Anti-Money Laundering and Countering the Financing of Terrorism Policies (AML/CTF)

Responsible Area: Legal & Compliance
Director in Charge: Ricardo Reis
Approval Date: [25/07/2025]
Internal Code: [08]
Version: 2.0

_____

This document is temporary, and may be updated at any time and at the sole discretion of FacilitaPay

Summary

DEFINITIONS

All capitalized terms in this Policy shall have the meanings listed below:

"ABR", "risk-based approach", means the methodology whereby financial institutions and other regulated entities assess and mitigate money laundering and terrorist financing risks based on the identification, assessment, and understanding of the risks to which they are exposed, applying enhanced due diligence measures proportionate to the level of risk identified;

"Affiliate" means, in relation to FacilitaPay, any Subsidiaries, Parent Companies, companies under common control and other companies that are part of its economic group;

"BCB" means the Central Bank of Brazil;

"BSA" means the Bank Secrecy Act of the United States, as codified in various sections of Title 31 of the United States Code, including but not limited to 31 U.S.C. 5330, under which FacilitaPay, as a Money Services Business (MSB), is subject to federal registration, reporting, and compliance requirements pursuant to the implementing regulations found in 31 CFR Chapter X;

"Final Beneficiaries" or "UBOs" means the natural persons who ultimately own or control a legal entity or on whose behalf a transaction is being conducted, including those persons who exercise ultimate effective control over a legal person or arrangement;

"Client" means the individuals or legal entities, as the case may be, who contract or use the products and services offered by FacilitaPay;

"Circular No. 3,978/20" means Circular No. 3,978, of January 23, 2020, issued by the BCB, as amended, which provides for the policy, procedures and internal controls to be adopted by the institutions authorized to operate by the BCB in order to prevent the use of the national financial system for the practice of money laundering and terrorist financing crimes, together with the corresponding U.S. federal regulations under 31 CFR 1022.380 which outline parallel requirements for MSBs, including registration maintenance, record-keeping obligations, and agent list requirements;

"COAF" means the Council for the Control of Financial Activities, a body created by the Ministry of Economy for the purpose of disciplining, applying administrative penalties, receiving, examining and identifying the occurrences of suspected illegal activities provided for in Law No. 9,613/98, without prejudice to the competence of other bodies and entities, and which serves functions analogous to those of FinCEN (Financial Crimes Enforcement Network) under the U.S. Department of the Treasury for anti-money laundering and counter-terrorist financing oversight;

"Subsidiaries" means the company or entity that is controlled by another person or entity, according to the definition of control provided for in article 116 of Law No. 6,404, of December 15, 1976;

"Parent Company" means the person or entity that has the power of control of a given company, as defined in article 116 of Law No. 6,404, of December 15, 1976;

"Employee" means any and all individuals or legal entities that have a position, function, position, corporate, employment, professional, contractual or trust relationship with FacilitaPay;

"FinCEN" means the Financial Crimes Enforcement Network, a bureau of the U.S. Department of the Treasury that administers the Bank Secrecy Act and requires MSB registration pursuant to 31 U.S.C. 5330 and implementing regulations under 31 CFR 1010.100(t) and (ff), which provide the regulatory definition of "money services business," and 31 CFR 1022.380(b)(2), which mandates biennial registration renewal on or before December 31st;

"UNSC" means the United Nations Security Council;

"Close Collaborator" means any natural person known to be a close associate or collaborator of a Politically Exposed Person, including business partners, advisors, or other individuals who maintain close professional, personal, or financial relationships with such PEPs;

"FacilitaPay" means Facilita Instituição de Pagamento S.A., FacilitaPay US LLC, FPay Internacional SA de CV., FPay Colombia SAS, or FacilitaPay Chile SPA, together or separately;

"Family members" means spouses, partners, children and their spouses or partners, parents, siblings, and any other relatives by blood, marriage, or adoption who maintain close personal or financial relationships with a Politically Exposed Person;

"Terrorist Financing" means the financing of terrorist acts, and of terrorists and terrorist organizations, regardless of whether a terrorist act occurs, including the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, to carry out terrorist activities;

"Money Laundering" means the process of concealing or disguising the proceeds of crime or converting such proceeds into apparently legitimate assets, encompassing any act or

attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources;

"Money Laundering Law" means Law No. 9,613, of March 3, 1998, and with respect to U.S. operations, includes compliance obligations under the Bank Secrecy Act as implemented through 31 CFR Chapter X;

"MSB" means Money Services Business, as defined under U.S. federal law in 31 CFR 1010.100(t) and (ff), requiring registration with FinCEN pursuant to 31 U.S.C. 5330 and adherence to the regulatory framework established under the Bank Secrecy Act and its implementing regulations;

"Anti-Terrorism Law" means Law No. 13,260, of March 16, 2016, (Brazil);

"OFAC" means the *Office of Foreign Assets Control*, which is an agency of the United States of the Treasury Department, responsible for the creation of the Specially Designated Nationals (SDN List), which lists the countries and persons embargoed or restricted to carry out transactions of certain products with certain countries and persons accused of practicing among others, drug trafficking, terrorism, producing, using and proliferating weapons of mass destruction;

"PEPs" or "Politically Exposed Persons" means natural persons who are or have been entrusted with prominent public functions, including heads of state or government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, and important political party officials, as well as their family members and close collaborators;

"PIX" means the instant payment arrangement instituted by the BCB and which FacilitaPay is part of;

"AML/CFT" means prevention of the practice of Money Laundering and Terrorist Financing crimes, encompassing compliance with both Brazilian regulations under the BCB and COAF oversight, and U.S. federal requirements under the Bank Secrecy Act, FinCEN regulations, and OFAC sanctions programs; and

"Policy" means this Policy for the Prevention of Money Laundering and Terrorist Financing Crimes.

OBJECTIVES

The purpose of this Policy is to establish guidelines and responsibilities that govern FacilitaPay's internal procedures, controls and systems in order to ensure that FacilitaPay's

internal ecosystem, products and services are not used or involved in illicit activities, especially those described in the Money Laundering Law and the Anti-Terrorism Law.

