PayBitoPro

Transaction Monitoring (Travel Rule) Policy

(AUSTRALIA)

JUNE 2024

TABLE OF CONTENTS

- **Introduction**

The Transaction Monitoring policy of PayBitoPro underscores the company's dedication to combating money laundering, terrorism financing, proliferation financing, financing for weapons of mass destruction (WMDs) and related illicit activities. It outlines the measures implemented to prevent users from exploiting its services for criminal purposes, aligning with pertinent Australia's laws such as the Anti-Money Laundering and Counter-Terrorism Financing Act 2006, Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007, The Criminal Code Act 1995 (Criminal Code) and other relevant regulations. PayBitoPro has developed this policy to ensure trading transparency and to safeguard against terrorism financing and unlawful practices.

In this Policy "we", "us", "our" means PayBitoPro and the terms "user", "individuals", "non-individuals" means the residents of Australia and the business enterprises registered in Australia under the Corporations Act, 2001.

The Transaction Monitoring Policy is uniformly applicable to all Users intending to utilize the Services or gain advantages from the Online Platforms of PayBitoPro, constituting an integral element of the User Terms and Conditions. Before engaging with the Online Platforms or divulging any personal information, it's imperative to thoroughly examine this Transaction Monitoring Policy. Your use of the Online Platforms implies your explicit acknowledgment and adherence to the User Terms and Conditions and, consequently, this Transaction Monitoring Policy.

- **Purpose**

The purpose of this policy is to set out how PayBitoPro is complying with the laws of Australia and how PayBitoPro is carrying out the business and operation. PayBitoPro follows the procedures of transaction monitoring mentioned in this policy for the purpose of mitigating the Money Laundering (ML) / Terrorist Financing (TF) risks[1].

PayBitoPro has designed a set of Transaction Monitoring (TM) rules which are implemented to recognize / identify abnormal or suspicious transactions. This policy demonstrates how PayBitoPro performs ongoing monitoring of the activities of the users of PayBitoPro.

Some of the actions of the users require pre-approval or permissions on some transactions to reduce the potential risk which might arise from PayBitoPro's services and products.

- **Roles and Responsibility**

PayBitoPro acts as Cryptoasset Exchange Provider which facilitates the customers with a variety of services. Keeping in mind the risks of the nature of the business PayBitoPro has some responsibilities in regards to the Anti-Money Laundering and Counter-Terrorism Financing Act 2006, Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007, ensures

[1] Section 15.4-15.7 of Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007

that the individuals / non-individuals are restricted from exploiting the services provided by PayBitoPro.

For the purpose of monitoring the transactions made by the customers, PayBitoPro has different teams with different roles and responsibilities which are as follows:

1. The Cybersecurity Team: the cybersecurity team of PayBitoPro has been given the responsibility of designing a robust system of platforms to monitor the transactions made by the customers and all the activities of the user of the services provided by PayBitoPro.

2. Investigators: the investigators have the responsibility to review the reports generated as well as review the alerts triggered by the system of PayBitopro. The investigators shall determine the appropriate course of action after the review, which is to be taken. For an instance, the transaction having the potential of being a high-risk transaction ($10,000 or above), the investigators shall approve the customer's transaction order or escalate the matter to the compliance department.

3. The Head of Compliance: the head of the compliance department is the Money Laundering Reporting Officer (MLRO) and it is the duty / responsibility of the officer to regularly review this policy and consider its appropriateness. It is also the responsibility of the MLRO to provide support and advice to other teams timely and appropriately. In the event of any suspicious activity / transactions the MLRO shall file a Suspicious Transaction Report (STR)[2] or a Suspicious Activity Report (SAR) to the regulatory authorities which is, Australian Transaction Reports and Analysis Centre (AUSTRAC)

[2] Part 3, Division 2, Section 41 of Anti-Money Laundering and Counter-Terrorism Financing Act 2006

- **Continuous Monitoring**

Provided that, suspicious activities are not easily detected within a short period of time, PayBitoPro follows the rule of continuous monitoring of the accounts / activities / transactions to understand the behaviour of the customers. This procedure makes it easier to detect unusual activities / transactions.

