PayBitoPro

Counter Terrorism Financing (CTF) Policy

(AUSTRALIA)

Created by:	Avisek Banerjee
Approved by:	Suchismita Chakrabarti
Documentation Version:	2.2
Submission Date:	15th May, 2024

TABLE OF CONTENTS

INTRODUCTION 3
POLICY SCOPE 3
DEFINITIONS 4
Terrorism Financing: 4
Proliferation Financing 5
RISK BASED APPROACH 6
COUNTER TERRORISM FINANCING PROGRAM 7
CUSTOMER DUE DILIGENCE PROCEDURES 8
EMPLOYEE DUE DILIGENCE 9
NAME SCREENING 10
INDEPENDENT REVIEW/TESTING OF THE CTF PROGRAM,PROCEDURE 11
RECORD RETENTION 12
SUSPICIOUS TRANSACTION REPORTING 13

INTRODUCTION

The CTF policy of PayBitoPro underscores the company's dedication to combating money laundering, terrorism financing, and related illicit activities. It outlines the measures implemented to prevent users from exploiting its services for criminal purposes, aligning with pertinent Australia's laws such as Anti-Money Laundering and Counter-Terrorism Financing Act 2006, Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007, The Criminal Code Act 1995 (Criminal Code) 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 Australia and the business enterprises registered in Australia under the Corporations Act, 2001.

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

POLICY SCOPE

This Policy aims to outline the guiding principles and framework governing PayBitoPro's procedures, processes, and systems dedicated to identifying, prohibiting, and thwarting potential instances of terrorism financing.

Additionally, it serves as a tool to familiarize PayBitoPro's representatives with the relevant laws of Australia pertaining to the terrorism financing.

The Representatives of PayBitoPro are obligated to stay informed about and comply with the latest requirements outlined in this Policy, alongside other internal procedures of PayBitoPro and/or the applicable laws of Australia. The Chief Compliance Officer is tasked with periodically reviewing the Policy to ensure its compliance with legal requirements and industry best practices. Additionally, the Managing Director of PayBitoPro is responsible for promptly disseminating all internal policies, procedures, and amendments to all Representatives following their approval by the relevant governing body which is the Australian Transaction Reports and Analysis Centre (AUSTRAC).

The Policy conforms to the national regulations of Australia and extends to compliance with International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. This includes adherence to the FATF Forty Recommendations and Special Recommendations on Terrorism Financing, as well as the FATF Standards on AML Principles and best international practices for combating money laundering and terrorism financing.

DEFINITIONS

Terrorism Financing:

> Terrorism financing, as defined in the United Nations International Convention for the Suppression of the Financing of Terrorism (1999), involves any action by an individual who, knowingly and unlawfully, either directly or indirectly, provides or gathers funds with the intention or awareness that they will be utilized, wholly or partially, to carry out:

- An act classified as a terrorist act[1] under the Criminal Code Act 1995 (the Criminal Code) or;
- Any additional action with the intent to cause death or severe bodily harm to a civilian or any non-combatant in an armed conflict scenario, designed to intimidate a population or compel a government or international organization to act or refrain from acting.

Terrorist activities are primarily financed through two sources. The first source involves acquiring financial support from countries, organizations, or individuals, while the second source consists of revenue-generating activities.

Proliferation Financing

Proliferation financing means the act of providing funds or financial service, which are used or will be used, in whole or in part:

- for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling of weapons or,
- for the use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non- legitimate purposes), that contravenes any laws of Australia.

In order for terrorists and terrorist organizations to acquire weapons of mass destruction, they must possess adequate funds and access to financial services for purchasing such weaponry. PayBitoPro is responsible for ensuring that our

[1] Division 101 of the Criminal Code Act 1995 (the Criminal Code)

business operations, services are not misused by terrorists and terrorist organizations to funnel funds to weapons suppliers.

Hence, PayBitoPro ensures that its CTF program is robust, comprehensive, and efficient in identifying and reporting proliferation financing to the appropriate supervisory authority in compliance with relevant legal statutes.

RISK BASED APPROACH

As a digital asset services provider, PayBitoPro acknowledges the existence of Terrorism Financing (TF) risks, which could potentially involve its services and products in facilitating money laundering or terrorist financing schemes. Alongside the regulatory risks of non-compliance with legislation, these TF risks may impact PayBitoPro's business, including its reputation and license.