This Policy was prepared in accordance with the risk profiles of FacilitaPay, its Customers, operations, products and services offered and Employees, as well as in accordance with the legislation and regulations applicable to FacilitaPay, notably in accordance with Circular No. 3,978/20.

SCOPE

This Policy is applicable to all FacilitaPay Employees and Customers, as applicable.

THE CRIMES PREVENTED BY THIS POLICY

According to article 1 of the Money Laundering Law, the crime of "Money Laundering" is defined as the act of "concealing or dissimulating the nature, origin, location, disposition, movement or ownership of goods, rights or values deriving, directly or indirectly, from a criminal offense".

The money laundering process consists of three steps (not necessarily sequential):

- **Placement.** introduction of money or other assets proceeding from illegal/criminal activities into financial or non-financial institutions;

- **Occultation.** Separating the proceeds of criminal activities from their origin through the use of layers of complex financial operations. These layers are intended to hinder the audit trail, mask the origin of the funds and provide anonymity; and

- **Integration.** put the "laundered" resources back into the economy in such a way that they re-enter the financial system as resources of apparently licit origin.

FacilitaPay, as a payment institution authorized to operate by the BCB, as an issuer of electronic money, as well as as a participant in the Brazilian foreign exchange market, may be a victim of offenders in any of the steps mentioned above.

The term "Terrorist Financing" can be interpreted as the financing of terrorist acts, terrorists or terrorist organizations. The Anti-Terrorism Law stipulates a strict penalty for anyone who offers or receives, obtains, keeps, keeps in deposit, requests, invests or in any way contributes to obtaining an asset, good or financial resource, for the purpose of financing, in whole or in part, a person, group of people, association, entity, criminal organization whose main or secondary activity, even on an occasional basis, the practice of terrorist acts.

Additionally, due to the measures adopted by the UNSC involving the fight against the proliferation of weapons of mass destruction. Thus, the UNSC has compelled UN member states to cease any support to non-state actors for the development, acquisition, production, possession, transportation, transfer or use of nuclear, biological and chemical weapons and their means of delivery.

FacilitaPay, when offering its products and services, can be a victim of offenders and criminals, as well as used as an instrument to enable terrorist acts and/or the proliferation of weapons of mass destruction.

In view of the above, FacilitaPay internally establishes a series of guidelines, mechanisms, procedures and systems aimed at preventing the aforementioned crimes, which are described in the following internal documents:

- this Policy;
- Customer Identification, Qualification and Classification (KYC) Manual;
- Manual for the Identification, Qualification and Classification of Employees, Partners and Service Providers (KYE, KYP and KYS);
- Manual for Monitoring, Selection and Analysis of Operations and Suspicious AML/CFT Situations;
- AML/CFT Internal Risk Assessment Report; and
- AML/CFT Policy Effectiveness Report.

To manage the regulatory and reputational risks associated with the crimes of money laundering, terrorist financing and proliferation of weapons of mass destruction, FacilitaPay adopts a risk-based approach by implementing internal controls with the aim of preventing, detecting and reporting suspicious situations and activities involving said crimes.

ROLES AND RESPONSIBILITIES

Senior Management

FacilitaPay's Senior Management is currently represented by a Board of Directors composed of three (3) officers.

The creation, maintenance and implementation of an effective Policy in compliance with current regulations are the responsibility of Senior Management through one or more executive officers who are members of the Executive Board.

In addition, FacilitaPay's Senior Management is responsible for:

- disclose, in a timely and transparent manner, the risks related to the practice of crimes of money laundering, terrorist financing or proliferation of weapons of mass destruction;

- disseminate AML/FTP standards (including this Policy) so that Employees are aware of and comply with all the rules set forth therein;

- keep the Head of Compliance regularly updated on any changes to this AML/CFT Policy and related documents, as well as in case of identification of new risks associated with AML/CFT;

- to approve and periodically review this AML/CFT Policy and other AML/CFT documents, including the AML/CFT Internal Risk Assessment Report; and

- evaluate and approve, when applicable, the action plan and the respective follow-up report, resulting from the Effectiveness Assessment of this Policy and related documents.

FacilitaPay's Senior Management must request the opinion of FacilitaPay's internal compliance department whenever it makes adjustments to this Policy and other AML/CFT documents of FacilitaPay.

Head of Compliance

FacilitaPay's Head of Compliance must report directly to Senior Management, as well as manage and ensure that FacilitaPay's Compliance area performs its functions in accordance with this Policy and other internal rules of FacilitaPay.

FacilitaPay designates a BSA/AML Compliance Officer pursuant to 31 CFR 1022.210(b)(1). This officer maintains sufficient authority, independence, and resources to develop, implement, and maintain an effective BSA/AML compliance program. This Compliance Officer shall be known as the "Head of Compliance".

The Head of Compliance has the following duties:

- coordinate and supervise all Compliance topics, including AML/CFT, and must meet with Senior Management quarterly (or at a shorter interval when necessary) to evaluate and discuss FacilitaPay's performance from a Compliance perspective;

- assist Senior Management in the formulation of FacilitaPay's Compliance strategies and execute such strategies, including supervising their development and implementation;

- examine the annual budget proposal of the Compliance area;

- promote investigations in relation to complaints received;

- understand the legislation and regulations applicable to FacilitaPay, as well as the products and services offered by FacilitaPay to its Customers; and

- analyze other matters related to Compliance.

Commercial and Business Area

The Employees who are part of FacilitaPay's Commercial and Business area are responsible for creating and maintaining the relationship with Customers, as well as encouraging the contracting and use of products and services offered by FacilitaPay.

Employees who are part of FacilitaPay's Commercial and Business area must be diligent in relation to the risks of money laundering, terrorist financing and proliferation of weapons of mass destruction, and must report all atypical and/or suspicious situations to Compliance with a copy to FacilitaPay's AML/CFT team.

Such Employees must also, before launching new products and services to the public or making substantial changes to FacilitaPay's existing products and services, necessarily involve: (i) the internal legal department; (ii) Head of AML/CFT; and (iii) Senior Management.

It is the duty of FacilitaPay's Commercial and Business Employees to continuously evaluate the relationship and activity of the Customers under their responsibility and to inform the Registration and Compliance areas of any changes (such as changes related to registration information, financial situation, among others, of the Customer) of which they become aware.

