PayBitoPro

ANTI-MONEY LAUNDERING POLICY (AML)

(AUSTRALIA)

JUNE 2024

TABLE OF CONTENTS

1. Introduction

The stated Anti-Money Laundering (AML)[1] / Counter Terrorism Financing (CTF) policy underscores PayBitoPro's dedication to combating money laundering, terrorism financing, and related illicit activities. It outlines the company's measures to prevent users from exploiting its services for criminal purposes, aligning with relevant Australian 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), Privacy Act, 1988, and other applicable regulations. PayBitoPro has crafted this policy to ensure trading transparency and safeguard against money laundering 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 AML/CTF Policy applies uniformly to any User intending to access the Services or derive benefits from the Online Platforms and is considered an integral component of the User Terms and Conditions. Prior to utilizing the Online Platforms or disclosing any personal information, it is essential to thoroughly review this AML/CTF Policy. Through your use of the Online

[1] Chapter 10, Part 10.2, Division 400 of The Criminal Code Act 1995 (Criminal Code)

Platforms, you are expressly acknowledging your agreement to adhere to the User Terms and Conditions and, by extension, this AML/CTF Policy.

2. Definition

2.1) In this AML / CTF policy:

a. "Beneficial Owner" means[2]:

- In the case of corporations, if a natural person holds ownership of more than 25% (twenty-five percent) of the shares, has the right to receive over 25% (twenty-five percent) of the profits, or exercises the power, whether directly or indirectly, to appoint or elect more than half of the company's board of directors, they meet the defined conditions.

- In the context of partnership firms or Limited Liability Partnerships (LLPs), an individual qualifies under the stated conditions if they hold ownership of more than 15% (fifteen percent) of the capital or are entitled to receive profits exceeding 15% (fifteen percent).

[2] Part 1.2 (1) of Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007

b. “Identification Document(s)” refers to:

- A passport or official identification document (such as a national identification card, birth certificate, or driver’s license) should include a photograph, full name (including any aliases), unique identification number, date of birth, nationality, and, if necessary, proof of a name change.

- Proof of address, such as a utility or telephone bill, bank statement, or correspondence from a government agency, must be dated within the last 3 months and display the full name. P.O. Box mailing addresses are not permitted.

- Any other additional document that the Company may notify at any time will also be considered. "Periodic Updates" involve re-verifying the User's identity according to the procedure detailed in Clause 11 (Customer Verification Procedure) of this AML Policy, at intervals deemed suitable by the Company or directed by relevant enforcement authorities.

c. “Sanction Lists” refer to:

The enumeration includes natural and legal persons listed in any roster circulated by countries, governments, or international bodies, such as the US Department of the Treasury’s Office of Foreign Assets Control (“OFAC”), the US Department of State, the United Nations Security Council, the European Union, Her Majesty’s Treasury, the Hong Kong Monetary Authority, or the Monetary Authority of Singapore, along with relevant applicable laws.

d. "Suspicious Transactions"[3] refers to the following activities, whether attempted or executed

- Terrorist Financing denotes transactions that, to an individual acting in good faith, appear to involve funds collected, either fully or partially, for use by a terrorist organization or its affiliates, or to support activities associated with terrorism or terrorist acts.
- Unusually Complex: Unusually Complex transactions are those that, to an individual acting in good faith, appear to have been organized in a manner displaying unusual or unjustified complexity.

- Malafide Purpose: Malafide Purpose pertains to transactions that, to a person acting in good faith, seem to have been conducted without a legitimate purpose or a valid economic rationale.

2.2) The capitalized terms used herein, but not defined, shall have the meaning given to such terms in the Terms (defined below)

3. **AML Policy Is Part Of Our Terms**

This AML / CTF policy is a part of and incorporated within and is to read along with the User Terms and Conditions.

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

4. **Policy Changes**

The Company retains the authority to amend and update this AML/CTF Policy as needed, with changes taking effect immediately and applying prospectively, not retroactively. It is recommended to review this policy whenever accessing the Online Platforms.

5. **Your Obligations**

- You acknowledge your duty to comply with the terms and conditions set forth in this AML/CTF Policy and consent to refrain from using the Services and Online Platforms in any way that could result in the commission or attempted commission of criminal offenses. Additionally, you agree to and accept any future modifications to this Privacy Policy, even if they occur without prior notification.

