

PayBitoPro

ANTI-MONEY LAUNDERING POLICY (AML)

(REST OF THE WORLD)



Created by:	Avishek Banerjee
Approved by:	Souhardya Sarkar
Documentation Version:	2.1
Submission Date:	6th May, 2024

TABLE OF CONTENTS

• Introduction	3
• Purpose:	3
• Roles and responsibilities:	4
• Customer Relationship:	4
• Vendor or Partner:	5
• Know Your Customer (KYC) and Customer Due Diligence (CDD)	5
• Name Screening	7
• Risk Based Approach on Money Laundering	8
1. Money Laundering Through Cryptoasset Exchanges:	9
2. Money Laundering Through Mixers and Privacy Wallets:	9
3. Money Laundering Through Decentralized Finance (DeFi) and Cross-chain Services:	9
4. Money Laundering Involving Tokens and Stablecoins:	10
5. Money Laundering Involving Privacy Coins:	10
6. Money Laundering Involving Wallet Specific Behaviors:	10
7. Terrorist Financing Involving Cryptoassets:	11
8. Sanctions Evasion Involving Cryptoassets	11
• Customer Money Laundering (ML) Risk Classification	11
• Risk score calculation	12
• Periodic and Trigger Review (On-going KYC)	13
• Prohibited Countries and Customers	15
• Red Flags (Examples of Suspicious Activity)	16
❖ Transaction-related:	16
❖ Customer-related	17
❖ Employee Related	17
• Suspicious Transactions Reporting	18
• Record Retention	19
• Employee Training	19
• Risk Assessment and Testing	20



- **Introduction**

The AML 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 to the respective laws of the member states of the Financial Action Task Force (FATF) 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 the respective member states of the FATF and the business enterprises registered in the member states of the FATF.

The AML 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 AML Policy. Your use of the Online Platforms implies your explicit acknowledgment and adherence to the User Terms and Conditions and, consequently, this AML Policy.

- **Purpose:**

The purpose of this policy is to set out how PayBitoPro is complying with the mandates of the FATF and how PayBitoPro is carrying out the business and operation.



This policy also serves as a guideline for the employees of PayBitoPro to carry out and execute the appropriate procedure / actions as per the requirements laid down in FATF mandates.

This policy directs all the functional units of PayBitoPro to follow the steps or guidelines or procedures as adopted in this policy.

This policy is subject to changes or updates from time to time as and when relevant amendments to the guidelines and mandates by the Financial Action Task Force (FATF) and it is directed to all the employees of PayBitoPro to follow the updated guidelines.

- **Roles and responsibilities:**

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 Financial Action Task Force (FATF) recommendations and mandates, ensuring, that the individual(s) / non-individual(s) are restricted from exploiting the services provided by PayBitoPro. The roles and responsibilities of the employees of PayBitoPro is to collect the relevant information or data including personal and professional information from the individual or non-individual for the purpose of the Know Your Customer (KYC) and Customer Due Diligence (CDD) purposes before availing any services from PayBitoPro. Any business and operational executive might directly or indirectly approach prospective or existing customers to collect such relevant information, data, files or documents.

The compliance team of PayBitoPro shall act as an adviser and provide training and guidance to the business and operational teams timely and appropriately during the KYC and CDD procedure.



- **Customer Relationship:**

If any service is provided by PayBitoPro to any individual(s) / non individual(s) then it is deemed to be an establishment of agreement between the customer and PayBitoPro (Customer On-Boarding), which makes the customer subject to the Anti Money Laundering (AML) regulations.

Otherwise, except by any condition in external regulation or where an approval is obtained from the head of the compliance department; the requirements in respect to the KYC/CDD are mandatory and should be satisfied before a customer relationship is established.

To protect the security of the customers' accounts, PayBitoPro conducts periodic KYC/CDD reviews. PayBitoPro additionally performs immediate review of an account if a system alert is triggered.

