PayBitoPro

Know Your Customer (KYC) and Customer Due Diligence (CDD) Policy

(UNITED ARAB EMIRATES)

July 2024

Table of Contents

Introduction and Purpose

To help PayBitoPro comply with the relevant laws and regulations in the UAE controlled by the Financial Action Task Force (FATF) and following the regulations of Central Bank of United Arab Emirates (CBUAE) and of VARA[1] through Virtual Assets and Related Activities Regulations 2023, PayBitoPro's best practice of Know Your Customer (KYC) and Customer Due Diligence (CDD) regulations which is subject to updates as and when relevant recommendations to the FATF Guidelines and the regulations of the CBUAE in compliance with the regulations of VARA through Virtual Assets and Related Activities Regulations 2023 is shown in this policy, which the KYC CDD procedure of PayBitoPro abides by.

In this Policy "we", "us", "our" means PayBitoPro and the terms "user", "individuals", "non-individuals" means the residents of the UAE and the business enterprises registered in the UAE licensed by CBUAE under Federal Decree Law No. 32 of 2021 on Commercial Companies from where the users of PayBitoPro reside and operate.

[1] The Virtual Assets Regulatory Authority (VARA) is the sole authority regulating virtual assets across Dubai's free zones and mainland, except within the jurisdiction of Dubai International Financial Centre (DIFC)- Law No. (4) of 2022 .

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

The purpose of this policy relating to KYC and CDD Rules and Regulations is to considerably reduce identity theft and fraudulent activities. PaybitoPro collects and verifies key data about the valuable customers to truly understand who they are.
Besides this, the importance of KYC and CDD regulations lies in the following cardinal points:

- Improved customer transparency and trust
- Reduced potential for money laundering and other scams
- Reduced legal risks
- Enhanced stability

This policy aims to meet all of the highest security standards and store Personal Identifiable Information (PII) securely in the system, implying that the clients will not have to bear the liability of any potential infraction or violation of law or leaked customer data but still have easy and reliable access to it whenever they need it.

Timing to Conduct

The KYC and CDD processes and requirements mentioned in this Procedure shall be conducted and completed by the KYC team[2] at PayBitoPro in any or all of the situations as cited below:

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

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

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

(4) In case of any suspicion of money laundering or terrorist financing, or

(5) Any other unusual activity identified or detected.

(6) In case of an occasional transaction, whether it is executed in a single operation or in several operations which appear to be linked, that amounts to a transfer of funds at least partially carried out by electronic means, exceeding EUR 15,000.

(7) Customer due diligence measures are also to be strictly applied in relation to a transfer of funds through PayBitoPro for making funds available to the customer including a credit transfer, a direct debit or a transfer carried out using an electronic money instrument or a mobile phone where the

[2] Section 2.4 of AML/CTF Regulations in CBUAE Rulebook

sum does not exceed EUR 1,000.

Additionally, KYC and CDD procedures are also conducted and applied in case of an occasional transaction in cash that amounts to EUR 15,000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked.[3]

Account opening shall not be guaranteed even if all processes and requirements are satisfied thereto. PayBitoPro still shall have its own discretion to accept the application.

Failure to Complete

No service shall be provided by PayitoPro to any applicant who fails to complete the KYC and CDD under this Procedure. PayBitoPro shall have full entitlement to cease or stop all kinds of operations with and/or for the client in case of failure of completion of KYC and CDD procedure under this policy. PayBitoPro shall also be liable to terminate such a relationship with the customer and file a Suspicious Transaction Report to the Financial Intelligence Unit (FIU) in relation to such a customer.

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

[3] FATF Recommendations, 2012

terminated completely and the customer shall also be liable to be levied a penalty. The customer might also be exposed to various regulatory risks and perils for which PayBitoPro shall not be held responsible for any such unforeseen circumstances.

Prohibited Customers

In any case identified as one where there is a high risk of money laundering or terrorist financing or Business relationship with any person established in a high-risk third country[4] or where PayBitoPro has determined that a customer or potential customer is a Politically Exposed Person (PEP), or a family member or known close associate of a PEP, they shall call for performance of Enhanced Customer Due Diligence Procedure[5].

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,

[4] High Risk Third country: Countries having High-Risk Jurisdictions and subject to a Call for Action, jurisdiction under increased monitoring, identified and recommended by Financial Action Task Force (FATF)

[5] FATF Recommendations, 2012

Yemen, and Zimbabwe.

