PayBitoPro

Counter Proliferation Financing (CPF) Policy

UNITED STATES OF AMERICA (USA)

June 2024

TABLE OF CONTENTS

INTRODUCTION

The Counter Proliferation Financing (CPF) policy of PayBitoPro underscores the company's dedication to combating money laundering, terrorism financing, proliferation financing, financing for weapons of mass destruction (WMDs)[1] and related illicit activities. It outlines the measures implemented to prevent users from exploiting its services for criminal purposes by integrating into broader anti-money laundering (AML) and counter-terrorism financing (CTF) laws and regulations in the United States such as The Bank Secrecy Act, 1970, Anti Money Laundering Act, 2020, Patriot Act, 2001, Sanctions Act (P.L. 115-44) as amended by Section 6506 of the Fiscal Year 2022 National Defense Authorization Act (P.L. 117-81) and other relevant regulations like United Nations Security Council (UNSC) Resolutions. PayBitoPro has developed this policy from the aforementioned legislations and laws to ensure trading transparency and to safeguard against terrorism financing and unlawful practices.

[1] For a definition of WMD, see Crimes and Criminal Procedure, U.S. Code 18 (2001) § 2332a (c)(2)(A-D).

In this Policy “we”, “us”, “our” means PayBitoPro and the terms “user”, “individuals”, “non-individuals” means the residents of the USA and the business enterprises registered in the USA under the Model Business Corporation Act, 1984[2]. The CPF 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 CPF Policy. Your use of the Online Platforms implies your explicit acknowledgment and adherence to the User Terms and Conditions and, consequently, this CPF 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 proliferation financing. Additionally, it serves as a tool to familiarize PayBitoPro’s representatives with the relevant laws of the United States pertaining to the terrorism financing.

[2] Amended and revised last in 2016, published in Dec 9th, 2017

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 the United States. 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 Financial Crimes Enforcement Network (FinCEN) and Financial Action Task Force (FATF).

The Policy conforms to the national regulations of the US 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 and proliferation financing.

DEFINITIONS

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 the USA.

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

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

RISK BASED APPROACH

As a digital asset services provider, PayBitoPro acknowledges the existence of Terrorism Financing (TF) / Proliferation Financing (PF) 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 / PF risks may impact PayBitoPro's business, including its reputation and license.

The risk of exposure to Proliferation 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 PF adheres to a risk-based approach. PayBitoPro has evaluated and will persist in assessing and quantifying PF 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 PROLIFERATION FINANCING PROGRAM

As per the statutory regulations and guidelines[3], it is obligatory 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 are created:

- 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 the United States 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,

[3] U.S. law and Executive Orders 13382 (Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters) and 13551 (Blocking Property of Certain Persons with Respect to North Korea), UN Security Council Resolution 1540

- 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 along with CPF 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 along with the CPF Program is to set out the applicable customer identification and verification procedures for customers of PayBitoPro.

COUNTRIES HAVING HIGH RISKS OF PROLIFERATION FINANCING

PayBitoPro assesses the Proliferation Financing (PF) risks based on the geography where the risks are higher. Over the review period, the United States has seen persistent efforts by Proliferation networks, operating on behalf or at the direction of state actors, including the Russian Federation, Democratic People's Republic of Korea (DPRK), Iran, the People's Republic of China (PRC), Syria, and Pakistan, to exploit the U.S. financial system and other U.S. private sector actors to finance WMD proliferation. Therefore, it is made sure that if the transactions are being made from any of the mentioned countries then it goes through various checks which includes name screening, account monitoring, transaction monitoring, flagging the transactions made from the listed country, on-going monitoring and enhanced KYC / CDD measures are taken[4].

The countries listed below are:

- Russia and proliferation financing risks:

  Russia possesses the largest nuclear stockpile globally, coupled with a substantial military presence. It has collaborated with its allies and partners to reinforce its conventional weaponry while also augmenting its reliance on nuclear, cyber, and space capabilities.

[4] FinCEN and BIS, "FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Announce New Reporting Key Term and Highlight Red Flags Relating to Global Evasion of U.S. Export Controls."

Russia is giving precedence to the illicit acquisition of goods and technologies, violating international sanctions and aiding in the proliferation of weapons of mass destruction (WMD)[5]. Russian proliferation financing networks utilize front and shell companies to place orders for necessary components. These networks frequently obscure the end-user and destination for the goods, redirecting shipments through third countries before ultimately delivering them to customers in Russia.

- North Korea and proliferation financing risks:

  North Korea, officially known as the Democratic People's Republic of Korea (DPRK), has been conducting tests involving Intercontinental Ballistic Missiles (ICBMs) and military satellite launch technology. The regime in Pyongyang considers the possession and acquisition of nuclear weapons crucial for its survival, focusing primarily on enhancing its nuclear capabilities and maintaining its arsenal.

  North Korea is actively involved in cybercrime and illicit trade to fund its illicit Weapons of Mass Destruction (WMD) program. The country has sought to acquire up to $2 billion through cybercrime networks.