Either or both the customer and PayBitoPro can terminate the customer relationship on the basis of the process/conditions applicable (The customer off-boarding).

If the customer wishes to resume, to avail the services of PayBitoPro then the customer must go through the KYC/CDD process all over again.

- **Vendor or Partner:**

Verifying the background of the vendor or partner, whether they are working with the parallel policies of PayBito or not. Timely review of relationship with the vendor/partner, whether any changes are made or not and whether the relationship can be maintained or not.



- **Know Your Customer (KYC) and Customer Due Diligence (CDD)**

The KYC and CDD process is a mandate before the on-boarding of the customer. Additionally, the satisfaction of the following stated requirements is necessary to avail the services provided by PayBito:

1. Paybito shall understand the purpose and intention of the customer for establishing a customer relationship with our concern. Thus Paybito will collect the relevant information and documents required.
2. Paybito shall collect information on whether the customer willing to avail the services, is a Politically Exposed Person (PEP) or not; which not only includes the customer but it extends to the family members or a person known to be a close associate of the customer.
3. The KYC and CDD procedure shall be extended to the beneficial owner (if any) of the customer, and to understand the customer's ownership and control structure from the information/documents collected by Paybito.
4. If any person(s) acts on behalf of the customer, the KYC and CDD procedure as well as the right of representation shall be extended to such person.

In the event of any doubts about the veracity or non-adequacy of the data provided by the customer as per the requirement of PayBitoPro, additional documents or information shall be demanded from the customer to complete the KYC and CDD procedure as per the guidelines.

If the customer is unable to comply with the KYC and CDD procedure as described, the establishment of the customer relationship (Customer On-Boarding) shall be refused/rejected.



For any existing customer, if they refuse to provide the documents/information for the periodic KYC and CDD procedure, it shall be deemed to be a fundamental breach of the contract and termination of the customer relationship. In addition, PayBitoPro and the compliance team shall assess whether the circumstances constitute any material risk, and if found so a Suspicious Activity Reporting (SAR) shall be filed before the respective regulatory authorities of the member states of FATF and the Financial Intelligence Unit (FIU).

Please refer to the KYC and CDD Procedure for further information.

- **Name Screening**

Name screening is one of the major parts of the KYC and CDD procedure. The KYC verification agency shall perform name screening, watchlist checks. The name screening involves checking (with fuzzy matching capabilities) a customer's name against a commercial database for possible matches of PEPs, sanctions and adverse media checks. The commercial database is provided by Comply advantage which, together with KYC verification agency, collectively includes the following lists:

1. International sanctions lists or the blacklist from the Financial Action Task Force (FATF), the United Nations (UN), the European Union (EU), the Office of Foreign Assets Control (OFAC), and Her Majesty's Treasury (HMT).
2. PEP lists covering 200+ countries
3. Criminal and law enforcement lists;
4. Interpol wanted lists;



5. Regulatory enforcement lists;
6. Adverse media.

PayBitoPro conducts the AML name screening process by following these below mentioned steps:

1. Acquiring the necessary information / data: PayBitoPro collects the relevant information / data from the customers for the name screening purpose.
2. Organizing the data: PayBitoPro uses a professional methodology to organize the information / data which are to be screened, for instance, making sure that the names are in correct format.
3. Conducting the screening: PayBitoPro uses manual as well automated searching methods throughout the various lists such as Sanctions list or PEPs list.
4. Analyzing the result: PayBitoPro reviews the matches that were found in the screening process and determines whether they are true matches or false positives.
5. Taking appropriate action: PayBitoPro after analyzing the result, takes appropriate action, for instance, freezing the account or ending the business relationship with the customer, if a match is found.



● Risk Based Approach on Money Laundering

PayBitoPro adopted a Risk Based Approach (RBA) to assess the risks¹ 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.

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:

1. 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.

¹ FATF recommendation



2. 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.

3. 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

4. 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.

5. 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.

6. 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

7. 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

8. 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.