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

Due to legal and compliance uncertainties: Japan, China, and Singapore

All the above-mentioned zones are tagged as High-Risk Zones for conduct of business for prevalent risk factors or other respective factors limited to that particular country or state. But as per the FATF Recommendations and guidelines of CBUAE regulated by VARA[6], the presence of one or more risk factors may not always indicate that there is a high risk of money laundering or terrorist financing in a particular situation. Therefore, PayBitoPro shall be at a complete liberty and shall have complete discretion to not cease transactions altogether based on a particular potential risk factor to continue business operations.

Documents and Information by Individual Account

An individual shall initiate the account application from registration verification via App or Web as mentioned below and then complete the Identification and Verification processes by providing documents and information mentioned further

[6] The Virtual Assets Regulatory Authority (VARA) is the sole authority regulating virtual assets across Dubai's free zones and mainland, except within the jurisdiction of Dubai International Financial Centre (DIFC) - Law No. (4) of 2022 .

in the following paragraph to complete fundamental steps of KYC and CDD.

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

(1) Name

(2) Address

(3) Place and Date of birth

(4) UAE Pass, Emirates ID, Emirates Facial Recognition or Passport number[7]

(5) Email

(6) Phone number

(7) Account password

The Applicant must also provide their Employment Information in the subsequent steps via their mobile applications or web browsers:

(1) Industry

(2) Occupation

(3) Source of Funds

(4) Employment Category

(5) Employment Type

(6) Annual Income

(7) Net Worth

(8) Transaction Volume

[7] National-level identification systems and processes currently in place or under development in the UAE

(9) If the Applicant is a Politically Exposed Person (PEP) or not

(10) Purpose of the account

(11) Current Banking Partner

(12) How long the Applicant had that banking relationship

The applicant shall also 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:

(2) UAE Pass, Emirates ID, Emirates Facial Recognition or Passport.

(3) National Identity Card

(4) Driver's License

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

(6) Real-time live selfie of themselves

(7) 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.

The information needs to be verified by the system to finish the Registration Verification, also known as Tier II Verification. After Tier II Verification and subsequent Approval by the designated officials at the KYC CDD Team of PayBitoPro, the applicant obtains access to the Customer Service team, and transaction services are provided henceforth.

As needed, other relevant information or documents may be further collected for KYC and CDD purposes to evaluate the application comprehensively.

Documents and Information by Non-Individuals Account

The representative of a non-individual customer (e.g. Corporate, Enterprise) initiates the account application from registration verification via PayBitoPro App or Web and then completes the Identification and Verification processes by providing documents and information to complete fundamental steps of KYC and CDD[8].

The representative of the non-individual customer 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.

(1) Name
(2) Country
(3) Email
(4) Phone number
(5) Account password

After Verification, the representative only shall have limited access to the Customer Service team and basic transaction service will be provided up to a

[8] Article 8 of AML-CFT Decision, UAE

limited transaction cap. 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.

Basic Company data

- Company name
- Company registration number
- Country of incorporation
- Corporate Structure
- Company registered address
- Company office address (if different from registered address)
- Company website (if applicable)
- Current Banking Partner
- Tenure of Business Relationship
- Description of Business
- Industry and business activity
- Purpose of account
- Profit
- Bank account details (if necessary)
- Source of investment funds
- Annual revenue, profit and total company assets
- Estimated transaction volumes and frequency

Company Registered Address

- Company Registered Name
- Company Registered City
- Company Registered State
- Company Registered Zip Code/PIN Code
- Company Registered Country

Company Office Address Information (If different from Registered Address)

- Company Registered Name
- Company Registered City
- Company Registered State
- Company Registered Zip Code/PIN Code
- Company Registered Country

Company documents

- Certificate of Incorporation
- Memorandum and Articles of Association or Incorporation
- Business registration document or Certificate of Incumbency or company search report (issued within the last 6 months)

- Register of Directors
- Memorandum or Operating Agreement
- Register of Shareholders
- Board Resolution or similar written authorisation to open an account with PayBitoPro
- Proof of Address (issued within the last 3 months showing company business address)
- If there are persons authorised to access and operate the account,
    - ❖ Authorisation Letter indicating the capacity
    - ❖ Identity documents of Beneficial Owners (such as the Board of Directors, Ultimate Beneficial Owners with more than 25% shares of the company, and Authorised Persons): Selfie, Proof of Identification (such as passport, national ID or driver's license), and Proof of Address.

