PayBitoPro

Account Takeover (ATO) Prevention and Response Policy

(United States of America)

Created by:	Avisek Banerjee
Approved by:	Souhardya Sarkar
Documentation Version:	4.3
Submission Date:	10th Jan, 2025

CONTENTS

1. Introduction

Account Takeover (ATO) fraud is a critical cybersecurity risk where malicious actors gain unauthorized access to a legitimate user's account. At PayBitoPro, prevention, detection, and response to ATO attempts are integrated into our broader cybersecurity and data protection frameworks.

This policy outlines the technical, procedural, and operational safeguards implemented to mitigate ATO risks and outlines escalation and response procedures in the event of a compromise.

2. Objectives

a. Prevent unauthorized access to user accounts.

b. Protect client funds and sensitive personal data.

c. Detects ATO attempts in real-time through automated and manual means.

d. Establish clear protocols for response and user recovery.

e. Ensure compliance with the GDPR, applicable data protection regulations, and relevant guidelines.

3. Scope

This policy applies to:

a. All registered users of PayBitoPro's platform (web and mobile);

b. Internal users (admin and customer service);

c. Contractors and API integrators;

d. All systems responsible for identity, access, and authentication.

4. Risk Identification and Monitoring

a. **<u>PayBitoPro deploys layered detection systems to identify potential ATO threats:</u>**

i. Device fingerprinting, IP reputation checks, and login pattern analysis.

ii. Real-time Intrusion Detection Systems (IDS) to flag abnormal access attempts.

iii. Geo-velocity logic to detect impossible travel or location inconsistencies.

iv. Monitoring for SIM-swapping, credential stuffing, brute-force attempts, and phishing behavior.

b. **<u>High-risk triggers include:</u>**

i. Login from new device or unusual location;

ii. Repeated failed login attempts;

iii. Sudden change in user behavior (e.g., withdrawal patterns);

iv. Update requests to key credentials (email, phone, 2FA settings).

5. Prevention Controls

***a.* <u>Multi-Factor Authentication (MFA):</u>**

i. All users must enable MFA using TOTP (Time-Based One-Time Password) or biometric verification (for mobile users).

ii. High-value transactions or account changes require step-up authentication (e.g., MFA re-verification).

***b.* <u>Secure Authentication Standards:</u>**

i. Passwords are hashed using a crypt and salted.

ii. Login endpoints are rate-limited and protected via CAPTCHA.

iii. Sessions expire after 15 minutes of inactivity.

***c.* <u>Device and IP Whitelisting:</u>**

i. Users can whitelist trusted devices and locations.

ii. Sensitive actions trigger alerts when accessed from unrecognized environments.

6. User Awareness and Training

a. Security awareness notifications (e.g., login alerts) are sent in real-time.

b. Educational content about phishing, password hygiene, and social engineering is available in the user dashboard.

c. Support staff receive periodic training to identify and triage ATO attempts.

7. Detection and Verification Mechanisms

When an ATO event is suspected:

a. The system flags the account for review and locks sensitive functions (withdrawals, API access).

b. The user is prompted to complete identity verification, including biometric selfie and document revalidation.

c. Internal analysts review session logs and behavioral patterns.

8. Incident Response and User Recovery

a. **<u>If an ATO is confirmed:</u>**

i. Immediate Account Lockdown to prevent fund movement.

ii. User Notification via registered email and alternate contact methods.

iii. Re-verification Protocol involving ID documents, face match, and security questions.

iv. Audit and Report:

1. All sessions terminated;

2. A case file generated;

3. A SAR (Suspicious Activity Report) may be filed if needed.

b. **<u>If funds were moved:</u>**

i. Transaction freeze or rollback initiated (if applicable);

ii. Engagement with legal and regulatory bodies as required.

9. Data Privacy and Confidentiality

Per the GDPR and the Data Protection Act 2018:

a. All account activity logs, ATO reports, and communications are securely retained for five years.

b. Personal data obtained during investigations is encrypted, pseudonymized, and access-restricted.

c. No data is shared externally without lawful basis, regulatory demand, or user consent.

10. Technical Safeguards

Based on IT and Security Policy (Sections S5, S6, S10):

a. Encryption at rest and in transit using TLS 1.3 and AES-256.

b. Security Event and Incident Monitoring (SIEM) integration with behavioral analytics.

c. Endpoint protection on admin and customer service devices.

d. Periodic vulnerability scans and penetration tests.

11. Redress and Escalation

Users who believe their accounts have been compromised can:

a. Use the "Report Suspicious Activity" link on the login page;

b. Contact 24/7 support or email security@paybitopro.com;

c. Request a formal ATO review from the Data Protection Officer (DPO) or MLRO.

All complaints are handled under our Complaints Handling Policy aligned with relevant standards.

12. Partner and API Integrator Responsibilities

All partners or vendors with system-level access must:

a. Adhere to PayBitoPro's cybersecurity standards;

b. Use encryption and secure authentication for any user-level API actions;

c. Report any observed ATO incidents within 24 hours.

13. Logging, Auditing, and Policy Review

a. All account activities are logged and stored securely for audit and compliance purposes.

b. This policy is reviewed semi-annually by the CISO and MLRO.

c. Critical updates are approved by the Board and communicated via internal training and platform notifications.

14. Enforcement and Penalties

a. Any internal failure to follow this policy may result in disciplinary action.

b. Regulatory breaches involving compromised accounts are reported in accordance with applicable guidance and data breach protocols.