The risk of exposure to terrorism financing varies across customers, countries, products, services, and over time. High-risk situations require stronger controls compared to lower-risk situations. To effectively manage and mitigate these risks, a risk-based approach is implemented. This approach prioritizes the allocation of resources to address the most significant risks.

In accordance with the relevant laws, PayBitoPro's assessment of its exposure to TF adheres to a risk-based approach. PayBitoPro has evaluated and will persist in assessing and quantifying TF risks by considering the risks associated with the following factors:

- its customer types
- the types of designated services it provides
- the methods by which it delivers designated services;
- the foreign jurisdictions with which it deals; and
- the staff recruitment and retention

COUNTER TERRORISM FINANCING PROGRAM

As per the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 & Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007, and as per the AUSTRAC guidelines it is mandatory for a Digital asset service provider to establish and adhere to an AML & CTF Program hence PayBitoPro's AML & CTF Program has been designed, as per the regulations. The AML & CTF Program is applicable to all Representatives of PayBitoPro. The policies, processes and procedures:

- To implement the transaction and activity reporting requirements,
- To implement customer due diligence requirements,
- To implement the record keeping requirements,
- To inform PayBitoPro's officers and employees of the laws of Australia about money laundering and financing of terrorism, of the policies, processes, procedures and systems adopted by the entity to deal with money laundering and financing of terrorism,
- To train the entity's officers and employees to recognize and deal with money laundering and terrorism financing,
- On the role and responsibility of AML and ATF Compliance officer,
- On the establishment of an independent audit function which is able to test its AML & CTF processes, procedures and systems,
- On the adoption of systems by PayBitoPro to deal with money laundering and terrorism financing, on the staff screening, recruitment and retention program.

The core aim of the AML & CTF Program is to recognize, alleviate, and oversee the risk that PayBitoPro may encounter (whether intentionally or inadvertently) by enabling money laundering or terrorism financing through the provision of its designated services.

The primary purpose of the AML & CTF Program is to set out the applicable customer identification and verification procedures for customers of PayBitoPro.

CUSTOMER DUE DILIGENCE PROCEDURES

The KYC and CDD process is a mandate before the on-boarding of the customer[2]. 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.

[2] Division 4, Section 32 Anti-Money Laundering and Counter-Terrorism Financing Act 2006

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 by the Australian Transaction Reports and Analysis Centre (AUSTRAC).

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 regulatory authorities[3] which is the Australian Transaction Reports and Analysis Centre (AUSTRAC).

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

EMPLOYEE DUE DILIGENCE

PayBitoPro will also enforce thorough supervision procedures to authenticate the identity and previous record of prospective employees. Recognizing the potential risk due to staff turnover, PayBitoPro has instituted protocols for training, monitoring, and applying transactional limits to new staff members (or existing

[3] Part 3, Division 2, Section 41 of Anti-Money Laundering and Counter-Terrorism Financing Act 2006

staff members elevated to roles with heightened AML & CTF duties). Comprehensive training on the company's policies and procedures is mandatory at different points in employment.

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.

INDEPENDENT REVIEW/TESTING OF THE CTF PROGRAM, PROCEDURE

A review of the CTF Program will be undertaken at least annually also in case of important changes of legal acts.

PayBitoPro will set up an independent internal audit function (or opt for outsourcing to a third-party provider) to evaluate its CTF processes, procedures,

and systems. This review and testing will be conducted either internally by a person independent from business units and the PayBitoPro's CTF Compliance Officers, such as an internal auditor, or by an external service provider engaged specifically for this purpose.

The purposes of the review will be to:

- Assess the effectiveness of the AML & CTF Program having specific regard to the ML/TF risk faced by PayBitoPro;
- Assess whether the CTF Program complies with the AML & CTF Rules;
- Assess whether the CTF Program has been effectively implemented; and
- Assess whether PayBitoPro has complied with the CTF Program.

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 Seven 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 Seven years after the completion of a transaction.

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

SUSPICIOUS TRANSACTION 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 24 (Twenty Four) hours or 3 (Three) business days depending on the matter from the date of identifying the activity, submit a suspicious transaction report (STR) to the appropriate supervisory authority which is the Australian Transaction Reports and Analysis Centre (AUSTRAC)[4].

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

After submission of the STR to the appropriate regulatory authority (AUSTRAC), 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.

[4] Part 3, Division 2, Section 41 of Anti-Money Laundering and Counter-Terrorism Financing Act 2006

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 (AUSTRAC), but not later than 3 (Three) business days from the date of identifying / recognizing such activity.

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