Ultimate Beneficial Owner (UBO) Information[9]

- Name of the Owner
- Email
- Phone number
- Address of the Beneficiary Owner

[9]Provided in FATF Recommendations, 2012 and Section 2.5 of Guidance for Licensed Financial Institutions on Digital Identification for Customer Due Diligence by CBUAE

- Date and Place of Birth
- National Identity no. or Passport no.
- Percentage of Ownership
- If the Beneficiary Owner is a Politically Exposed Person
- Proof of Identity as approved by the National Authority
- Proof of Address as approved by the National Authority
- Selfie holding the identity document
- Proof of document supporting the Source of Investment

Bank Details of the Ultimate Beneficial Owner

- Beneficiary name
- Bank Name
- Bank address
- Account no.
- Account type
- Routing no.
- Swift code
- IFSC Code

According to the request, information and documents provided during the account application will be considered and judged by the KYC and Compliance teams as to 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.

Identification and Verification (ID&V)[10]

Anyone expecting to have services by PayBitoPro shall complete the KYC and CDD procedure first. Identification and Verification (ID&V) are fundamental requirements of KYC and CDD which shall be completed via APP and Web designed by PayBitoPro. PayBitoPro complies with the requirements as to verify the identity of the customer, any person purporting to act on behalf of the customer and any beneficial owner of the customer before the establishment of a business relationship or the carrying out of the transaction. But if the verification of the customer/applicant, any person purporting to act on behalf of the customer and the customer's beneficial owner as aforementioned, is completed as soon as practicable after contact is first established, the verification may be completed during the establishment of the business relationship under the following circumstances:

[10] Reliable, independent source documents, data or information will hereafter be referred to as "identification data and Article 8 of AML-CFT Decision

(a) this is necessary not to interrupt the normal conduct of business; and

(b) there is little risk of money laundering and terrorist financing.

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: PayBitoPro determines the authenticity of the customer's identity documents by comprehensive image analysis for signs of tampering or modification through the use of editors. If any fraudulent or modified copy is detected, the AI will automatically flag fake or forged documents.

Text Recognition: PayBitoPro 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 at PayBitoPro 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

Confirmation result will be rendered of “Match” or “Doesn’t Match”.

Additional Check: The AI at PayBitoPro also includes the following checks -

1. Completion 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 take different actions, including but not limited to declining the application directly, enquiring more information from the applicants, or discussing with the Compliance team to finally allow the Applicant to commence business using PayBitoPro.

Prohibited and High-Risk Countries

The country risk of each customer is highly relevant to the risk taken by PayBitoPro. Thus, PayBitoPro includes the nationality of the customers and the country they live in. As per the FATF Recommendations in 2012 and of the subsequent years, the High Risk third countries which were termed as such because of either being subject to financial sanctions measures by the FIU, or by competent authorities like FATF, which required firms to take additional

measures, or require an onsite visit to verify if their action plan has been completed, or the Financial Action Task Force (FATF) was unable to conduct an onsite visit due to security issues which were later removed in 2024 defining High Risk Countries as countries named on either of the following lists published by the Financial Action Task Force as they have effect from time to time:

1. high-risk jurisdictions subject to a call for action
2. jurisdictions under increased monitoring

In case either the nationality or country where the 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 as per the latest FATF plenary meeting, the KYC team will consider this factor and classify the customer's risk level pursuant to the Scoring Mechanism.

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 at PayBitoPro will consider this factor and classify the risk level of the customer pursuant to the Scoring Mechanism. The table below shows the relevant industries for reference which are checked for risk scores.

Industry
Accounting
Aviation/Airlines
Alternate Dispute Resolution
Alternative Medicine
Animation
Apparel and fashion
Architecture and Planning
Arts and Craft
Automotive
Aviation and Aerospace
Banking
Biotechnology
Broadcast Media
Building Materials
Business Supplies and Equipments
Capital Markets
Chemicals
Civic and Social Organization
Civil Engineering

Commercial Real Estate
Computer and Network Security
Computer games
Computer Hardware
Computer Networking
Computer Software
Construction
Consumer Electronics
Consumer Goods
Consumer Services
Cosmetics
Dairy
Defence and Space
Design
Education Management
e-learning
Electrical and electronic manufacturing
Entertainment
Environmental Services
Events Services
Executive Office

Facilities Services
Farming
Financial Services
Fine Art
Fishery
Food and Beverages
Food Production
Fundraising
Furniture
Gambling and Casinos
Glass, Concrete and Ceramics
Govt. Administration
Govt. Relations
Graphic Design
Health, Wellness and Fitness
Higher Education
Hospital and Health Care
Hospitality
Human Resource
Import and Export
Individual and Family Services