Internal Compliance

FacilitaPay's internal Compliance area is responsible for:

a) for managing the process related to the beginning of FacilitaPay's relationships with Customers (together with the Commercial and Business team), as well as for verifying that the documentation and information provided by the Customer are in compliance with the rules established in this Policy and Customer Identification, Qualification and Classification (KYC) Manual.

Before and after starting a relationship with a Client, the member of the Registration area must:

- request information that allows the identification and qualification of the Client, as stipulated in the Customer Identification, Qualification and Classification (KYC) Manual, in order to identify, verify and validate the authenticity of the information received by the Customer (e.g., request and analyze the Client's shareholding structure and/or identity of the respective Final Beneficiaries, directors and legal representatives, when a legal entity);

- obtain all information and evidence necessary for the verification of the Customer's identity, including their family members (where applicable);

- prepare Customer KYC dossiers, as required by the Customer Identification, Qualification and Classification (KYC) Manual, as well as prepare Customer and Suspicious Transactions monitoring dossiers, as required by the Suspicious Transactions Monitoring, Selection and Analysis Manual; and

- coordinate periodic reviews of Customer registration databases.

b) for carrying out all global AML/CFT aspects and efforts, which includes:

- develop, maintain, supervise and (where applicable) test the implementation of new AML/CFT strategies, including suggestions for adjustments to this Policy and related documents, or the creation of new appropriate procedures and controls to ensure compliance with the laws and regulations applicable to FacilitaPay;

- monitor the evolution of AML/CFT legislation and best market practices;

- promote awareness programs, training, and training of Employees on the subject of AML/CFT;

- promote the AML/CFT organizational culture, including, in addition to Employees, any partners and outsourced service providers when applicable;

- report AML/CFT issues to Senior Management through FacilitaPay's internal systems;

- carry out the proper analysis of new relationships with Customers, as well as check that relationships with new Customers have been properly carried out in the registration process and that periodic reviews have been completed in accordance with internal AML/CFT documents, with emphasis on the Customer Identification, Qualification and Classification (KYC) Manual and the Monitoring Manual, Selection and Analysis of Suspicious Transactions;

- ensure that Clients go through national and international lists of persons sanctioned by the UNSC, OFAC, and other authorities required by the BCB or FacilitaPay's private partners;

- classify Clients by risk categories as defined in the procedures for classifying Clients and assessing Clients' internal risks;

- assess the risks included in FacilitaPay's Annual Internal Risk Assessment Report; and

- correct any deficiencies identified in the AML/CFT Policy Effectiveness Report.

c) responsible for verifying compliance with this Policy, AML/CFT procedures, as well as internal controls related to AML/CFT, through the AML/CFT Policy Effectiveness Report.

In addition, this department must identify any deficiencies in the internal AML/CFT processes and routines.

Internal Audit

FacilitaPay's internal audit department must monitor the implementation of any action plan, resulting from the AML/CFT Policy Effectiveness Report, as well as monitor compliance with said action plan.

All Employees

FacilitaPay's Employees must conduct their duties in compliance with the applicable legislation and FacilitaPay's internal rules, including this Policy. In addition to the specific obligations and responsibilities defined above, all FacilitaPay Employees must ensure faithful compliance with this Policy and related documents, as well as immediately report to the Compliance team any suspicious situation of the practice of money laundering, terrorist financing and/or proliferation of weapons of mass destruction.

RISK-BASED APPROACH (ABR)

FacilitaPay, as a payment institution issuing electronic money and participating in the Brazilian foreign exchange market, is part of the Brazilian Payment System (SPB) and the Brazilian foreign exchange market, both environments being regulated by the BCB, Bandeiras and other private entities that are partners of FacilitaPay.

In view of the regulatory risks inherent to FacilitaPay's business, as well as due to the reputational risks involving the practice of money laundering, terrorist financing and proliferation of weapons of mass destruction, FacilitaPay has adopted a risk-based approach ("ABR") as the main governance tool for AML/CFT purposes.

The Compliance area is responsible for the analysis, elaboration and implementation of the ABR process at FacilitaPay, which was mapped and prepared aiming at the effective management of the process of identification, monitoring, analysis and mitigation of risks of the practice of money laundering, terrorist financing and proliferation of weapons of mass destruction.

To execute this approach internally, FacilitaPay classifies its Customers, based on their risk profiles and the nature of the relationship, into the following risk categories: (i) "low risk"; (ii) "medium risk"; or (iii) "high risk" which are duly described in the Customer Identification, Qualification and Classification (KYC) Manual.

Such risk ratings must be reassessed by FacilitaPay: (i) annually; or (ii) whenever there are changes in the risk profile and/or nature of the business between Client and FacilitaPay. When reassessing the Client's risk rating, the Compliance team must reassess all the information and variables available in the Client's background check (e.g., KYC and Client Monitoring Dossiers), according to the Client's current risk and procedures described in the Client Identification, Qualification and Classification (KYC) Manual.

The ABR analysis should consider, at a minimum:

- FacilitaPay's ability to combat the practice of money laundering, terrorist financing and proliferation of weapons of mass destruction, with the appropriate level of continuous monitoring to be applied in view of the risk of the Client and/or Employee;

- level of risk of money laundering, terrorist financing and/or proliferation of weapons of mass destruction, which the Client presents to FacilitaPay;

- nature of the Client and/or Employee, such as government entities, non-regulated funds, *trusts*, foundations, among others;

- function of the commercial activity, such as the evaluation of activities most susceptible to illegal exploitation (Casinos, Bookmakers and other Activities Related to Gambling, religious and charitable entities, gas stations, among others), and the creation of a list of "Prohibited Activities";
- risk to FacilitaPay's reputation;
- risk by product, service or activity, in addition to foreign exchange operations;
- risk linked to operations carried out within the scope of PIX, especially at night;
- financial impacts;
- impacts related to Environmental, Social and Governance (ESG);
- AML-relevant media;
- PEP - Politically Exposed Persons;
- accounts opened by proxy;
- geographical factors, such as border cities or those located in countries at higher risk;
- number of alerts in monitoring;
- dual citizenship / Foreigner;
- time of the last registration review;
- Judicial blockade/Breach of bank secrecy;
- communications made to COAF;
- incomplete registration information; and
- identification of vulnerable audiences.