The customers who have a higher transaction volume or frequency shall be reviewed monthly or quarterly according to the degree of the transaction to ensure the consistency to the KYC / CDD profiling.

- **Watch List**

PayBitoPro utilises an unique feature of Watch List to monitor transactions of specific customers to mitigate the Money Laundering (ML) / Terrorist Financing (TF) risks, arising from abnormal activities from the customer's / user's account.

Once the KYC team of PayBitoPro approves a customer for availing the services provided by PayBitoPro, the individual / non-individual are enlisted on the Watch List for the purpose of continuous monitoring / identification of the behaviours that points towards the association with potentially higher risky activities.

PayBitoPro periodically monitors the transactions of the customers who are enlisted on the Watch List, and the investigators make a record after completing each transaction monitoring review.

Upon identification of the high risk factors, PayBitoPro further classifies the customers enlisted on the Watch List, into three levels for the purpose of reviewing the activities in accordance with the rules below respectively:

1. LEVEL A: Customers having more than two high risk factors (such as PEPs, adverse media and high risk industries), or upon finding some unusual transactions PayBitoPro has the discretion to review the transactions made by the customer and for the Level A customers post transactions reviews are made per week.

2. LEVEL B: Customers having two high risk factors (such as PEPs, adverse media), their transactions are reviewed per month.

3. LEVEL C: Customers having one high risk factor (working in a high risk industry), their transactions are reviewed quarter.

For further information of the investigation process and Suspicious Activity Report (SAR), please refer to respective points below.

PayBitoPro might exclude a customer from the Watch List on an exception basis or have their level of monitoring downgraded, provided that if there are no alerts triggered, or no abnormal / unusual activities are found within a span of more than 12-18 months and the approval is given from both the Head of the compliance and CEO.

• Purposes of Red Flags

For the purpose of preventing the misuse of Virtual Assets and funds for committing financial crimes and terrorism funding, PayBitoPro implements the transaction monitoring rules[3] which are designed in such a manner where

[3] Section 15.4-15.7 of Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007

developing the red flags indicators helps strengthen the control in accordance with the detection targets below:

1. Monitoring the transactions which have an unexpected higher value (pecuniary value) or where the frequency of the transactions are very frequent, without a justifiable reason.

2. Preventing any individual from using PayBitoPro's services or product on behalf of another principal.

3. Detecting unusual login where the IP addresses are inconsistent without any justifiable reason.

4. Identifying transactions from sanctioned and high-risk countries imposed by the UN, EU, FATF, OFAC, HMT;

5. Identifying high risk Virtual Assets Service Providers (VASP) and E-wallets.

- **Red Flags Categories**

PayBitoPro has designed the red flags into two categories:

1. Transaction based triggers: this red flag category is based on the transaction timing, either pre-transaction, real-time, and post-transaction (e.g., monthly accumulated trading volume).

2. Non transaction based triggers: this red flag category is 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.

- **Investigation Process**

PayBitoPro has investigators who were given the responsibility to initiate the investigation process while any alerts of any suspicious activities are triggered.
Pre-approval of the investigator or any equivalent role is required before taking any actions, if the activity / transaction is found out that the activity / transaction has a risk factor.
The investigator in charge is responsible for reviewing the alerts triggered and taking immediate action as it deems fit by the investigator. If an alert is triggered, the investigator is responsible for evaluating whether the activity / transaction is indeed a suspicious activity / transaction and take actions pursuant to the case as necessary. For instance:

1. Checking the profile of the customer in the system.

2. Referring to the transaction history in the system.

3. Communicating with the sales department or an employee who knows the customer.

4. Collecting more information or documents from the customer via the KYC team.

An investigation report shall be made by the investigator if the dispute / issue cannot be resolved within a reasonable time frame. The investigator shall input the actions to be taken into the report and provide relevant information and supporting documents to the Head of the Compliance department.