● Customer Money Laundering (ML) Risk Classification

Complying by the Risk Based Approach (RBA) taken by PayBitoPro to take into account the factors like Country Risk, Customer Risk and Business Risk all the individual / non-individual shall be assessed and classified into either categories below, corresponding to Due Diligence measures commensurate with their ML risks:

1. Low-risk customer
2. Medium risk customer
3. High risk customer



Whenever customers are classified as High-risk Customers, the Enhanced Due Diligence process (“EDD”) is implemented by PayBitoPro. The following factors are considered and to calculate a score for each applicant to decide whether such customers shall be classified as High-risk Customers:

1. The customer’s occupation or the nature of the business of the company is a high-risk industry which indicates higher ML risks.
2. The customer, who is not a sanctioned target, is from a high-risk country or region (High Risk and Prohibited Country List) where certain sanctions (restricted measures) are taken by the FATF, UN, EU, OFAC, or HMT.
3. The customer is identified as a PEP (is an individual who is or has been entrusted with a prominent public function, such as heads of state or head of government, senior government, a senior politician, a judicial or military official, senior executive of a state-owned corporation, and an important political party official. Many PEPs hold positions that can be abused for the purpose of laundering illicit funds or other predicate offenses such as corruption or bribery.), a family member or a close associate of a PEP.
4. The customer had or has been involved in the criminal or administrative investigation due to a positive match of any adverse news concerning law enforcement.
5. PayBitoPro reasonably believes there is a higher ML risk based on available information.

- **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

● **Periodic and Trigger Review (On-going KYC)**

The periodic review of the documents / informations provided by the customer previously while registering at PayBitoPro while going through the KYC / CDD procedure, is done on the basis of of the risk categories of the customers in the following manner:

1. High risk customer: Once in every year
2. Medium risk customer: Once in every two years.



3. Low risk customers: Once in every three years.

PayBitoPro reviews the existing KYC / CDD records upon triggered events. For instance, the trigger events compiles of the following:

1. Re-activation of a dormant account;
2. Changes in the beneficial ownership or control of the user or account;
3. Changes in a significant (the term “significant” is not necessarily linked to monetary value. It may include transactions that are unusual or not in line with the knowledge of the customer. Significant transaction includes a wide range of transaction abnormality, such as a deviation from the user's transactional volume or frequency) transaction pattern;
4. A material change occurs in the customer's information;
5. Any other material change which affects the customer's risk rating to be higher.

PayBitoPro retains and monitors the transaction and communication of customers / users to ensure that the transactions made by the customer / users are for reasonable and legitimate business activities and the whole transaction is based on the true knowledge of the customer / users without any ulterior motives. The monitoring of the transactions are also based on the risk profiles of the customers.

If any of the below mentioned situations or cause of action arises then PayBitoPro shall have the authority to block the customer from availing the services provided by PayBitoPro or atleast the customers' risk profile shall be updated accordingly upon the discretion of PayBitoPro. The cases / situations are as follows:



1. If the question of the authenticity or the truthfulness of the documents / information provided by the customer for the KYC / CDD procedure before availing the services of PayBitoPro arises.
2. The customers' / users transaction has been identified and marked as suspicious. Upon identifying the transaction to be suspicious a report shall be prepared and sent to the appropriate supervisory authority which is the Financial Conduct Authority (FCA)

- **Prohibited Countries and Customers**

Considering the efforts and resources required in maintaining and monitoring business relationships with specific customers / users which may reduce PayBitoPro's ability to provide services to other customers / users upon complying with the regulations of the member states of FATF, PayBitoPro is under no obligation to provide services to some specific customers / users or customers / users conducting business in a specific area. Applications concerning with either situation below will **NOT** be accepted:

1. Applicants in the lists of any sanctions or embargoes imposed by the United Nations (UN) , the European Union (EU) , the Office Of Foreign Assets Control (OFAC) , and the Her Majesty's Treasury (HMT);
2. Identifiable addresses associated with cryptocurrency wallets involved with sanctioned events;
3. Applicants from "High-risk Jurisdictions" subject to a "Call for Action" by Financial Action Task Force (FATF) [High risk and other monitored



jurisdictions by FATF]² These jurisdictions are subject to change by FATF from time to time.