INTERNAL RISK ASSESSMENT

FacilitaPay's ABR is evaluated by an internal process called Internal Risk Assessment, which is formalized and reviewed annually, through the AML/CFT Internal

Risk Assessment Report, which contains the parameters and guidelines that underlie FacilitaPay's ABR.

The AML/CFT Internal Risk Assessment Report must be: (i) prepared and approved by the Director of Senior Management responsible for AML/CFT by the last business day of March of the year following the base date of the last report; (ii) previously examined by the Head of Compliance, who must formalize his technical and non-binding opinions to the Officer responsible for AML/CFT before approving said report; and (iii) reviewed every two years, in which case items "i" and "ii" should occur again.

The implementation and management of the AML/CFT Internal Risk Assessment Report is under the responsibility of Compliance.

EFFECTIVENESS EVALUATION

FacilitaPay's Compliance, Internal Controls, Risk Management and Internal Audit areas must evaluate, in accordance with current regulations, the effectiveness of the internal risk assessment, as well as this Policy and related documents. Such evaluation must occur every two years through a specific methodology, adopted for the verification of all AML/CFT documents and procedures, and must be formalized in the AML/CFT Policy Effectiveness Report, until the last business day of March of the year in which the review of the report must be carried out.

As a general rule, the Effectiveness Test must contain, among other determinations, information that describes: (i) the methodology adopted in the evaluation of effectiveness; (ii) the tests applied; (iii) the qualification of the evaluators; and (iv) the deficiencies identified.

In addition, it must contain, at least, the evaluation: (i) of the procedures aimed at getting to know Customers, including the processes of verification and validation of Customer information and the adequacy of registration data; (ii) the monitoring, selection, analysis and communication procedures to the COAF, including the evaluation of the effectiveness of the parameters for selecting operations and suspicious situations; (iii) the governance of this Policy; (iv) measures to develop organizational culture aimed at AML/CFT; (v) periodic training programs for personnel; (vi) the procedures aimed at getting to know the Employees; and (vii) the actions to regularize the notes arising from the internal audit and supervision of the BCB, when applicable.

After the preparation of the AML/CFT Policy Effectiveness Report, Senior Management together with the Head of Compliance must prepare, when necessary, an action plan with the objective of solving any deficiencies identified through the effectiveness assessment. The monitoring of the implementation of the action plan must

be documented by means of a follow-up report, which is the responsibility of the Internal Audit team.

EVALUATION OF NEW PRODUCTS, SERVICES AND/OR TECHNOLOGIES

In line with current regulations and best market practices, the Head of Compliance must always be involved in the discussion and prior approval of new products and services, as well as in the possible use of new technologies, so that he or she can assess and analyze in advance possible risks of money laundering, terrorist financing and proliferation of weapons of mass destruction.

Likewise, the Head of Compliance must be involved in advance in discussions regarding any substantial change in existing products and services, and must even approve such changes before the adjustments are released to the public.

GUIDELINES: KNOW-YOUR-CUSTOMERS (KYC) PROCEDURES

Among the rules, procedures and internal controls adopted by FacilitaPay aimed at AML/CFT practices, the process of identification, qualification and classification of Customers constitutes one of the main pillars of AML/CFT risk management and prevention adopted by the institution, being the process that enables FacilitaPay to identify, prior to the beginning of the commercial relationship with its Customers, the risks of the Client's involvement with irregular practices and/or that may constitute evidence of the practice of crimes of money laundering, terrorist financing and/or proliferation of weapons of mass destruction. Through this process, the institution is able to mitigate any AML/CFT risks.

In order to perform the procedures for identifying, qualifying and classifying Customers satisfactorily and in accordance with the standards of this Policy, at least the following steps must be carried out: (i) registration and receipt of information and documents; (ii) validation and analysis of information and documents received and additional, when applicable; and (iii) classification of the Clients' risk profile; including its Final Beneficiaries, administrators and/or legal representatives, in the case of legal entities and any attorneys-in-fact, in the case of individuals.

The rules and procedures set forth in this Policy and in the Customer Identification, Qualification and Classification (KYC) Manual shall be applicable to all FacilitaPay Customers and all requirements set forth therein shall be followed by the applicable Employees during the term of FacilitaPay's relationship with its Customers.

FacilitaPay shall, within the limits of its duties, identify, analyze and mitigate the AML/CFT risks inherent to its activities and its Customer base, in view of the risk approach strategies defined internally.

Based on this approach, FacilitaPay must determine the depth and amount of information and documents that will be requested from Customers, as well as the criteria used to validate the information and documents received, as indicated in the Customer Identification, Qualification and Classification (KYC) Manual.

After receiving the relevant documentation, and performing the necessary validations, the Client must be classified according to its applicable risk category, according to the parameters established in the Customer Identification, Qualification and Classification (KYC) Manual.

In the event that a Client does not clearly fit into any of the risk categories used by FacilitaPay, as well as in the case of conflicts and exceptions involving the classification of Clients, the information and documents of this Client must be forwarded to the Head of Compliance, who has the necessary authority to provide the appropriate guidelines for the classification of said Client.

Customer Registration and Identification

FacilitaPay must maintain an updated register of its Customers, which must contain, at least, the information and documents described in the Customer Identification, Qualification and Classification (KYC) Manual.

The registration of Customers will be carried out by filling out a form to be sent by FacilitaPay's Commercial team if the prospected Customer or who presents himself before FacilitaPay has initial compatibility with the flows of products and services made available by FacilitaPay, with solutions that can be identified in accordance with the applicable legislation and regulations.

Once the Client has made the relevant information and documents available for registration purposes, the Compliance area will carry out the necessary procedures to identify it, including its Final Beneficiaries, administrators and/or legal representatives, as applicable.

The Customer Identification, Qualification and Classification (KYC) Manual establishes the minimum requirements for the registration and identification of Customers who wish to contract the products and services offered by FacilitaPay, such as the provision of payment services, international transfers, opening of prepaid payment accounts, issuance of payment instruments, as well as services associated with the closing of exchange transactions.