If the PayBitoPro system has triggered any alert and the issue cannot be resolved within a reasonable time then the customer has to go through the Re-KYC / CDD procedure as mentioned in KYC / CDD policy.

For further information, kindly refer to the KYC / CDD policy.

- **Suspicious Activity**

To comply with the requirements of Anti Money Laundering (AML) / Counter Terrorism Financing (CTF), all the employees of PayBitoPro shall report to the Head of Compliance or the immediate line manager upon finding any suspicious activity.

Activities below-mentioned are not exhaustive but shows suspicious situations:

1. Transactions made by the customers which 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 which shows that the customer has logged in from various countries within a short period.

While the investigator of PayBitoPro detects any suspicious activity, taking appropriate action accordingly is the duty of the investigators. It is also the responsibility of the investigator to provide relevant information and

supporting documentation shall be provided to the Head of the Compliance department to determine what appropriate actions could be taken against the unusual activity / transactions.

Filing a Suspicious Activity Report (SAR)[4] to the regulatory authority (AUSTRAC) is required when the Head of Compliance department determines the dispute / issue of suspicious activity can not be resolved.

For further information / details, kindly refer to the Suspicious Activity Report ("SAR") Procedure.

- ## Travel rule

PayBitoPro always makes sure that the transactions that are happening on the portal are legal transactions. As per the FATF mandate, the Travel Rule for crypto assets states that any crypto transaction that crosses a certain threshold must be accompanied by the personal information of the customer. PayBitoPro follows the travel rule regulations for every transaction that happens on the platform. Additionally, PayBitoPro screens the counterparty customer, and performs due diligence on the counterparty VASP. PayBitoPro takes time to understand and prepare to abide by these regulations or run the risk of losing their operational licences.

[4] Part 3, Division 2, Section 41 of Anti-Money Laundering and Counter-Terrorism Financing Act 2006

- ## Travel rule questions

  It is the responsibility of PayBitoPro to look into the legality of transactions, hence some questions are being asked to the customers before completing the transaction. The questions which are being asked are as follows:

  1. Sending crypto-currency to other addresses:

     - Originator's Tax Filing Number (TFN) or National Identity Number

     - Originator's name (i.e., the sending person's accurate (i.e., verified) full name);

     - Originator's account number used to process the transaction. In the VDA context, this would mean the "wallet address" of the originator;

     - Originator's physical (geographical) address that uniquely identifies the originator to the ordering institution, or date and place of birth. Provided that such an address has been verified for accuracy by PayBitoPro as part of its KYC process;

     - Beneficiary's name (i.e., the name of the person who is identified by the originator as the receiver of the VDA transfer). This is not required to be verified by PayBitoPro for accuracy, but should be reviewed for the purpose of STR monitoring and sanction screening; and

- Beneficiary account number used to process the transaction. In the VDA context, this could mean the "wallet address" of the beneficiary.

2. Receiving crypto-currency from other addresses:

    - Originator's Tax Filing Number (TFN) or National Identity Number

    - Originator's name (i.e., the sending person's name). PayBitoPro does not need to verify the originator's name for accuracy, but should review it for the purpose of STR monitoring and sanction screening.

    - Originator's account number used to process the transaction. In the VDA context, this could mean the "wallet address" of the originator.

    - Originator's physical (geographical) address that uniquely identifies the originator to the ordering institution, or date and place of birth.

    - Beneficiary's name (i.e., the name of the person who is identified by the originator as the receiver of the VDA transfer). PayBitoPro verifies the beneficiary's name for accuracy, if the name of their customer has not been previously verified. Thus, PayBitoPro can confirm if the beneficiary's name and account number they obtain from the ordering institution match with the beneficiary institution's verified customer data.

- Beneficiary's account number used to process the transaction. In the VDA context, this could mean the "wallet address" of the beneficiary

Lastly, the customer has to agree to the terms and conditions box, which leads to sharing of the personal information, including full name, national identification, physical address, etc. with the receiving exchange, in free will and consent for availing the services of PayBitoPro.