- You must ensure that any personal information and/or Identification Documents submitted by you belong to you.

- You must file a fresh proof of address within six months of making any changes to the address mentioned as per the 'proof of address' submitted by you.

- If you are acting on behalf of a legal entity, you must identify the Beneficial Owner and also help verify the identity of both the Beneficial Owner and any individual claiming to represent the said legal entity.

6. **Purpose of this Policy**

In order to mitigate the risks relating to money laundering and other illegal activities, the Company intends to put in place this policy[4] which has the following elements:

- Customer Acceptance Terms; and
- Risk Management Procedure; and
- Customer Verification Procedure; and
- Transaction Monitoring Terms

7. **Customer Acceptance Terms**

The Company may either at the time of opening the User Account, or while undertaking any transactions, or during Periodic Updates, or for any other reason, ensure your compliance with the following:

- Require that you undergo a verification process during the activation process of your User Account by submitting your Identification Documents and such other details, as mandated under Clause 11 (Customer Verification Procedure) of this AML / CTF Policy.

[4] Part 7 of Anti-Money Laundering and Counter-Terrorism Financing Act 2006

- If the Company suspects that you are listed in the Sanctions Lists, it may require you to provide additional details to verify your identity, as deemed necessary.

- Require you to submit such additional information and/or data as may be directed by a competent enforcement authority.

- You are required to confirm that your Linked Bank Account is maintained solely with a scheduled commercial bank that adheres to all Know Your Customer (KYC) procedures mandated by the applicable laws of Australia.

The Company retains the discretion to decline opening new accounts, give notice of termination to existing User Accounts, or refuse to process transactions on the Online Platforms if it cannot ensure compliance with the aforementioned conditions. This could be due to the User's lack of cooperation or if the details provided by the User are found to be listed on any Sanctions Lists or deemed unreliable or unverifiable to the Company's satisfaction.

8. **Risk Based Approach on Money Laundering**

PayBitoPro adopted a Risk Based Approach (RBA) to assess the risks of a customer in regards to the AML regulations. This approach helps to filter out the customers into various categories of risks of customers. The RBA is a principle to adopt a more dynamic set of measures to target resources more effectively and apply appropriate preventive measures that are commensurate with the nature of risk so that the efforts can be focused in a more efficient manner.[5]

[5] Anti-Money Laundering and Counter-Terrorism Financing Act 2006

The general application of the RBA is that where customers are associated with higher money laundering (ML) risks, enhanced measures shall be taken to manage and mitigate those risks. Correspondingly where the stakes are lower, simplified measures shall be applied.

PayBitoPro assesses the risks of every transaction and customer and takes appropriate measures to mitigate those risks. Some of the risks and key control that can be taken against those risks are listed below:

A. Money Laundering Through Cryptoasset Exchanges:

- Use of non-compliant exchanges
- Use of exchanges in high-risk jurisdictions
- Use of money mules or fraudulent documents at crypto exchanges
    - ❖ Controls we take: Wallet and transaction screening solutions which detect activity involving high-risk exchanges counterparties and Virtual Asset Service Provider (VASP) Due Diligence solutions that provide a view of exchanges' risk.

B. Money Laundering Through Mixers and Privacy Wallets:

- Use of mixers or privacy wallets to obscure the source of funds.
- Use of mixers or privacy wallets to obscure the destination of funds
    - ❖ Controls we take: Wallet and transaction screening solutions that can detect activity with exposure to mixers and privacy wallets and blockchain forensics capabilities which can visualize complex transactional activity involving mixers and privacy wallets.

C. Money Laundering Through Decentralized Finance (DeFi) and Cross-chain Services:

- Use of decentralized exchanges (DEXs) to swap illicit-origin assets
- Use of DeFi mixers
- Use of cross-chain bridges
    - ❖ Controls we take: Blockchain analytics solutions featuring Holistic Screening capabilities, which enable the detection of illicit and high risk activity despite the use of "cross-chain" money laundering techniques conducted through DeFi services

D. Money Laundering Involving Tokens and Stablecoins:

- Using tokens and stablecoins to "clean" illicit origin funds
- Use of new token sales to perpetrate "rug pulls" and other scams
- Using DEXs to launder stolen tokens and stablecoins
    - ❖ Controls we take: Blockchain analytics solutions featuring Holistic Screening capabilities, which enables the detection of illicit and high risk activity despite the use of "cross-chain" money laundering techniques conducted through DeFi services and Wallet and transaction screening solutions which can detect activity with exposure to token scams.