Thus, the parameters and requirements used by FacilitaPay for the registration and identification of Customers include information and documents that attest to and enable the verification of the Customer's identity and the analysis of the Customer's corporate

structure, including its administrators, partners, Final Beneficiaries, controllers and any subsidiaries.

The Client's identification process must be able to support and enable FacilitaPay's understanding of the Client's risk profile, activities performed, and economic and financial capacity (as the case may be), so that the other KYC steps (qualification and classification) are properly completed.

If FacilitaPay identifies that potential Customers perform the activities and/or work in the sectors indicated in Annex I of this Policy, FacilitaPay will immediately reject them.

Once the relevant information and documents have been made available by the Client, FacilitaPay's Compliance area will validate the authenticity of the documents and information collected using public and private databases, previously approved by the Head of Compliance, and as indicated in the Customer Identification, Qualification and Classification (KYC) Manual.

Customer Validation and Qualification

After completing the Customer identification process, the Compliance area will start the Customer qualification process. At this stage, FacilitaPay shall, through independent research in reliable public and private sources, at least:

- identify and validate the place of residence provided by the Client in the identification process, in the case of an individual Client;
- identify and validate the location of the headquarters or branch made available by the Client in the identification process, in the case of a legal entity Client;
- evaluate and validate the Client's financial capacity, including income, in the case of an individual, or billing, in the case of a legal entity;
- verify that the Client, including its Final Beneficiaries, administrators and/or legal representatives, Family Members and Close Collaborators (including in the role of representative) qualify as PEPs;
- verify and validate the information and documents made available by the Client involving its Final Beneficiaries; and
- any additional information from the Client compatible with the risk of using FacilitaPay's products and services in the practice of money laundering, terrorist financing and/or proliferation of weapons of mass destruction.

For the purposes of this Policy, politically exposed persons ("PEPs") are considered to be:

- holders of elective mandates of the Executive and Legislative Branches of the Union;

- the occupants of a position, in the Executive Branch of the Union, of: (a) Minister of State or equivalent; (b) Special or equivalent nature; (c) president, vice-president and director, or equivalent, of indirect public administration entities; and (d) Superior Management and Advisory Group (DAS), level 6, or equivalent;

- the members of the National Council of Justice, the Federal Supreme Court, the Superior Courts, the Federal Regional Courts, the Regional Labor Courts, the Regional Electoral Courts, the Superior Council of Labor Justice and the Federal Justice Council;

- the members of the National Council of the Public Prosecutor's Office, the Attorney General of the Republic, the Deputy Attorney General of the Republic, the Attorney General of Labor, the Attorney General of Military Justice, the Deputy Attorneys General of the Republic and the Attorneys General of the States and the Federal District;

- the members of the Federal Court of Accounts, the Attorney General and the Deputy Attorneys General of the Public Prosecutor's Office at the Federal Court of Accounts;

- the presidents and national treasurers, or equivalent, of political parties;

- the Governors and the Secretaries of State and of the Federal District, the State and District Deputies, the presidents, or equivalents, of state and district indirect public administration entities and the presidents of Courts of Justice, Military Courts, Courts of Accounts or equivalent of the States and the Federal District;

- the Mayors, Councilors, Municipal Secretaries, the presidents, or equivalent, of entities of the indirect municipal public administration and the Presidents of Courts of Auditors or equivalents of the Municipalities;

- persons who, abroad, are: (a) heads of state or government; (b) politicians of higher echelons; (c) occupants of government positions of higher echelons; (d) general officers and members of higher echelons of the Judiciary; (e) senior executives of public companies; or (f) leaders of political parties; and

- the heads of senior echelons of public or private international law entities.

Also, during the verification of qualification as a PEP, FacilitaPay must consider the following definitions:

- "Family members" such as: relatives, in the direct or collateral line, up to the second degree, the spouse, the partner, the stepson and the stepdaughter; and

- "Close Collaborator" as: (a) an individual known to have any type of close relationship with PEP, including for: (1) having a joint interest in a legal entity governed by private law; (2) appear as an agent, even if by private instrument of the person mentioned in item 1; or (3) have joint interest in unincorporated arrangements; and (b) an individual who has control of legal entities or arrangements without legal personality, known to have been created for the benefit of PEP.

For the purposes of this Policy, the following shall be considered as Final Beneficiaries:

- individuals who hold, directly or indirectly, 25% or more of equity interest in the Client; or

- individuals who exercise, in fact, direct or indirect command over the activities of the Client on behalf of which a transaction is being conducted or benefits from it, including their respective agents, attorneys-in-fact or representatives.

The information collected during the Client's qualification process must be kept updated and reassessed, at least, annually or in a shorter period, depending on the Client's risk profile.

In addition, the process of qualifying Customers (including their requalifications) must be carried out in a manner proportional to the risk of Customers using FacilitaPay to commit the crimes of money laundering, terrorist financing and/or proliferation of weapons of mass destruction.

In order to comply with the obligations described above, without prejudice to the fulfillment of the Customer identification process, the registration data of legal entity Customers must include information about the individuals authorized to represent them, as well as all their direct and indirect controllers, and individuals who have significant influence over them, until reaching the individual characterized as Final Beneficiary, in addition to the indication of whether one or more of these (including their Family Members and Close Collaborators) qualify as PEPs.

The Customer qualification procedure must have been completed by FacilitaPay before starting the relationship with new Customers. Exceptionally, FacilitaPay may initiate a relationship with its Client for a maximum period of 30 days without the Client's qualification process having been completed, provided that there is no prejudice to the procedures for monitoring and selection of Clients and suspicious transactions. Notwithstanding, no service contract may be entered into with Customers who do not pass the properly processed customer qualification procedure.

Classification of Customer Risk Profiles

Once the Customer identification and qualification processes have been completed, the Compliance area must carry out the procedures for classifying the Customer's risk profile, in order to verify the degree of risk of the Customer's practice of money laundering, terrorist financing and/or proliferation of weapons of mass destruction.

The compliance area will be responsible for defining appropriate procedures for accepting Clients, as well as for properly classifying Clients in the risk category applicable to their profile, which will be segmented into "low risk", "medium risk" or "high risk", as indicated in the Customer Identification, Qualification and Classification (KYC) Manual.