Industrial Automation
Information Services
Information Technology and Services
Insurance
International Affairs
International Trade and Development
Internet
Investment Banking/Venture
Investment Management
Judiciary
Law enforcement
Law Practice
Legal Service
Legislative Office
Leisure and Travel
Library
Logistics and Supply Chain
Luxury goods and jewellery
Machinery
Management Consulting
Maritime

Marketing and Advertising
Market Research
Mechanical or Industrial Engineering
Media Production
Medical Device
Medical Practice
Mental Health Care
Military
Mining & Metals
Motion Pictures & Film
Museums & Institutions
Music
Nanotechnology
Newspapers
Nonprofit Organization Management
Oil & Energy
Online Publishing
Outsourcing/Offshoring
Package/Freight Delivery
Packaging & Containers
Paper & Forest Products

Performing Arts
Pharmaceuticals
Philanthropy
Photography
Plastics
Political Organisation
Primary/Secondary
Printing
Professional Training
Program Development
Public Policy
Public Relations
Public Safety
Publishing
Railroad Manufacture
Ranching
Real Estate
Recreational
Facilities & Services
Religious Institutions
Renewables & Environment

Research
Restaurants
Retail
Security & Investigations
Semiconductors
Shipbuilding
Sporting Goods
Sports
Staffing & Recruiting
Supermarkets
Telecommunications
Textiles
Think Tanks
Tobacco
Translation & Localization
Transportation/Trucking/Railroad
Utilities
Venture Capital
Veterinary
Warehousing
Wholesale

Wine & Spirits
Wireless
Writing & Editing

Ultimate Beneficiary Owner (UBO)[11]

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

PayBitoPro determines the UBO of the customers via various methods, including applicants' voluntary disclosure, sales team's inquiry, and the KYC team screening process. This helps to verify if an ultimate beneficial owner is a real person who is accurately representing himself. It also checks if that person is conducting legitimate business, including getting their funds from non-criminal sources. It is ensured by the states within the UAE where PayBitoPro provides service that the information on Beneficial Ownership is accessible to the competent authorities like FATF and the respective FIUs.

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

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

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

[11] FATF Recommendations, 2012

(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 UBO 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;

Basic details that should be recorded about any ultimate beneficial owner here at PayBitoPro include:

- Full name
- Title
- Date of birth
- Country of residence
- Home address
- Citizenship
- UAE Pass or Emirates ID or Emirates Facial Recognition
- Passport number
- Any other ID issued by a Federal Government

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

Name Screening

As an important part of the KYC and CDD, Name Screening is supported through the KYC verification team 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 team at PayBitoPro uses a commercial database by including 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.

Name screening has a practical application in the operation of PayBitoPro, particularly in preventing money laundering, enhancing KYC processes, and mitigating fraud and financial crimes. By incorporating name screening into the workflows, PayBitoPro strengthens due diligence measures by identifying potential risks associated with customers or transactions, and takes appropriate actions to mitigate those risks encompassing and not limited to money laundering and terrorist financing activities. By screening the names of customers, beneficiaries, and related parties against government sanctions lists and watchlists, PayBitoPro identifies individuals or entities with known links to illicit activities and takes appropriate measures to prevent their involvement by conducting comprehensive screenings during customer onboarding. By cross-referencing names against adverse media databases and internal watchlists, PayBitoPro identifies individuals or entities associated with previous fraudulent activities or negative reputations. PayBitoPro performs the Name Screening process by the following methods:

- **Conducting Comprehensive Name Screening**

PayBitoPro conducts comprehensive name screenings that cover a wide range of data sources, including government sanctions lists, PEP lists, internal watchlists, and adverse media databases.

- **Utilising Advanced Screening Technologies**

Advanced screening technologies used at PayBitoPro enhances the efficiency and effectiveness of name-screening processes which utilise sophisticated algorithms and nebulous matching techniques to accurately identify potential matches.

- **Implementing Risk-Based Approaches**

A risk-based approach to name screening conducted by PayBitoPro involves assessing the level of risk associated with each customer or transaction and applying appropriate screening measures accordingly pertaining to high-risk and low-risk customers and transactions respectively.

- **Regularly Updating Data Sources**

Name screening at PayBitoPro always ensures that the data sources are up-to-date and regularly refreshed.

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, the application shall be declined directly.

