Schedule 2

PayBitoPro

Anti-Money Laundering (AML) & Counter-Terrorism Financing (CTF) Policy

---

Document Type	Document Owner	Written By	Date
Policy	Compliance	Rohan Gupta	May 31, 2022

Table of contents

1. The Purpose

To comply with the PayBitoPro FCC Statement, as well as relevant laws and regulations in the countries PayBitoPr

Operates;

To serve as a guideline for employees of PayBitoPro to carry out and meet applicable requirements of AML/CTF;

To direct all functional units of PayBitoPro to follow the steps and controls as adopted in this Procedure.

2. Risk-Based Approach

The Risk-Based Approach ("RBA") is a principle to adopt a more dynamic set of measures to target resources more effectively and apply preventative measures that are commensurate to the nature of risks, so the efforts can be focused in the most effective way.

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

In determining whether a customer is associated with higher or lower ML/TF risks, including but not limited to the following risk categories shall be taken into account:

(1) Risks relating to customer's profession, employment or industry.

(2) Risks relating to countries, geographic areas or jurisdiction(s).

(3) Risks relating to products, services or transactions being utilized.

(4) Risks relating to communication, delivery or distribution channels with customers.

The Procedure is maintained and reviewed as needed or at least annually by the Compliance Department.

3. Role and Responsibilities

Business and operational personnel may directly or indirectly approach prospective or existing customers to collect information, files or documents.

The compliance team as an adviser shall provide training and guidance to Business and operational teams timely and appropriately during the KYC and CDD.

4. Vendor or Partner

PayBitoPro takes reasonable actions to verify the background of a vendor or partner who supports or supplements PayBitoPro' s compliance work.

PayBitoPro shall timely review its relationship with a vendor or partner whenever PayBitoPro is aware of any material changes in the existing vendor or partner. The material changes include change of ownership or operation team and adverse media regarding the vendor or partner. After the review, PayBitoPro shall decide whether it should continue the relationship with the existing vendor or partner.

5. Customer Relationship

Any services provided to any individual or non-individual may be deemed as an establishment of a relationship ("the Customer on-boarding"), so AML/CTF requirements shall be applicable.

Except stipulated in any external regulations or where an exceptional internal approval from the Head of Compliance has been obtained, requirements in respect of the KYC and CDD shall be satisfied before a relationship is established.

To protect customers' account security, PayBitoPro conducts periodic KYC and CDD reviews or performs an immediate review if a system alert is triggered.

Either or both the customer and PayBitoPro can terminate the customer relationship according to processes applicable ("the Customer off-boarding"). Thereafter, no services would be provided to the customer. If the customer wishes for the resumption of services, the customer will be required to complete KYC and CDD processes again.

6. Know Your Customer (KYC) and Customer Due Diligence (CDD)

The KYC and CDD processes must be completed before on-boarding, including the satisfaction of the following requirements:

(1) PayBitoPro shall understand the purpose and intended nature of establishing customer relationships, where relevant, gathering information thereon;

(2) PayBitoPro shall gather information on whether a person receiving service is a politically exposed person (PEP), including their family member or a person known to be a close associate;

(3) If any beneficiary owner is in relation to the customer, the KYC and CDD shall be extended to the beneficiary owner and to understand the customer's ownership and control structure.

(4) If any person acts on behalf of the customer, the KYC and CDD shall be extended to the person and the right of representation.

In the case of doubts about the veracity or adequacy of customer data previously obtained, further information or files shall be obtained.

If unable to comply with the KYC and CDD required, the establishment of a customer relationship should be refused.

Suppose any existing customer refuses to provide information or documents required for the KYC and CDD, it shall be deemed a fundamental breach of the contract and a termination of the customer relationship. In addition, PayBitoPro and the Compliance team will assess whether the circumstances constitute a material risk. If so, a STR will be filed to the regulatory authority within two days.

Please refer to the **KYC and CDD Procedure** for more detailed information.

7. Identification and Verification (ID&V)

Identification and verification are core parts of the KYC and CDD processes.

Identification of a customer and verification of the submitted information shall be based on information obtained from a reliable and independent source[1].

Documents and information to be collected for a non-individual user are far more complex than an individual account as corporations differ in various legal forms in different country jurisdiction(s) with various control structures.

8. Name Screening

As part of the KYC and CDD, KYC verification agency will also perform Name Screening, Watchlist Checks. The Name Screening checks (with the fuzzy matching capability) a customer's name against a commercial database for possible matches of PEPs, sanctions, and adverse media. The commercial database is provided by ComplyAdvantage which, together with KYC verification agency, collectively includes the following lists:

(1) International sanctions lists or blacklist from the FATF, the UN, the EU, the OFAC, and the HMT;[3]

(2) PEP lists covering 200+ countries;

(3) Criminal and law enforcement lists;

(4) Interpol wanted lists;

(5) Regulatory enforcement lists;

(6) Adverse media.

[1] Information obtained from a reliable and independent source is based on a government-issued photographic and valid identification, e.g. passport, national/resident ID card or driver's license.

9. Customer ML/TF Risk Classification

Based on RBA to take account of factors such as country risk, customer risk, and business risk, all customers shall be assessed and classified into either category below corresponding to due diligence measures commensurate with their ML/TF 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") should be completed accordingly. 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 business nature of the company is a high-risk industry which indicates higher ML/TF risks.

(2) The customer, who is not a sanctioned target, is from a high-risk country or region[4] where certain sanctions (restricted measures) are taken by the FATF, UN, EU, OFAC, or HMT.

