Schedule 1

PayBitoPro

Know Your Customer (KYC) & Customer Due Diligence (CDD) Procedure

---

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

Table of contents

1. Timing to Conduct

The KYC and CDD processes and requirements mentioned in this Procedure shall be conducted and completed in either situation below:

(1) Before establishing a business relationship with any new customer,

(2) Any doubts against the veracity or adequacy of obtained documents or information from any existing customer,

(3) Any material change of customers' information that affects the customers' risk rating to be higher,

(4) Any suspicion of money laundering or terrorist financing, or

(5) Any other unusual activity identified or detected.

Account opening is not guaranteed even if all processes and requirements are satisfied. PayBitoPro still has its own discretion to accept the application or not.

2. Failure to Complete

No service shall be provided to any applicant who fails to complete the KYC and CDD under this Procedure.

Any existing customer who fails to complete regular or irregular KYC and CDD under this Procedure shall be deemed as a fundamental breach of obligation by the customer, so the accessing services will at least be suspended tentatively or terminated completely.

3. Prohibited Customers

3.1. Customers from the jurisdictions and regions mentioned below will be blocked or declined because of the rationale and concern respectively. These jurisdictions and regions will be updated from time to time.

Subject to sanctions or embargoes imposed by the UN, EU, OFAC, and HMT:
Afghanistan, Belarus, Bosnia and Herzegovina, Burundi, Central African Republic, Cuba, Ethiopia, Guinea, Guinea-Bissau, Iran, Iraq, Lebanon, Libya, Mali, Myanmar, Nicaragua, North Korea, Republic of the Congo, Russia, Somalia, South Sudan, Sudan, Syria, Tunisia, Turkey, Ukraine, Venezuela, Yemen, and Zimbabwe

Subject to a Call for Action by Financial Action Task Force
(FATF): Democratic People's Republic of Korea and Iran

4. Documents and Information by Individual Account

An individual shall initiate the account application from registration verification in point 5.1.1 via App or Web and then complete the Identification and Verification processes by providing documents and information mentioned in point 5.1.2 to complete fundamental steps of KYC and CDD.

The applicant shall provide the following information via mobile applications or web browsers:

(1) Email
(2) Phone number
(3) Account password

The information needs to be verified by the system to finish the Registration Verification. After Verification, the applicant obtains limited access to the Customer Service team, and no transaction service will be provided yet.[1]

The applicant shall provide and upload the following documents and information via mobile applications or web browsers. Applicants obtain access to Basic Account after being identified, verified, and approved.

(1) One of these government-issued identity documents bearing the individual's photograph, an identification number and date of birth:

(a) Passport

(b) National Identity Card

(c) Driver's License

(2) Proof of residence issued within the last three months.

(3) Real-time live selfie of themselves

(4) Industry and occupation

Basic Account Customers can apply for the Premium Account by completing an additional form for more transaction services or a higher transaction limitation cap.

As needed, other relevant information or documents may be further collected for KYC and CDD purposes to evaluate the application comprehensively. PayBitoPro may ask applicants to submit sources of funds, transaction volume, annual income, net worth, details of employment, and so on.

5. Documents and Information by Non-Individuals Account

The representative of a non-individual customer (e.g. Corporate) shall initiate the account application from registration verification in point 6.1.1 via App or Web and then complete the Identification and Verification processes by providing documents and information mentioned in point 6.1.2 to complete fundamental steps of KYC and CDD.

The representative shall provide the following information via mobile applications or web browsers, and the information will be verified by the system to complete the Registration Verification. After Verification, the representative only has limited access to the Customer Service team and no transaction service will be provided yet.[2]

(1) Email

(2) Phone number

(3) Account password

The representative of a non-individual customer shall provide and upload the following documents and information via APP or Web, and then after being identified, verified, and approved to have access to Basic Account.

(1) Company data

(a) Company name

(b) Company registration number

(c) Country of incorporation

(d) Company registered address

(e) Company office address (if different from registered address)

(f) Company website (if applicable)

(g) Industry and business activity

(h) Purpose of account

(i) Bank account details (if necessary)

(j) Source of investment funds

(k) Annual revenue, profit and total company assets

(l) Estimated transaction volumes and frequency

(2) Company documents

(a) Certificate of Incorporation

(b) Memorandum and Articles of Association

(c) Business registration document or Certificate of Incumbency or company search report (issued within the last 6 months)

(d) Register of Directors

(e) Register of Shareholders

(f) Board Resolution or similar written authorisation to open an account with PayBitoPro

(g) Proof of Address (issued within the last 3 months showing company business address)

(h) If there are persons authorised to access and operate the account, Authorisation Letter indicating the capacity

(i) Identity documents of Beneficial Owners (such as the Board of Directors, Ultimate Beneficial Owners with more than 25%[3] shares of the company, and Authorised Persons): Selfie, Proof of Identification (such as passport, national ID or driver's license), and Proof of Address

(j) Proof of Address of Ultimate Beneficial Owners (UBOs)

(k) Selfie with holding their identity documents of the Beneficial Owners

(l) Proof of document supporting the source of investment funds (if necessary)

[3] 10% for high risk customers.

