PayBitoPro

Safeguard Policy

(UAE)

Created by:	Avisek Banerjee
Approved by:	Suchismita Chakrabarti
Documentation Version:	4.7
Submission Date:	16th Jan, 2025

CONTENTS

1. Introduction

PayBitoPro is committed to the highest standards of customer protection and financial integrity. This Safeguarding Policy outlines the framework and principles for protecting customer funds, personal data, and the interests of vulnerable users. The policy supports our obligations under applicable regulatory requirements and industry best practices.

This policy ensures that client assets are segregated from the firm's own assets and that all operational, financial, and data handling practices are aligned with safeguarding obligations.

2. Safeguarded Clients Covered by the Policy

This policy applies to all:

a. Individual customers (retail and professional),

b. Corporate clients (non-individuals),

c. Vulnerable customers (e.g., those with mental capacity limitations, financial distress, or language barriers),

d. Third-party beneficiaries or counterparties where services or assets are held in trust or transacted on their behalf.

3. Responsibilities

a. **<u>The Board of Directors is responsible for:</u>**

i. Establishing a governance framework for safeguarding;

ii. Ensuring client fund segregation protocols are in place and audited;

iii. Approving the annual safeguarding audit report;

iv. Ensuring business continuity and financial resilience plans are maintained.

b. **<u>The MLRO / Chief Compliance Officer is responsible for:</u>**

i. Monitoring adherence to this policy;

ii. Reporting breaches or safeguarding failures to the appropriate authority;

iii. Coordinating internal and external audits;

iv. Overseeing risk assessments related to client fund management and vulnerable client interaction.

c. **<u>Finance and Operations Teams are responsible for:</u>**

i. Executing client fund segregation procedures;

ii. Monitoring reconciliation and accounting practices;

iii. Preventing the commingling of firm and customer funds.

d. **<u>All Employees are responsible for:</u>**

i. Complying with this policy;

ii. Reporting concerns or anomalies under the Whistleblowing Procedure;

iii. Completing annual safeguarding and AML training.

4. Policy Context

As a cryptoasset service provider, PayBitoPro operates in a high-risk environment where customer assets and data are vulnerable to misuse. We recognize our duty to:

a. Comply with safeguarding principles for client money and cryptoassets;

b. Promote transparent and ethical handling of customer funds;

c. Ensure systems are in place to prevent abuse, exploitation, or harm to any customer, particularly those in vulnerable circumstances.

5. Key Safeguarding Principles

a. **<u>Segregation of Client Funds:</u>**

PayBitoPro ensures strict separation of customer assets from its own funds:

i. Client fiat and cryptoasset funds are held in designated segregated accounts or wallets.

ii. These accounts are clearly titled and managed under trust principles, ensuring they are ring-fenced from insolvency claims or creditor actions.

iii. No firm operational or treasury funds are held in client accounts.

b. **Regular Reconciliation and Controls:**

i. Daily reconciliation of client accounts against transaction ledgers and custody systems.

ii. Automated alerts are in place for balance discrepancies or unauthorized access attempts.

iii. Monthly internal reviews and quarterly independent reconciliations are conducted.

c. **Safeguarding Vulnerable Customers:**

Aligned with relevant regulatory guidance:

i. Staff are trained to recognize indicators of vulnerability.

ii. Enhanced support and escalation procedures are in place for those facing financial hardship, cognitive challenges, or exploitation.

iii. Communication materials and customer interactions are designed with accessibility in mind.

6. Partner and Vendor Responsibilities

PayBitoPro requires all third-party service providers, including custodians, payment processors, and KYC vendors to:

a. Adhere to this Safeguarding Policy and applicable safeguarding standards;

b. Maintain clear segregation of client assets where applicable;

c. Include safeguarding commitments in their contracts with PayBitoPro.

7. Incident Management Procedure

All safeguarding breaches or anomalies must be reported immediately to the MLRO. This includes:

a. Unauthorized access to customer funds;

b. Delays in reconciling segregated accounts;

c. Suspected financial abuse or exploitation of a customer.

An incident log is maintained, and critical incidents are reported to the appropriate authority within 24–48 hours in line with regulatory obligations.

8. Reporting Safeguarding Breaches

a. **<u>Safeguarding concerns may be reported by:</u>**

i. Internal whistleblowing;

ii. Transaction monitoring alerts;

iii. Customer complaints.

b. **<u>All such reports are investigated by Compliance. Outcomes may involve:</u>**

i. Filing a Suspicious Activity Report (SAR);

ii. Initiating customer protection measures;

iii. Disciplinary action or partner contract termination.

9. Preventative Controls and Monitoring

To ensure compliance with this policy:

a. Safeguarding controls are reviewed quarterly by internal audit;

b. An annual safeguarding audit is conducted by an independent external auditor;

c. Continuous monitoring systems track account balance thresholds and client movement patterns.

10. Training and Awareness

a. All staff undergo safeguarding training during onboarding and annually thereafter.

b. Specific training is provided to teams in direct contact with clients (e.g., customer service, onboarding).

c. Staff are assessed on knowledge of fund segregation and vulnerability indicators.

11. Recordkeeping and Data Security

a. All safeguarding records, including reconciliations, training logs, and partner attestations, are maintained for a minimum of five years.

b. Systems handling customer data and funds are protected through access controls, encryption, and multi-factor authentication.

12. Review and Policy Governance

This Safeguarding Policy is:

a. Reviewed annually by the Head of Compliance and MLRO;

b. Updated in line with changes to applicable regulations, the PSRs, or PayBitoPro's business model;

c. Presented to the Board for approval and then communicated firm-wide.