Politically Exposed Persons (PEPs)[12]

Recommended by the Financial Action Task Force ("FATF") and the guidelines of CBUAE, 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. In determining what risk-management systems and procedures are appropriate for a beneficial owner or customer, PayBitoPro takes account of—

- the risk assessment performed to evaluate the risks of money laundering and terrorist financing; and
- the extent to which the risk would be heightened by the business relationship or transactions carried out by PayBitoPro with a PEP or a family member or known close associate of a PEP.

If PayBitoPro has ascertained that a customer or a potential customer is a PEP, or a family member or known close associate of a PEP[13], PayBitoPro shall assess—

[12] FATF Recommendations, 2012 and Article 15 of the AML-CFT Decision
[13] PEP associates and relatives (Related Customers) refer to a person who is not a PEP, however, having close relations with the PEP.

- the level of risk associated with that customer, and
- the extent of the enhanced customer due diligence (enhanced CDD) measures to be applied in regards to that customer.

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.

Adverse Media

Adverse media refers to negative or unfavourable information about individuals, entities, or organisations that could indicate potential involvement in financial crimes, corruption, or other illicit activities. Except for the Sanction or PEPs character, adverse media is also a significant factor which is considered to decide the ML/FT risk level of each user. PayBitoPro includes structured adverse media, presented within the database, helping the clients identify entities and individuals reported in the reputable media as being accused, investigated, arrested, or convicted of specific offences.

For any potential match of adverse media, 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 other set criteria pursuant to the procedures and risk-based approach by setting parameters to filter via secondary identifiers, keywords, categories, sub-categories, location and more.

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

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.

Review and Approval

The KYC team at PayBitoPro reviews the ID&V result and asks 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 cases, and then the Compliance team reviews to decide whether to accept the application. If there persists any concern that 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 a false hit. ID&V is an essential part of the KYC and CDD process, so all applications shall be verified and if found viable, approved by the KYC team. However, if necessary, the KYC team shall further seek for additional approval of the Compliance team who shall align ongoing monitoring with risk policies.

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.

Scoring Mechanism

The KYC Team at PayBitoPro grants a score to each customer in accordance with the information and documents collected to decide the ML/TF risk level of each customer. These are considered, clearly articulated and recorded across the risk assessment and due diligence is readily performed. If any concern of the score, the KYC team shall discuss with the Compliance team without delay.

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 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[14]: 10

[14] Some services or a higher transaction cap will be provided to a premium account user only

7. More than one Fiat Money: 10.7.
8. BitCheck[15]: 10

The table tabulated below shows the various parameters on which Risk Score weightage of Individuals pertaining to the basic heads is calculated:

Sl. No	**Parameter**
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	PEP
12	Person Relation with bank of Fl
13	Purpose of Account

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

14	Person Watchlist
15	Person Negative News

Customer Risk Classification

PayBitoPro uses deep learning to understand the details of each customer and the broader context they operate in, delivering actionable insights in seconds with much fewer false positives. All customers of PayBitoPro thus shall be assessed and classified into three categories as per the FATF guidelines 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

Rules of High-Risk Customer and Enhanced Due Diligence is applied by PayBitoPro by adapting to changes in sanctions and other regulatory requirements.

The KYC team shall input the classification into the system to monitor when and how to conduct ongoing KYC and CDD in the future. The respective FIUs, through the Joint Committee, shall issue an opinion on the risks of money laundering and terrorist financing affecting the Union's financial sector (the 'joint opinion'). Thereafter, the ESAs, through the Joint Committee, shall issue an opinion every two years.

The Head of Compliance approves to allow the high-risk customer while on-boarding. The KYC team prepares the report and relevant evidence in regards to acceptance or decline of the application.

Enhanced Due Diligence (EDD)

PayBitoPro duly applies Enhanced Customer Due Diligence measures and enhanced ongoing monitoring, in addition to the customer due diligence measures to manage and mitigate the risks arising in any case identified by PayBitoPro itself or in information made available to PayBitoPro, as one where there is a high risk of money laundering or terrorist financing. PayBitoPro has in place appropriate risk-management systems and procedures in case of a customer or the beneficial owner of a customer being a PEP or a family member or a known close associate of a PEP, and efficiently manages the enhanced risks arising from the business relationship or transactions with such a customer with expertise and prowess.