According to the request, information and documents provided during the account application, KYC and Compliance teams will consider and judge whether the Premium Account could be approved or not.

Other relevant information (and documents as needed) may be further collected for KYC and CDD purposes in order to evaluate the application comprehensively, e.g. documents of Board of Directors, additional information and source of funds of UBOs, AML Policy/Questionnaire as proof of compliance or audited financial statement as proof of source of funds.

Financial or Quasi-Financial Institutions shall additionally complete and provide the FCCQ document to complete the KYC and CDD process.

6. Identification and Verification (ID&V)

Anyone expecting to have services by PayBitoPro shall complete the KYC and CDD first.

Identification and verification (ID&V) are fundamental requirements of KYC and CDD which shall be completed via APP and Web designed by PayBitoPro.

Collection of Identity Evidence: Three types of identity evidence shall be collected and uploaded into the system via mobile applications or web browsers,

(1) A photo of the identity document of the prospective individual user or the representatives and beneficial owners of a non-individual user (e.g. passport, national identity card or driver's license),

(2) A real-time live selfie of themselves, and

(3) A photo of a proof of address (e.g. bill of water or gas, or banking statement) issued within the last 3 months.

Document Authenticity Check: The AI determines the authenticity of the customer's identity documents by comprehensive image analysis for signs of tampering or modification through the use of graphic editors. Each reviewed document receives a trust score. If any fraudulent or modified copy is detected, the AI will automatically flag fake or forged documents.

Text Recognition: The AI deploys an automatic recognition by extracting data from customer's identity documents (e.g. passport, national identity card or driver's license) and matches their data (e.g. full name, date of birth and address) against other documents (e.g. proof of address).

Facial Recognition: The AI compares the face on the customer's selfie with the identity document (e.g. passport, national identity card or driver's license) by an automatic confirmation of a match of the customer's face. The AI will render a confirmation result of "Match" or "Doesn't Match".

Additional Check: The AI also includes the following checks -

(1) Completeness of the identity documents;
(2) If photos have been retaken from a screen;
(3) Cross-check of all data from all submitted documents (name, date and place of birth and signature).
(4) Duplicate accounts.
(5) Address check.

Depending on the results of ID&V, the KYC team will and shall take different actions, including but not limited to declining the application directly, enquiring more information from the applicants, checking with KYC verification agency, or discussing with the Compliance team.

7. Prohibited and High-Risk Countries

The country risk of each customer is highly relevant to our risk. Thus, PayBitoPro includes the nationality of the customers and the country they live in.

In case either the nationality or country where our customers are located or live is treated

as a prohibited country, then the application will be declined during the ID&V process. Similarly, if

treated as a high-risk country, the KYC team will consider this factor and classify the customer's risk level pursuant to the Scoring Mechanism.

8. Prohibited and High-Risk Industries

Industry risk, including the occupation and the business nature, is highly relevant to each customer.

In case either the occupation or the business nature is treated as a prohibited industry, then the application will be declined. Similarly, if treated as a high-risk industry, the KYC team will consider this factor and classify the risk level of the customer pursuant to the Scoring Mechanism.

9. Beneficiary Owner (BO)

To reach the goal of ML/FT control, identifying the BO of the applicant is essential, whether they are Individual and Non-Individual customers. For non-individual customers, the identification of BO is mandatory and required via the information and documents collected.

PayBitoPro determines the BO of our customers via various methods, including applicants' voluntary disclosure, sales team's inquiry, and the KYC team screening process.

Shareholders owning more than 25% shares of the company will be deemed as BOs of the non-individual customer.

Anyone with significant influence on the Individual and Non-Individual customers shall be deemed as BO as well. Information and measures mentioned below are clues to consider. For example:

(1) An individual identified as a BO of a customer based on the ownership and control structure of the customer;

(2) A voluntary claim to act on behalf of the customer with identification and verification of their right of representation;

(3) Reasonable inference of a BO of a customer based on nature of business relationships and business transaction, as shown by the information available;

(4) Gathering information on whether a person is a politically exposed person (PEP), their family member or a person known to be close associates;

Anyone deemed or treated as a BO of the applicant shall provide his or her information and relevant documents to complete the ID&V process as well.

