

PayBitoPro

Counter Proliferation Financing (CPF) Policy

(EUROPEAN UNION)



Created by:	Avisek Banerjee
Approved by:	Soumendu Roy
Documentation Version:	2.3
Submission Date:	23rd May, 2024

TABLE OF CONTENTS

INTRODUCTION	3
POLICY SCOPE	4
DEFINITIONS	5
Proliferation Financing	5
RISK BASED APPROACH	6
COUNTER PROLIFERATION FINANCING PROGRAM	7
COUNTRIES HAVING HIGH RISKS OF PROLIFERATION FINANCING	8
• Russia and proliferation financing risks:	9
• North Korea and proliferation financing risks:	9
• Iran and proliferation financing risks:	10
• China and proliferation financing risks:	10
• Syria and proliferation financing risks:	10
• Pakistan and proliferation financing risks:	11
CONDUCTING PROLIFERATION FINANCING ASSESSMENT ON GEOGRAPHIC RISKS	11
1. Country score: Restricted	11
2. Country score: Medium-High	12
3. Country Score: Medium Low	13
4. Country score: Low	13
SUSPICIOUS TRANSACTION REPORTING	14
Changes to Policy	15
Contact	16



INTRODUCTION

The CPF policy of PayBitoPro underscores the company's dedication to combating money laundering, terrorism financing, proliferation financing, financing for weapons of mass destruction (WMDs) and related illicit activities. It outlines the measures implemented to prevent users from exploiting its services for criminal purposes, aligning with pertinent laws of the European Union such as The Anti Money Laundering Directives and other relevant regulations pertaining to the recommendations of the Financial Action Task Force (FATF). 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 the member states of the European Union and the business enterprises registered in the member states of the European Union.

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 European Union and its member states 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 the European Union. 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 European Banking Authority (EBA) and European Securities and Markets Authority (ESMA) in imbibement to the guidelines and recommendations of the Financial Action Task Force (FATF).

The Policy conforms to the regulations of the EU and its member states 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 EU and the member states of EU.

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 (ESMA and EBA) 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 AML Directives, it is mandatory for a Digital asset service provider to establish and adhere to an AML & CTF Program along with updated Counter Proliferation Financing Technique.¹ Hence PayBitoPro's AML & CTF Program has been designed, as per the relevant regulations. The AML & CTF Program along with CPF technique is applicable to all Representatives of PayBitoPro where the policies, processes and procedures are processed:

- To implement the transaction and activity reporting requirements,
- To implement customer due diligence requirements,

¹ Reg 6 of Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets



- To implement the record keeping requirements,
- To inform PayBitoPro's officers and employees of the laws of EU 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 CTF 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.

COUNTRIES HAVING HIGH RISKS OF PROLIFERATION FINANCING

PayBitoPro assesses the Proliferation Financing (PF) risks based on the geography where the risks are higher. We make sure that if the transactions are being made from any of the below-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.

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.

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). 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:

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:

Pakistan regards its nuclear capability as crucial given the nuclear arsenal and conventional force superiority of neighbor country India.



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.

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 the stipulated time as applicable according to relevant laws in the respective member state from the date of identifying the activity, submit a suspicious transaction report (STR) to the appropriate supervisory authority which is the Financial Intelligence Unit (FIU) to the regulatory authorities like European Securities and Markets Authority (ESMA) as well as the European Banking Authority (EBA).

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

After submission of the STR to the appropriate regulatory authority (ESMA and EBA), 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 (ESMA and EBA), but not later than two working days from the date of identifying / recognizing such activity.

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

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]