E. Money Laundering Involving Privacy Coins:

- Using privacy coins to layer illicit proceeds.
- Using coinswap services to launder illicit-origin privacy coins.
    - ❖ Controls we take: Wallet and transaction screening solutions which detects activity involving high risk coinswap services.

F. Money Laundering Involving Wallet Specific Behaviors:

- Using "chain-peeling" techniques to obscure the source of funds.
- Using hosted wallets at an exchange to move funds between members of a criminal network.
    - ❖ Controls we take: Transaction screening solutions which can identify exposure to illicit and high risk wallets through a limitless number of hops and Blockchain forensics capabilities can visualize complex peeling chain activity

G. Terrorist Financing Involving Cryptoassets:

- Use of crypto crowdfunding campaigns to raise funds
- Use of crypto to enable lone actor or small cell activity
    - ❖ Controls we take: Wallet and transaction screening solutions which detects activities involving addresses associated with known terrorist campaigns and activities involving crypto exchanges in high risk jurisdictions

H. Sanctions Evasion Involving Cryptoassets

- Use of crypto to attempt to conceal sanctions-related activity.
  - ❖ Controls we take: Wallet and transaction screening solutions which detect activities involving wallets associated with sanctioned actors and Blockchain analytics solutions featuring Holistic Screening capabilities, which enable the detection of sanctions-related activity despite the use of "cross-chain" money laundering techniques conducted through DeFi services.

9. Risk Management Procedure

The Company may categorize its Users including you into low, medium or high-risk categories, after undertaking an appropriate risk assessment of each User based on the following factors (including without limitation)

- Sufficiency and adequacy of identification information submitted under Clause 11 (Customer Verification Procedure); or
- Its social and/or financial status; or
- Nature of User's business/vocational activities; or
- You recognize that the Company will uphold the confidentiality of your risk categorization and associated data to preserve the integrity of the Risk Management Procedure. It's understood that you cannot request disclosure of your risk categorization. Nevertheless, the Company may share your risk categorization data with the relevant enforcement authority if it identifies that a specific User has conducted or is likely to conduct any Suspicious Transaction.

10. Risk score calculation

PayBitoPro pays serious attention and always strives to ensure that the services are being provided to authentic individuals / non-individuals. The documents / data provided by the customers during the KYC / CDD procedure are received for assessing the risks before providing the services. The personal and professional information / data are collected from the customer to calculate the risk score of an individual / non individual in the following manner:

1. Identity Verification
2. User Country
3. Industry
4. Occupation
5. Source of funds
6. Transaction volume
7. Annual Income
8. Net worth
9. Employment category
10. Employment Type
11. Politically Exposed Person (PEP)
12. Person relation with bank or Financial Institution (FI)
13. Purpose of account
14. Person watchlist
15. Person Negative News

11. **Customer Verification Procedure**

The Company, during activation of User Accounts or while undertaking any transactions or for any other reason, may require for the purposes of verification of any User's identity, following details:

- For individuals, it is necessary to furnish one copy of any Identification Document containing their identity and address details, along with one recent photograph. Additionally, they may need to provide any other documents concerning their business or financial status as specified by the Company periodically.

- In the case of Companies, the documents to be submitted are copies of the national official or governmental company search extract equivalent, Certificate of Incorporation, Memorandum and Articles of Association, and a Board resolution authorizing transactions on the Online Platform. Additionally, provide Identification Documents with identification and address details of the authorized individual to transact, along with a copy of the authorization document.

- For Partnership Firms/Limited Liability Partnerships, the documents to be submitted includes one copy each of the national official or governmental company search extract equivalent, Registration/Incorporation Certificate, partnership deed, and Identification Documents with identification and address details of the authorized individual to transact, along with a copy of the authorization document. It is the responsibility of users to ensure that all copies of these Identification Documents are appropriately certified.

For identity verification of any User, the Company may depend on suitable and licensed third-party service providers to authenticate the Identification Documents and other associated details provided by the User.

