 2002 and MLR 2017.

3. DEFINITIONS

a. ***Fraud:*** Any intentional act or omission designed to deceive, manipulate, or circumvent laws, policies, or controls for unlawful gain or to cause loss.
Examples include:

i. Misappropriation of funds, tokens, or cryptoassets.

ii. Forgery or falsification of documents or transactions.

iii. Manipulating KYC/CDD or AML processes.

iv. Collusion between employees and customers to bypass security or compliance procedures.

b. ***Corruption:*** Includes bribery, extortion, and conspiracy to influence decisions for personal or third-party gain, especially in relation to government or regulatory matters.

c. **Proliferation Financing Fraud:** Use of crypto-related products to finance the development or distribution of weapons of mass destruction.

4. RESPONSIBILITIES

a. **All Employees:** Required to report suspected fraud to the Compliance Department without delay.

b. **Management:** Accountable for implementing fraud controls within their teams and reporting irregularities.

c. **Compliance Department:** Oversees fraud policy enforcement, training, investigations, and regulatory reporting.

d. **Money Laundering Reporting Officer (MLRO):** Coordinates fraud reporting and ensures regulatory compliance.

5. PROCEDURES

a. ***Prevention:***

i. Implement robust KYC/CDD and name screening protocols as part of AML/CTF compliance.

ii. Conduct employee and third-party due diligence (vendors, partners, suppliers).

iii. Use transaction monitoring, blockchain analytics, and wallet screening to detect suspicious crypto activity (e.g., mixers, DeFi scams, high-risk exchanges).

iv. Provide regular training to all staff on fraud awareness and response procedures.

b. ***Monitor for red flags, including:***

i. Unusual or unexplained transactions.

ii. Use of privacy coins, mixers, or DEXs to obscure sources.

iii. Clients resisting verification or CDD procedures.

iv. Employees demonstrating undue influence or avoiding internal controls.

c. ***Reporting:***

i. All suspicions must be escalated to the MLRO or Compliance Officer.

ii. STRs (Suspicious Transaction Reports) must be filed within two business days.

iii. Tipping-off is strictly prohibited.

***d. Investigation*:**

i. Investigations are led by the Compliance Department with access to all necessary internal records.

ii. External auditors or legal counsel may be engaged where appropriate.

iii. Investigation outcomes are documented and shared with senior management and, where applicable, the Board or Audit Committee.

e. Corrective Action:

i. May include employee dismissal, criminal prosecution, restitution claims, or regulatory notification.

ii. Enforcement is consistent regardless of employee seniority or role.

6. EXCEPTIONS

There are no exceptions to this policy. All suspected incidents of fraud must be addressed in accordance with this document.

7. REGULATORY REQUIREMENTS

a. Applicable anti-money laundering and anti-corruption laws and regulations in the relevant jurisdiction

b. Regulations related to money laundering, terrorist financing, and transfer of funds, as applicable in the relevant jurisdiction

c. Relevant regulatory or supervisory authority guidelines and rulebooks

d. FATF Recommendations and other international best practice standards

8. RELATED FORMS

a. Fraud Policy Acknowledgment Form

b. STR Reporting Template

c. Whistleblower Complaint Form

d. Risk Assessment Checklist