In the case of Customers classified as "high risk", FacilitaPay shall make additional efforts to identify the origin of the funds involved in its operations, as well as shall more rigorously monitor the evolution of the relationship and the services provided and products offered to such Customers, through the application of procedures related to differentiated risk assessment.

The elements used by FacilitaPay to determine the Client's risk profile consider information such as: type of Client, qualification as PEP, the nature and activity of the Client, the operations and distribution channels used by the Client, the products offered and/or services provided to the Client and the counterparty of the operations carried out by the Client, if applicable.

In the event of a change in the activities provided by the Client and in the other elements indicated above during the term of the relationship with the institution, FacilitaPay will carry out a new assessment of the Client's risk profile to potentially verify the need to adjust the risk of this Client's profile.

FacilitaPay will assign the Client's classification as "high risk" if the Client is qualified or relates to people qualified as PEP, including their Family Members and Close Collaborators, the Client, its Final Beneficiary[1] or corporate associates have a negative

[1] in accordance with 31 CFR 1010.230 and Circular 3.978/20, FacilitaPay shall verify the identity of each beneficial owner identified pursuant to the beneficial ownership requirements using the same customer

impact on the media (of a criminal nature). All criteria that give rise to the classification of Customers as "high risk" are regulated in the Customer Identification, Qualification and Classification (KYC) Manual.

Additionally, FacilitaPay Employees must observe the list of prohibited relationships provided for in the Customer Identification, Qualification and Classification (KYC) Manual.

GUIDELINES: KNOW YOUR EMPLOYEES, PARTNERS, AND CONTRACTORS (KYE, KYP, AND KYS)

Know Your Employee (KYE)

All FacilitaPay employees, at the time of their hiring, including finalist candidates in the selection processes, undergo a compliance assessment carried out by FacilitaPay's Human Resources area, in view of the identification of facts that discredit the candidate and, consequently, bring risk to the institution's reputation or, even, risks of the practice of money laundering crimes, financing of terrorism and/or proliferation of weapons of mass destruction.

When starting their relationship with FacilitaPay, Employees are duly trained for AML/CFT purposes and must mandatorily undergo training and/or adhere to this Policy.

FacilitaPay monitors the external activities of Employees, in order to avoid possible conflicts of interest, as well as to monitor the behavior of Employees.

All FacilitaPay employees must be classified in a risk category according to their internal attributions, which must be kept up to date.

The Employee, Partner, and Provider Identification, Qualification, and Classification Manual (KYE, KYP, and KYS) details all internal employee identification and qualification processes.

Know your Partner and Service Providers (KYP and KYS)

identification procedures applicable to opening accounts for individual customers. This verification shall occur within a reasonable period after account opening. For beneficial owners who **own twenty-five percent** or more of the legal entity, FacilitaPay shall obtain and verify identifying information including name, address, date of birth, and taxpayer identification number. For the control person identified under the beneficial ownership requirements, FacilitaPay shall obtain the same identifying information and verify the individual's identity. FacilitaPay may rely on the legal entity customer to provide beneficial ownership information but shall maintain procedures to verify the accuracy of the information provided and to update beneficial ownership information when FacilitaPay becomes aware of changes in the beneficial ownership structure of the legal entity customer.

All FacilitaPay's partners and outsourced service providers, before having any relationship with the institution, must undergo prior analysis by the Compliance area, including through research in reliable public and private data collections.

The surveys are intended to ensure that, before accepting the third party as a partner or service provider, FacilitaPay identifies and analyzes the negative information available about it and its controllers.

The relationship with the partner and/or service provider should not proceed until the verification of the surveys has been completed.

All FacilitaPay's partners and third-party service providers must be classified in a risk category according to their internal attributions, which must be kept up to date.

The Employee, Partner, and Contractor Identification, Qualification, and Classification Manual (KYE, KYP, and KYS) details all internal processes for identifying and qualifying partners and third-party contractors.

GUIDELINES: MONITORING, SELECTION, AND ANALYSIS OF OPERATIONS

In order to comply with the requirements of current legislation and regulations aimed at combating financial crimes, the transactions made by all Customers holding prepaid payment accounts are monitored in order to identify payment transactions that may constitute evidence of the practices of money laundering, terrorist financing and/or proliferation of weapons of mass destruction.

Suspicious transactions are those that present, for example, the following characteristics:

- demonstrate any evidence of the Client's involvement in money laundering crime;
- have no economic or legal basis;
- are not habitually carried out by the Customer and do not present any reasonable reason for the sudden change of pattern; and/or
- raise any suspicion that FacilitaPay is dealing with funds from criminal activities.

All situations considered suspicious by FacilitaPay are duly described in the Manual for Monitoring, Selection and Analysis of Suspicious Transactions.

Communication of Operations to COAF

FacilitaPay must report to COAF, Brazil's financial intelligence unit, the operations or situations suspected of money laundering and terrorist financing crimes of Customers, Customers in prospecting or operations carried out by non-third parties not classified as Customers.

The decision to communicate the operation or situation to COAF must be based on the information contained in the file of the Client, Prospecting Client or non-client third party, as well as be recorded in detail in the respective dossier.

Communications must be made to COAF by the business day following the communication decision.

The Manual for Monitoring, Selection and Analysis of Suspicious Operations establishes a series of objective and subjective situations that must be reported to COAF.

In cases of any doubts involving the communication of operations to COAF, the respective Employee must immediately contact FacilitaPay's Compliance area.

Suspicious Activity Reporting to FinCEN

FacilitaPay shall file Suspicious Activity Reports (SARs) with the Financial Crimes Enforcement Network (FinCEN) in accordance with 31 CFR 1022.320 for any transaction conducted or attempted by, at, or through FacilitaPay that involves or aggregates funds or other assets of at least two thousand dollars ($2,000), if FacilitaPay knows, suspects, or has reason to suspect that the transaction meets any of the following criteria:

- the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation. This includes transactions that appear to be structured to avoid currency transaction reporting requirements or other BSA reporting obligations.

- the transaction is designed to evade regulations promulgated under the Bank Secrecy Act, whether through structuring, the use of multiple accounts, or other means designed to circumvent regulatory oversight and detection.

