Schedule 3

PayBitoPro

Transaction Monitoring Procedure

Document Type	Document Owner	Written By	Date
Procedure	Compliance	Rohan Gupta	May 15, 2022

Table of contents

1. Purpose

The purpose of this Procedure is to comply with the PayBitoPro FCC Statement, as well as relevant laws and regulations in the countries PayBitoPro operates. This Procedure represents how PayBitoPro mitigates the ML/TF risk via Transaction Monitoring.

PayBitoPro has designed a set of TM Rules to flag out abnormal transactions. This Procedure demonstrates how PayBitoPro monitors ongoing abnormal activities and requires pre-approval or permissioning in some scenarios to reduce risk arising from PayBitoPro' s services and products.

2. Role and Responsibility

The Cybersecurity Team is in charge of designing a robust system of platforms to monitor the customer's transactions and activities via services provided.

Investigators shall review the reports generated and alerts triggered by the system and determine the appropriate course of action to be taken. For example, regarding high-risk transactions, Investigators have to approve the customer's transaction order or escalate certain cases to the Head of Compliance.

The Head of Compliance is the Money Laundering Reporting Officer (MLRO) and shall regularly review this Procedure to consider its appropriateness, and shall provide support and advice to other functions timely and appropriately. In the event of any suspicious transaction, the MLRO shall file a Suspicious Transaction Report (STR) to the regulatory authority of the countries PayBitoPro operates.

3. Continuous Monitoring

Given some suspicious activities are not easily detected in the short term or period, accumulation monitoring is created to understand the behaviors of some customers.

The customers who have higher transaction volume or frequency shall be reviewed monthly and quarterly to ensure consistency to the CDD and KYC profiling.

4. Watch List

PayBitoPro has designed a Watch List to monitor transactions by specific customers to mitigate the ML/TF risk arising from abnormal transaction activities.

Customers approved by the KYC team may be placed on the Watch List when the KYC team identifies behaviors that point to associations with potentially higher risk activities.

Transactions by the customers on the Watch List shall be monitored periodically, and the Investigator shall make a record after completing each transaction monitoring review.

Depending on the higher risk factors identified, customers on the Watch List will be further classified into three levels to be reviewed in accordance with the rules below respectively :

(1) Level A: Customers with more than two higher risk factors (such as PEPs, adverse media, and from high-risk industries) or transactions PayBitoPro deems necessary to be reviewed; post-transaction review per week;

(2) Level B: Customers with two higher risk factors (e.g. PEPs, in high-risk industries) shall be reviewed transactions per month;

(3) Level C: Customers with one higher risk factor (e.g. adverse media) shall be reviewed transactions per quarter.

With regard to the details of the investigation process and STR, please refer to paragraphs 7 and 8 below.

On an exception basis, customers may be removed from the Watch List or have their level of monitoring downgraded should the following criteria be met:

(1) Level A: no alerts hit or no abnormal activities found more than 18 months and approved both by the Head of Compliance and CEO;

(2) Level B: no alerts hit or no abnormal activities found more than 18 months and approved by the Head of Compliance;

(3) Level C: no alerts hit or no abnormal activities found more than 12 months and approved by the Head of Compliance.

5. Purposes of Red Flags

To prevent the misuse of virtual assets and funds for financial crime and terrorism, transaction monitoring rules are designed by developing red flags indicators to strengthen control in accordance with the detection targets below:

(1) Monitoring transferral in large amounts of value or in high frequency without justifiable reasons;

(2) Preventing any individual from using PayBitoPro's service or product on behalf of another principal;

(3) Detecting Inconsistent IP address login without justifiable reasons;

(4) Identifying transaction regarding sanctioned and high-risk countries imposed by the UN, EU, FATF, OFAC, HMT;

(5) Identifying high-risk VASPs (virtual asset service providers) and E-wallets.

6. Red Flags Categories

PayBitoPro designs the red flags by two groups:

(1) transaction-based triggers and;

(2) non-transaction-based triggers.

The first category of transaction-based triggers is a red flag based on transaction timing, either pre-transaction, real-time, and post-transaction (e.g., monthly accumulated trading volume).

The second category of non-transaction-based triggers means a red flag based on all other factors, including but not limited to multiple IP addresses a user uses within a short period, the type crypto or fiat used in a transaction.

7. Investigation Process

The Investigator shall initiate the investigation process while the alerts are triggered.

Pre-approval by the Investigator or any equivalent role might be required if the transactionhits some risk types.

The Investigator is in charge of reviewing alerts triggered and taking action required according to scenarios faced immediately after the alert is triggered.

As an alert triggered, the Investigator shall immediately evaluate whether it is indeed a suspicious activity and take actions pursuant to the case as necessary. For example:

(1) To check the profile of the customer in the system

(2) To refer to the transaction history in the system

(3) To talk to a sales or employee who knows the customer

(4) To collect more information or documents from the customer via the KYC team

An investigation report shall be initiated if the concern can not be removed to close the alert triggered in a reasonable time. The Investigator shall input actions taken into the report and provide relevant information and documents to the Head of Compliance.

The Re-KYC mentioned in the Know Your Customer (KYC) and Customer Due Diligence (CDD) Procedure might be triggered if necessary.

8. Suspicious Activity

To comply with the requirements of AML/CTF, all employees shall report to the Head of Compliance or line manager while finding any suspicious activity.

Activities below are not exhaustive but show suspicious situations:

(1) Transactions that are unusual and unexpected in comparison with the previous trading volumes, especially in previously dormant accounts.

(2) Transaction amounts that are not commensurate with the evidence of wealth provided by customers.

(3) IP address logged in to various countries within a short period.

While the Investigator detects any suspicious activity and takes appropriate action accordingly, relevant information and documents shall be provided to the Head of Compliance to determine what further actions to take.

Filing a suspicious transaction report (STR) to the regulatory authority is required when the Head of Compliance determines the concern of suspicious activity can not be removed. For more details, please refer to the **Suspicious Transaction Report ("STR") Procedure.**