If the Company finds any User information acquired in accordance with the procedure detailed under this Clause to be insufficient, inadequate, or included in the Sanctions Lists, it reserves the right, at its discretion, to either reject or terminate (where applicable) the registration of such User Account, or to request a re-verification of the User's Identification Documents.

12. **Transaction Monitoring Terms**

The Company consistently monitors all transactions[6] conducted or attempted on the Online Platforms, employing a combination of manual scrutiny and software-based algorithms. This ensures the swift identification and highlighting of various transaction types, including but not limited to the following:

- High value transactions
- Cross-border transactions
- Suspicious Transactions as per the laws of Australia.

At intervals, the Company may perform essential investigations to detect and analyze transactions that do not align with a User's risk profile (as determined in Clause 9 - (Risk Management Procedure), level of sophistication, or anticipated usage pattern.

[6] Chapter 15.4 of Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007

13. Suspicious Transactions Report (STR)

In any event, where any suspicion is recognized / identified by PayBitoPro during transaction monitoring[7] of any customer, the account shall be locked, and the transaction shall be suspended, and as soon as practicable, it shall be escalated with relevant account information and transaction details to the MLRO (Money Laundering Reporting Officer) for prompt review and investigation without undue delay. If warranted, the MLRO shall, within three business days from the date of identifying the activity, submit a suspicious transaction report (STR) to the appropriate supervisory authority which is the Australian Transaction Reports and Analysis Centre (AUSTRAC).

It is prohibited by law from disclosing (tipping-off) to any person, any information which might prejudice an investigation. For instance if a customer is told that a report or related information is being filed with the regulatory authority (AUSTRAC), this would prejudice the investigation and lead to a violation of the law.

It is the duty of PayBitoPro to report immediately, in case of any suspicion / unusual activity of money laundering and terrorist financing to the appropriate regulatory authority which is the Australian Transaction Reports and Analysis Centre (AUSTRAC), but not later than seven working days from the date of identifying / recognizing such activity.

[7] AUSTRAC guidelines

14. Maintenance Of Records

The Company will maintain and preserve the following information and/or data:

- Records of all transactions executed on the online platforms, for a period of at least 7 (Seven) years[8] from the date of each transaction.

- Records of all transactions identified under clause 12 (Transaction monitoring terms) above for a period of at least 7 (Seven) years, including but not limited to the information about the nature, value and parties to such transactions and their date to remittance.

- Identification records of Users (including but not limited to the Identification Documents submitted pursuant to Clause 11 (Customer Verification Procedure) above), during the subsistence of and for a period of at least 7 (Seven) years from the date of termination of such user account.

15. Compliance, Disclosure and Notices

- The Company may share, from time to time, information regarding transactions identified under Clause 12 (Transaction Monitoring Terms), identification information of such Users, or any other

[8] Part 10, Division 2, Section 107 of AML/CTF Act, 2006

information mandated under the applicable law, with the appropriate enforcement authorities.

- In order to improve the integrity and transparency of transactions on the Online Platforms, you are encouraged to report any information you are privy to or become privy to in the future regarding any Suspicious Transactions or transactions you have find or have reason to believe are dubious in nature, to our Compliance Officers by writing to them at *compliance@paybitopro.com*

- In order to ensure compliance with this AML Policy and/or the applicable laws, the Company may be required to send you notices from time to time. All such notices will be sent to such addresses as provided by you under Clause 11 (Customer Verification Procedure) of this AML Policy. Where you are required to share any information according to the procedures contained in this AML Policy, such communication may be made by you electronically by sending an email at *compliance@paybitopro.com*

16. **Employee Training**

PayBitoPro takes appropriate measures to ensure that the employees are well trained in the Anti Money Laundering regulations. PayBitoPro ensures that the employees are:

1. Made aware of the law relating to money laundering and terrorist financing, and to the requirements of data protection, which are relevant to the implementation of these regulations.

2. Regularly given training in how to recognise and deal with transactions and other activities or situations which may be related to money laundering or terrorist financing;

PayBitoPro also makes sure that the employees are capable of:

1. Identification and mitigation of the risks associated with money laundering, terrorist financing and proliferation financing.

2. Prevention or detection of money laundering, terrorist financing and proliferation financing

The compliance team of PayBitoPro shall provide the employee training on Anti Money Laundering (AML). The training shall be tailored to the employees and the business needs.

The AML training provided shall be applicable to all the employees regularly and irregularly.