- **Red Flags (Examples of Suspicious Activity)**

The activities / behaviors mentioned below are not exhaustive in nature. It is directed to all the employees of PayBitoPro to pay attention to any abnormal or unusual activity or transactions or behaviors taking place while using the services of PayBitopro and should be immediately reported to the line manager or the compliance team:

- ❖ Transaction-related:

1. Transactions which have no apparent legitimate purpose or appearance, which does not have a commercial rationale.
2. A customer making frequent purchases at a high price and then selling at a considerable low price making a loss to the same party.
3. A customer making multiple small deposits/withdrawals to avoid currency reporting requirements.
4. Where, without reasonable explanation, the volume or frequency of transactions is out of line with any pattern that has previously

² <https://www.fatf-gafi.org/en/countries.html#high-risk>



emerged. For instance, the volume and frequency of a customer's trades unexpectedly appears to be large and active whereas the previous pattern has been small and inactive.

5. Transferring to and from high risk jurisdiction(s) without reasonable explanation, which are not consistent with the customer's declared business dealings or interests.
6. Transactions detouring through third parties. For instance, cryptocurrency tumbler (also known as cryptocurrency mixing services) obscures the transaction details and making it difficult to track their source.

❖ Customer-related

1. Where the customers / users refuse to provide the information / data requested without reasonable explanation or refuses to cooperate with the CDD or ongoing monitoring process.
2. Where a customer who has entered into a business relationship uses the relationship for spontaneous or abrupt transactions, or for only a very short span of time without a reasonable explanation.
3. Where a customer has been introduced by a third party that is based in high risk jurisdiction(s).
4. Where a customer uses a bank account, telephone number, or mailing address that is located in high risk jurisdiction(s).



5. Where a customer has opened multiple accounts for no apparent business reason.

❖ Employee Related

1. Changes in employee characteristics. For instance, lavish lifestyles or avoiding taking holidays without reasonable cause.
2. Unusual or unexpected increase in the sales performance of an employee.
3. Incomplete or missing supporting documentation for customers' accounts or orders.

• **Suspicious Transactions Reporting**

In any event, where any suspicion is recognized / identified by PayBitoPro during transaction monitoring 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 the stipulated time period as defined under the member state's laws from the date of identifying the activity, submit a suspicious transaction report (STR) to the appropriate regulatory / supervisory authority of the member states of FATF.

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, this would prejudice the investigation and lead to a violation of the law.

After submission of the STR to the appropriate regulatory authority, a precept shall be made by them, and after the precept is complied with, the customer will be informed that the regulatory authority has restricted the use of his/her account or that another restriction has been imposed.

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, but not later than the stipulated time period as defined under the member states' laws from the date of identifying / recognizing such activity.

For further detailed information on STR, visit the **Suspicious Transaction Reporting (STR) Procedure**.

- **Record Retention**

The information / data / documents provided by the customers which might be personal data or professional data for the KYC / CDD for the verification purposes before availing the services of PayBitoPro are kept throughout the continuance of the business relationship with the customer and at least for five years after the end of the business relationship.



The transaction history or record made during the span of availing the services from PayBitoPro are kept at least for five years after the completion of a transaction.

PayBitoPro shall keep staff training records at least for three years after completing the training.

• **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 trainings shall be tailored to the employees and the business needs.

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

- **Risk Assessment and Testing**

The Compliance Department will regularly assess and test the AML systems to ensure effectiveness accordingly. The frequency and extent should be commensurate with the nature, size and complexity of the business. The Compliance Department may seek a review from external parties, i.e. professional outside auditors.