- the transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and FacilitaPay knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

- the transaction involves the use of FacilitaPay to facilitate criminal activity, regardless of whether the specific criminal activity is known, and includes transactions that may involve money laundering, terrorist financing, fraud, or other illicit financial activities.

All SARs must be filed electronically through FinCEN's BSA E-Filing System within thirty (30) calendar days of the initial detection of the reportable activity. If no suspect is identified at the time of initial detection, FacilitaPay may delay filing for an additional thirty (30) calendar days to identify a suspect, but in no case shall the filing be delayed beyond sixty (60) calendar days from initial detection.

The BSA/AML Compliance Officer or designated senior compliance personnel shall review and approve all SARs before filing. Each SAR shall include a detailed narrative describing the suspicious activity, the basis for suspicion, and all relevant facts and circumstances surrounding the transaction or pattern of transactions.

FacilitaPay shall maintain complete records of all filed SARs, including supporting documentation, investigative materials, and decision rationale. These records shall be maintained separately from customer files and shall be accessible only to authorized compliance personnel and senior management with a legitimate business need to know.

FacilitaPay and its employees are prohibited from disclosing the fact that a SAR has been filed or that a transaction has been reported as suspicious to any person involved in the transaction or to any other person except as authorized by FinCEN or other appropriate law enforcement or regulatory authorities.

No employee may inform a customer, account holder, or any third party that their transactions are being monitored for suspicious activity or that a SAR has been filed concerning their activity. Disclosure of SAR information may only be made pursuant to a court order or as specifically authorized by FinCEN regulation.

Recording and Retention of Operations and Transactions

FacilitaPay must keep records of all operations carried out, products and services contracted, including withdrawals, deposits, contributions, payments, receipts, transfers of funds and operations in the foreign exchange market, according to the criteria and parameters established in the Manual for Monitoring, Selection and Analysis of Suspicious Transactions.

All records required under BSA regulations may be maintained in their original form or in any format that accurately reproduces the original record and ensures its integrity and accessibility. Electronic storage systems shall include appropriate backup procedures and access controls to prevent unauthorized modification or destruction of records.

FacilitaPay shall maintain indexes or other systems to enable prompt location and retrieval of required records upon request by regulatory or law enforcement authorities. These systems shall be regularly tested to ensure their effectiveness and reliability.

When records are maintained by third-party service providers or in off-site storage facilities, FacilitaPay shall maintain appropriate contractual arrangements to ensure that records remain accessible within timeframes required for regulatory compliance and law enforcement purposes.

Additionally, FacilitaPay must retain the following internal records:

For a period of 10 years:

- the information collected in the procedures for getting to know the Customers (KYC), **counted from the first day of the year following the end of the relationship with the Customer**;

- the information collected in the procedures aimed at getting to know employees, partners and third-party service providers (KYE, KYP and KYS), **counting from the date of termination of the contractual relationship**;

- the information and records of all operations carried out, products and services contracted, including withdrawals, deposits, contributions, payments, receipts and transfers of funds; and

- the dossier related to the analysis of the operations and situations selected through the procedures established in the Manual for Monitoring, Selection and Analysis of Suspicious Operations.

For a period of 5 years:

- partnership agreements entered into between FacilitaPay and institutions not authorized to operate by the Central Bank of Brazil, or that participate in a payment arrangement, evidencing that FacilitaPay has the right to access the documents and information necessary to identify the final recipients of funds from the partner institution, as provided for in article 31 of Circular No. 3,978/20;

- previous versions of the AML/CFT Internal Risk Assessment Report;

- the Customer Identification, Qualification and Classification (KYC) Manual, including its previous versions;

- the Manual for the Identification, Qualification and Classification of Employees, Partners and Service Providers (KYE, KYP and KYS), including its previous versions;

- the Manual for Monitoring, Selection and Analysis of Suspicious Transactions, including its previous versions;

- the AML/CFT Policy Effectiveness Report;

- the data, records and information related to FacilitaPay's monitoring and internal control mechanisms that ensure the implementation of the processes provided for in this Policy and related documents; and

- the documents relating to the action plans taken to address identified AML/CFT deficiencies, including their follow-up reports.

All documents and information stored by FacilitaPay may be submitted to the BCB, if it requests them during the respective retention periods.

AML/CFT TRAINING AND ORGANIZATIONAL CULTURE

FacilitaPay Employees, regardless of their functions and area of expertise, receive practical and theoretical training aimed at maximizing their professional development.

The formal training program covers face-to-face training practices, online training and courses. Such training is provided and required depending on the position and function of the Employee, always aiming to qualify him according to his activity and degree of seniority.

All employees are required to undergo Compliance training, including annual AML/CFT training. Such training is mandatory regardless of the employee's area of activity and their degree of seniority.

In addition, there is targeted training, customized according to the activity performed by each business area, so that the employee has practical examples and can correlate AML/CFT practices with their daily life at the institution.

When appropriate, we invite law firms or experts from regulatory bodies to speak in the most sensitive business areas.

**** **** ****

MERCHANT CHANGE MONITORING AND RECORD POLICIES

FacilitaPay has established comprehensive internal procedures and standards to systematically monitor, document, and maintain current records of all material business characteristics and transactional attributes of its merchant clients. These procedures ensure compliance with applicable regulatory requirements and align with industry best practices under the Payment Facilitator (Payfac) model in the United States, providing a robust framework for merchant oversight and risk management.

The company maintains a centralized and continuously updated Merchant Profile Database that serves as the primary repository for structured merchant records. This database captures essential data points including projected annual transaction volumes, merchant URLs and primary transaction domains, detailed descriptions of business models and goods or services offered, assigned Merchant Category Codes (MCC) with complete change histories, and comprehensive records of checkout payment options available to end-users such as cards, digital wallets, and alternative payment methods.

FacilitaPay's current Know Your Business (KYB) protocols are sufficient to verify ongoing merchant relationships and ensure comprehensive due diligence throughout the client lifecycle. Manual review processes remain an integral component of the verification framework, with dedicated staff conducting thorough assessments to ensure client and merchant validity, business legitimacy, and compliance with established risk parameters.