- Iran and proliferation financing risks:

[5]The new amendment to E.O. 14024 authorizes the imposition of U.S. sanctions on foreign financial institutions that are either (1) facilitating significant transactions on behalf of persons designated for operating in certain key sectors of the Russian economy that support the country's military-industrial base; or (2) facilitating significant transactions or providing services involving Russia's military-industrial base, including those relating to specific manufacturing inputs and technological materials that Russia is seeking to obtain from foreign sources

Iran is enlarging its uranium stockpile and elevating its enrichment level, alongside conducting advanced research and development on centrifuges, all with the intention of acquiring a nuclear weapon. Additionally, Iran has effectively pulled out of the Non-Proliferation Treaty Safeguards Agreement.

Iran has a significant role as a financial and military supporter of sanctioned terrorist groups, including Hezbollah and Hamas. Transactions linked to Iran are crucial for terrorist financing.

- China and proliferation financing risks:

China has pledged to bolster its "strategic deterrent" and has expedited the modernization, diversification, and augmentation of its nuclear forces. Concurrently, China is advancing its cyber, space, and counter space capabilities. Additionally, China is involved in economic espionage and cyber theft aimed at pilfering technology.

- Syria and proliferation financing risks:

The Assad regime in Syria is recognized for its utilization of chemical weapons, classified as weapons of mass destruction, which are obtained through proliferation financing. Syria's capabilities have been partially developed through illicit procurement and fundraising activities. There is a notable export and sanctions risk associated with Syria. The sale of oil

and other petrochemicals to Syria generates substantial proliferation financing income for the Iranian regime.

- Pakistan and proliferation financing risks:

  In October 2023, the United States, for the first time, imposed blocking sanctions under E.O. 13382 on three PRC-based suppliers to Pakistan's ballistic missile program.[6] While the PRC[7] remains a key defense partner for Pakistan, individuals and entities acting on behalf of Pakistan have engaged in illicit procurement for specific U.S.-origin goods, violating relevant U.S. export control laws and where the underlying transactions have passed through U.S. financial institutions. Pakistan is persisting in the development of ballistic missiles, which includes acquiring technology and materials from China. Several individuals and entities associated with Pakistan have endeavored to engage in the illicit procurement of sanctioned materials and technology.

[6] Department of State, "United States Sanctions Entities Contributing to Ballistic Missile Proliferation.

[7] PRC- People's Republic of China

CONDUCTING PROLIFERATION FINANCING ASSESSMENT ON GEOGRAPHIC RISKS

There are a number of factors that PayBitoPro assesses when considering the geographic risk of Proliferation Financing (PF). PayBitoPro follows the methodologies which has been mentioned in the FATF:

1. Country score: Restricted
    - The country is under UN sanctions, notably North Korea and Iran.
    - The country faces other sanctions, such as those related to China, Syria, Russia, and Pakistan.
    - The country maintains a considerable corporate and trade network with state or ties to sanctioned countries.
    - The country offers flags of convenience or passports of convenience for shipping.
    - The country is listed on FATF's "high-risk country list" and/or the "grey list."
    - Intelligence indicates that the country may be contemplating the development of a nuclear capability through illicit procurement.

2. Country score: Medium-High
    - The country is identified as a known location for diversion, with a low effectiveness score in mutual evaluation reports.
    - The geographical proximity to a proliferating country raises concerns.
    - The country has been named by the UN Panel of Experts (UNPoE), Office of Foreign Assets Control (OFAC), and mainstream media for either trading with sanctioned states or lacking transparency in trade patterns.
    - The country fails to respond to UNPoE inquiries
    - The country is not a party to the Nuclear Non-Proliferation Treaty and is either maintaining, improving, or expected to maintain or improve its nuclear capabilities.
    - A proliferating state has diplomatic representation in the country.

3. Country Score: Medium Low
    - The country is adjacent to a proliferating state.
    - The country has a significant diaspora from a state of proliferation concern.
    - Country hosts a financial, trade center, or transshipment hub that appeals to proliferation financiers.
    - The jurisdiction is characterized by a manufacturing sector producing goods controlled by international supplier regimes

related to Weapons of Mass Destruction (WMD) and/or their delivery vehicles.

- The jurisdiction exhibits weak controls and/or enforcement mechanisms concerning Money Laundering (ML), Terrorism Financing (TF), and Proliferation Financing (PF).

4. Country score: Low
    - The country has robust regulation and enforcement mechanisms, which are acknowledged by the FATF. Additionally, it has not been assessed in any risk category reports, and it is not included in any of the FATF lists.
    - Country has robust company registry system
    - Country has performed national risk assessment (NRA) for ML/TF/PF and has identified and implemented mitigating controls to tackle high-risk issues raised in NRAs.

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 thirty calendar days working days from the date of identifying the activity, submit a suspicious transaction report (STR) to the appropriate supervisory authority which is the Financial Crimes Enforcement Network (FinCEN)[8].

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

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

It is the duty of PayBitoPro to report immediately, in case of any suspicion / unusual activity of money laundering and terrorist financing to the appropriate regulatory authority (FinCEN), but not later than thirty calendar days from the date of identifying / recognizing such activity.

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

[8] Section 352 of Patriot Act, 2001

Changes to 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*]