In case of scenarios requiring Enhanced Due Diligence (EDD) Procedure, KYC team shall provide the EDD form to applicable customers to complete the process taking into consideration but not limited to the risk assessment it carried out, the level of risk of money laundering and terrorist financing inherent in its business, the extent to which that risk would be increased by its business relationship or transactions with a PEP, or a family member or known close associate of a PEP and any relevant information in custody of PayBitoPro. Relevant files or documents of EDD shall be reviewed exhaustively and approved by the Head of Compliance Team and then filed by the KYC team.

The following measures are taken by PayBitoPro 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.

(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.

Watch List

PayBitoPro designs the control of the Watch List 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. PayBitoPro complies with KYC and CDD Procedure abiding by Anti Money Laundering Directives. Watchlist Screening provides powerful protection by screening users and other businesses against the common global watchlists and adverse media sources. The Watchlist Screening at PayBitoPro works in the following chain:

- Collection of data
- Identifying High-Risk Profiles
- Divulging into global intelligence by flagging enterprises and individuals when they appear in the global adverse media and list search
- Staying ahead of tentative risks by an on-going monitoring for safety and compliance
- Simplifying workflows and integrations

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"**.

Account Type

Basic Account:

The Applicant/customer after a successful login and entry of required details as aforementioned in this instant policy shall be approved to invest and obtain the basic services from PayBitoPro by the KYC team if deemed fit and proper. Once the KYC team passes the customer portfolio to the Compliance team, the Compliance team shall approve the same following which the customers will be allowed access to basic services provided.

Premium Account:

PayBitoPro customers can apply to upgrade to a premium account by submitting an application form, information or documents requested for more services, increased trading limits or higher transaction limitation cap with lesser trading fees. The Applicant/customer can apply for upgradation after a successful login and entry of required details as aforementioned, shall be approved to invest and obtain the basic and premium services from PayBitoPro by the KYC team if deemed fit and proper. Once the KYC team passes the customer portfolio to the Compliance team, the Compliance team shall approve the same following which the customers will be allowed access to basic and premium services provided.

Ongoing Monitoring

PayBitoPro offers a risk-based approach to maintaining Customer Due Diligence (CDD) information which involves monitoring accounts and transactions for risk patterns, and routinely verifying and updating client information. Ongoing

Monitoring is a critical component of effective CDD procedure which is ensured at PayBitoPro involving:

- Systematic review of accounts, transactions, and risks
- Understanding account status, even in real time
- Identifying transactions that deviate from the regular pattern of activity
- Valuing and updating client information

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:

- High-risk customers - every year.
- Medium risk customers - every two years.
- 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:

- Re-activation of a dormant account.
- Change in the beneficial ownership or control of the account.
- When a significant transaction is to take place ("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)
- 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.

Reporting

PayBitoPro provides information about compliance in regards to Money Laundering and Terrorist Financing, Customer Due Diligence, Reliance and Record Keeping, Ultimate Beneficial Owner Information and Cryptoasset Transfers to the Financial Intelligence Unit (FIU), being the Supervisory Authority pertaining to financial service industry which is imperative to calculate charges for cost of supervision, or is reasonably required by the FIU in connection to conduct any of its supervisory functions. The compliance information is provided to the FIU by PayBitoPro at a stipulated time as per the directions of the FIU of that particular member state where the users of PayBitoPro reside and operate in such form and manner as deemed fit. But PayBitoPro shall not be liable or be compelled to disclose information about conducting activities pertaining to money laundering and terrorist financing analysis to the customers of PayBitoPro.[16]

Review Process

Review process at PayBitoPro involves a comprehensive analysis that spans various facets of a project, including its market potential, tokenomics, team credibility,

[16] FATF Recommendations, 2012

technological innovation, and competitive positioning. The “last approved date” is the date a periodic review or an event-triggered review was completed previously at PayBitoPro. 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.
2. A triggered event review can not be completed within a reasonable time or more than one month.

Dormant Account

A dormant account is a control designed by PayBitoPro 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 6 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 and all the relevant access previously given to the customer will be blocked. 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.

Off-Boarding

It's the right of every user to terminate the business relationship and ask for account closing. The KYC team at PayBitoPro is 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.

Changes to this Privacy Policy

PayBitoPro updates its privacy policy from time to time. Any changes whatsoever shall be notified to the customers of PayBitoPro by posting the new Privacy Policy on this page. The customers are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page on the PayBitoPro Website.

Contact

For any query about this Policy, the contact information is given below:

● By visiting this page on the PayBitoPro website: [*www.paybitopro.com*]

● By sending an email: [*compliance@paybitopro.com]*