(3) The customer is identified as a PEP,[5] 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/TF risk based on available information.

[4] High Risk and Prohibited Country List.

[5] A politically exposed person (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.

10. Periodic and Trigger Review (On-going KYC)

To ensure the CDD documents, the data and information of a customer previously obtained in the following schedule:

(1) High-risk customers - every one year;

(2) Medium risk customers - every two years;

(3) Low-risk customers - every three years.

PayBitoPro shall regularly review existing CDD records upon trigger events. Examples of triggerevents include:

(1) Re-activation of a dormant account;

(2) Change in the beneficial ownership or control of the user or account;

(3) Change in a significant[6] 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 shall retain and check transactions and communications of customers to ensure that the transactions are reasonable business activities based on the knowledge of the customer, its activities, and risk profile.

In any case of situations below, the customer will be refrained from using service, or at least the customer's risk level shall be changed:

(1) Upon identification of a person or verification of submitted information, there are doubts about the truthfulness of the submitted data, authenticity of the documents or identification of the customer;

(2) The customer's transactions have been identified as suspicious and reported to the relevant authority.

[6] "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.

11. Prohibited Countries and Customers

Considering the efforts and resources required in maintaining and monitoring business relationships with specific customers, which may reduce our ability to service other customers and on complying with regulations, applications concerning either situation below will NOT be accepted:

(1) Applicants in the lists of any sanctions or embargoes imposed by the UN, the EU, the OFAC, and the HMT;

(2) Identifiable addresses associated with cryptocurrency wallets involved sanctioned events;

(3) Applicants from "High-risk Jurisdictions subject to a Call for Action" by Financial Action Task Force (FATF).[7] These jurisdictions are subject to change by FATF from time to time.

12. Transaction Monitoring

PayBitoPro has designed and maintained a Transaction Monitoring ("TM") system to monitor and identify any unusual or abnormal patterns and behaviors by customers. The parameters and thresholds are listed in the **Transaction Monitoring Procedure**.

TM alerts may arise whenever there are suspicious events or activities. TM Reports will be generated regularly based on what transactions should be triggered for ongoing transaction monitoring reviews.

To effectively reach the goal of AML/CTF, the Watch List monitoring is designed to monitor some specified customers, such as high-risk customers.

[7] High risk and other monitored jurisdictions by FATF, http://www.fatf-gafi.org/countries/#high-risk.

Compliance and Investigation teams shall review the Alerts and Reports timely, and decide what actions to be further taken appropriately, including initiating an internal investigation, filing an external suspicious transaction report, or both.

13. Wallet Monitoring

Due to a variety of methods through crypto transactions that can be used to hide the illicit origin of fund, PayBitoPro deploys many external service providers of crypto analytics, such as CipherTrace, Cybavo, and TRM Labs, to help in identifying and tracking suspicious activities associated with blacklists or sanctioned wallet addresses.

PayBitoPro is well-equipped to comply with the recommendations by FATF to mitigate cross-border ML/FT risk, particularly the "Travel Rule", which requires certain information disclosure and exchange between virtual currency exchanges in specific circumstances.

14. Red Flags (Examples of Suspicious Activity)

The activities and behaviors mentioned below are not exhaustive. All staff shall pay attention to any abnormal activities and behaviors detected and report to the line manager or Compliance team.

Transaction-related:

(1) Transactions or instructions which have no apparent legitimate purpose or appear not to have a commercial rationale.

(2) A customer makes frequent purchases at a high price and then sells at a considerable loss to the same party.

(3) A customer makes 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 emerged. E.g. The volume and frequency of a customer's trades unexpectedly appear to be large and active while the previous pattern has been small and inactive.

(5) Transfers 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 detour through third parties. E.g., cryptocurrency tumbler (also known as cryptocurrency mixing services) obscures the transaction details and make it difficult to

track their source.

Customer-related:

(1) Where the customer refuses to provide the information 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 sudden or abrupt transactions or for only a very short period without a reasonable explanation.

(3) Where a customer was 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. E.g., 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.

15. Suspicious Transaction Reporting

In any event, where any suspicion is identified during transaction monitoring, the account should be locked, and the transaction should be suspended, and as soon as practicable, escalated with relevant account information and transaction details to the MLRO[9] for prompt

[9] The Head of Compliance is the Money Laundering Reporting Officer (MLRO).

review and investigation without undue delay. If warranted, the MLRO shall, within two working days after identifying the activity, submit a suspicious transaction report (STR) to the regulatory authority.

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

After submission of a STR to the regulatory authority, a precept may be made by regulatory authority, and after the precept is complied with, the customer may be informed that 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 in case of suspicion of money laundering and terrorist financing to the regulatory authority immediately, but not later than within two working days after identifying the activity or facts or after receiving the suspicion.

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

16. Record Retention

Customer's CDD/KYC information and documents are kept throughout the continuance of the business relationship with the customer and for at least five years after the end of the business relationship.

Customer's transaction records are kept for at least five years after the completion of a transaction.

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

17. Staff Training

PayBitoPro will use a mix of training techniques and tools in delivering training and allocate sufficient resources to meet the educational needs of the staff members.

The Compliance Department will provide staff training on AML. The training materials shall be tailored to the staff and their business needs.

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

18. Risk Assessment and Testing

The Compliance Department will regularly assess and test the AML/CTF systems to ensure effectiveness accordingly.

The frequency and extent should be commensurate with the nature, size and complexity of PayBitoPro's businesses and the ML/TF risks arising from those businesses. Where appropriate, the Compliance Department may seek a review from external parties, i.e. professional outside auditors.

.