10. Name Screening

As an important part of the KYC and CDD, Name Screening is supported through KYC verification agency which provides vendor solutions and Watchlist Checks. The screening result shall be further reviewed by the KYC team. Name Screening shall check a customer's name against a commercial database for possible matches of PEPs, sanctions events, or adverse media with fuzzy matching capability. KYC verification agency uses a commercial database which is provided by ComplyAdvantage and includes the following lists:

(1) International sanction lists or blacklists from the FATF, the UN, EU, OFAC, and HMT,
(2) PEP lists covering 200+ countries,
(3) Criminal and law enforcement lists,
(4) Interpol wanted lists,
(5) Regulatory enforcement lists, and
(6) Adverse media.

The KYC team shall take appropriate actions to remove concern for any alert or reminder issued or triggered during identification, verification, or name screening. Furthermore, the KYC team shall report to the Head of Compliance to consider which actions shall be taken or not. If there is any suspicious activity found or the prospective customer is sanctioned (called "truly hit"), the application shall be declined directly.

11. Politically Exposed Persons (PEPs)

Recommended by the Financial Action Task Force ("FATF"), PEPs are deemed as persons with higher ML/FT risk because they always have powerful influence or more chances to facilitate or be exploited to suspicious or illegitimate activities.

PEP associates and relatives refer to the person who is not a PEP, however, having close relations with the PEP. For example, the family or secretary of a PEP might bring higher ML/FT risk. Therefore, PEP associates shall also be treated as PEPs.

Though not equivalent to prohibited or sanctioned users, more actions shall be taken before providing services to customers of PEPs. Specifically, PEPs shall be treated as high-risk level and Enhanced Due Diligence (EDD) shall be completed.

12. Adverse Media

Except for the Sanction or PEPs character, adverse media is also a significant factor which shall be considered to decide the ML/FT risk level of each user.

For any potential match of adverse media reminded, the KYC team shall browse the media and map the information collected to determine a true match or a false match. The mapping can be based on picture, full name, location, gender, age, education, working experience and so on.

If there is an uncertain concern on the adverse media and could not be removed, the KYC team shall consult with the Compliance team to determine what further action shall be taken.

The KYC team may seek advice from the Compliance team and shall input the logs of handling into the Compliance Case List which is designed to retain records of actions taken for potential match reminders.

Though any user with adverse media is accepted, the risk score shall be reflected to the ML/FT risk level.

13. Review and Approval

The KYC team shall review the ID&V result supported by KYC verification agency and ask the customer to further explain or provide more supplement if any deficiency or concern is detected. The action, process, and result of the further checking shall be inputted into the "KYC Compliance case", and then the Compliance team shall take a review to decide whether to accept the application.

If any concern on the ID&V result can't be removed, then the application shall be declined. If the concern is removed, the application can be accepted and the alert or reminder will be treated as "false hit".

ID&V is an essential part of the KYC and CDD process, so all applications shall be approved by the KYC team. However, if necessary, the KYC team shall further seek for additional approval by the Compliance team.

Any record or log is important to show the efforts on the AML/CFT framework. Therefore, all employees shall retain any record or log appropriately in place for any review or auditing purpose in the future.

14. Scoring Mechanism

A score shall be granted to each customer by the KYC team in accordance with the information and documents collected to decide the ML/TF risk level of each customer. If any concern of the score, the KYC team shall discuss with the Compliance team.
Hierarchy of scoring:

- below 39 is low-risk
- 40 to 79 is medium risk
- above 80 is high-risk

Factors and scoring covered under the Scoring Mechanism are listed below. The factors and scores mentioned will be updated or changed from time to time pursuant to the services provided and risk appetite borne.

(1) High-risk country, including nationality and POA: 80

(2) High-risk industry, including Industry and Occupation: 80

(3) PEP: 80

(4) Age: 30

(a) Individual: below 25 or above 65 years

(b) Corporate: registered or changed ownership within two years

(5) Adverse media (truly positive): 30

(6) Premium account[5]: 10

(7) BitCheck[6]: 10

(8) More than one Fiat Money: 10

15. Customer Risk Classification

All customers shall be assessed and classified into three categories corresponding to the due diligence measures commensurate with their ML/TF risks pursuant to Scoring Mechanism:

(1) Low-risk customer

(2) Medium risk customer

(3) High-risk customer

Customers though not belonging to the hierarchy of high risk but assessed other factors that may trigger other higher ML/TF risks. Rules of High-Risk Customer and Enhanced Due Diligence should be applied.

The KYC team shall input the classification into the system to monitor when and how to conduct ongoing KYC and CDD in the future.

Approval by the Head of Compliance is required to allow the high-risk customer on-boarding. The KYC team shall prepare the rationale and relevant evidence to support why to accept or decline the application.

16. Enhanced Due Diligence (EDD)

The KYC team shall provide the EDD form to applicable customers to complete the process. Relevant files or documents of EDD shall be reviewed and approved by the Head of Compliance and then filed by the KYC team.

If any, one or more of the following measures may be taken in order to manage and mitigate the ML/TF risk that is higher than usual:

(1) Obtain additional identification documents, data or information from credible and independent sources.

[5] Some services or higher transaction limitation caps will be provided to a premium account user only.

[6] BitCheck is a commercial escrow feature for both Fiat currencies and Cryptocurrencies exchanges between PayBitoPro's users.

(2) Gather additional information or documents on the purpose and nature of the business relationship.

(3) Gather additional information or documents for the purpose of identifying the source of funds and wealth of the customer.

(4) Gather information on the underlying reasons for planned or executed transactions.

(5) Increasing the number and frequency of control measures in monitoring customer relationships and/or transactions.

(6) Receiving permission from the Management team to establish or continue a business relationship.

17. Watch List

The control of the Watch List is designed to mitigate the ML/FT risk to those who bring higher risk, such as High-Risk Customer or Customers with adverse media.

After completing the KYC and CDD process, the KYC team shall input applicable users into the Watch List depending on different risk levels.

Users on the Watch List shall be monitored regularly by the Investigator to see whether any further actions shall be taken. For more details, please refer to the **Transaction Monitoring Procedure**.

18. Account Type

Basic Account:
Approved by the KYC team, then the customers will be allowed access to basic services provided.

Premium Account:
For more services or higher transaction limitation cap, customers can apply to upgrade to a premium account by submitting an application form, information or documents requested.

19. Ongoing KYC and CDD (Re-KYC)

To ensure the documents, data, and information previously collected from the customers are up-to-date, the KYC team shall undertake a regular review of existing records according to the following schedule:

(1) High-risk customers - every year.

(2) Medium risk customers - every two years.

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

In addition to the above periodic reviews, existing CDD records should be reviewed upon trigger events. Examples of trigger events include:

(1) Re-activation of a dormant account.

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

(3) When a significant transaction is to take place.[7]

(4) When a material change occurs in the way the customer's account is operated.

PayBitoPro will monitor customers' transactions to ensure that the transactions are reasonable to the knowledge of the customer and risk profile.

20. Review Process

The "last approved date" is the date a periodic review or an event-triggered review was completed previously. If the last approved date is not present or not recorded, the account opening date should be applied as the first date of the reviewing cycle.

The KYC team shall monthly check which customers to conduct the Re-KYC process and send the Re-KYC form to them according to the timeline mentioned in Ongoing CDD and KYC at least 30 days before the due date of previous CDD and KYC result.

The account shall at least be suspended tentatively or terminated directly, if:

(1) A periodic review can not be completed by the due date.

[7] "Significant" is not necessarily solely linked to monetary value. It may include transactions that are unusual or not in keeping with the expected behaviour of the customer. Significant transaction includes a wide range of transaction peculiarity, such as a deviation from the user's transactional volume or frequency.

(2) A triggered event review can not be completed within a reasonable time or more than one month.

21. Dormant Account

A dormant account is a control designed to make sure the resources are placed in the right group of customers. An account will be treated as a dormant account to be suspended after no activity more than 12 months or any exceptional situations determined by KYC and Compliance teams.

After being approached by PayBitoPro, Customers, who fail to update their information or to clarify concerns detected and no activity more than six months, will be deemed and tagged as a dormant account.

To reactivate the dormant account, the client must at least complete the Re-KYC process. The KYC team may need to collect more information or documents based on its risk evaluation.

22. Off-Boarding

It's the right of every user to terminate the business relationship and ask for account closing.

The KYC team shall be in charge of helping the user to complete the relevant process of closing the account, regardless of which contact the user reaches out to express their intent to close the account.

The Suspicious Transaction Reporting (STR) rule, along with other relevant policy and regulations, shall govern the issues of documentation and record-keeping when the customer begins and completes the off-boarding process.