All material changes to merchant profiles, including MCC reclassifications, newly introduced payment channels, business model modifications, or significant alterations to transaction volumes, are recorded promptly within the repository system. These changes may be identified through various channels including direct merchant communications, periodic risk reviews, automated monitoring tools, or routine compliance assessments, ensuring comprehensive capture of evolving merchant characteristics.

The Merchant Profile Database operates within a secure environment featuring comprehensive audit trail functionalities and maintains strict access controls while ensuring appropriate data availability. Relevant merchant information is made accessible upon request to qualified third parties including acquiring banks, payment scheme partners, and regulatory bodies to support continued compliance with market conduct standards, consumer protection requirements, accurate regulatory reporting, and financial crime prevention measures.

Once FacilitaPay's operations are fully established in the United States, the company shall modernize its merchant monitoring program within a reasonable timeframe to incorporate third-party solutions for real-time merchant URL and activity monitoring. This enhancement will complement existing manual review processes and automated

systems, providing advanced capabilities for continuous merchant oversight while maintaining the integrity of current KYB protocols and validation procedures.

Organizational responsibility for the Merchant Profile Database rests with the Compliance & Risk Oversight team, which ensures the integrity, accuracy, and timeliness of all database entries, while all merchant-facing departments bear responsibility for identifying and flagging relevant changes requiring record updates.

ANNEX I

Prohibited Activities and Sectors

As part of our commitment to ensure compliance with our regulatory obligations and taking into account the risks involved in our services, FacilitaPay has decided to place limitations and restrictions on specific business activities and sectors in which it and/or its Customers may operate. Any requests from Customers involved in the industries or activities listed below will be automatically rejected. FacilitaPay cannot engage in commercial relationships with Clients who fall into the following situations:

- Adoption agencies;
- Alcohol, tobacco, nicotine or related products;
- Asbestos;
- Biological material of human origin (i.e.: hormones, human hair, etc.);
- Products or services for augmentation of body parts;
- Cash, paper money or any other bearer securities;
- Controlled substances and/or other products that pose a risk to consumer safety;
- Corrosive and explosive materials, compressed gases and aerosols, flammable liquids, oxidizing materials, flammable solids;
- Debt collection;
- Drugs or any type of illegal substance, including products that simulate the effects of any illegal drug; as well as any substances for the manufacture of drugs and any equipment used to produce, compound, convert, process, prepare, conceal, and consume illicit drugs;
- Live animals;
- Medical practices;
- Military weapons and ammunition, simulacra and controlled equipment (archery, sporting weapons, hunting equipment, replica weapons, etc.);
- Multi-level marketing companies, pyramid schemes, Ponzi schemes or any other program that promises profit or *cashback* with any term;
- Pawn shop;
- Poisons: liquid, solid or gaseous;
- Political parties (i.e.: campaign financing, donations and subscriptions to politicians, political causes);
- Precious metals, jewelry or any other product manufactured from these materials - Purchase or exchange;
- Products prohibited by the local Public Health Agency, Health Authority or equivalent (i.e., Anvisa, Cofepris, ISPCH, etc.);

• Products related to pedophilia, child pornography, nudity of minors, as well as articles that involve in any way the illegal participation of minors;
• Products that infringe trademarks, patents, copyrights, and other intellectual property rights (i.e.: counterfeit products);
• Prostitution agencies;
• Radioactive material;
• Religious institutions (donations or charities);
• Schedule appointments for public services;
• State-owned companies;
• Products that are stolen, stolen in any way, smuggled, counterfeit, adulterated or replicated;
• Any other product, service, or activity in jurisdictions where it is considered illegal.

ANNEX II

Sanctioned Persons Lists

1. Financial Action Task Force (FATF) list: https://www.fatf-gafi.org/publications/high-risk-and-other-monitoredjurisdictions/?hf=10&b=0&s=desc(fatf_releasedate).

2. United States Security Council (CSNU): https://www.un.org/securitycouncil/content/un-sc-consolidated-list.

3. Complete International Lists (Shufti Pro AML Dataset December 2023.pdf)

4. INTERPOL: https://www.interpol.int/How-we-work/Notices/View-Red-Notices.

5. UK Financial Conduct Authority (FCA): https://register.fca.org.uk/s/.

6. Committee against Money Laundering, Illicit Resources and the Financing of Terrorism (MONEYVAL): https://ec.europa.eu/transparencyregister/public/consultation/search.do?locale=pt&reset=.

7. U.S. Office of Foreign Assets Control (OFAC): https://sanctionssearch.ofac.treas.gov/.

8. Law enforcement and regulatory agencies of each local jurisdiction, from the slave labor lists: https://siscoaf.coaf.gov.br/siscoaf-internet/pages/cadastroPO/tipoPO.jsf.

9. Expulsions from the federal administration (CEAF): http://www.portaltransparencia.gov.br/download-de-dados/ceaf.

10. Disreputable and suspicious companies (CEIS): http://www.portaltransparencia.gov.br/sancoes/ceis?ordenarPor=nome&direcao=asc.

11. Impeded for-profit entities (CEPIM): http://www.portaltransparencia.gov.br/sancoes/cepim?ordenarPor=nome&direcao=asc.

12. CNEP: http://www.portaltransparencia.gov.br/sancoes/cnep.

13. Federal Revenue Service rule containing countries, jurisdictions, dependencies or places with favorable taxation and subject to privileged tax regimes: http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=16002.

ANNEX III

RESTRICTED MONITORING JURISDICTIONS

The following is a comprehensive table showing FacilitaPay's compliance with FATF standards while staying up-to-date with current lists of sanctioned jurisdictions. Last updated February 2024. The next page will detail the contents of the table.

Name of the jurisdiction	State*	Lower risk	Medium risk	High Risk
Albania				X
Barbados			X	
Bulgaria			X	
Burkina Faso				X
Cameroon			X	
Cayman Islands			X	
Croatia		X		
Democratic People's Republic of Korea	Banned			
Democratic Republic of the Congo			X	
Gibraltar		X		
Haiti		X		
Iran	Banned			
Islamic Emirate of Afghanistan	Banned			
Jamaica			X	
Jordan			X	
Kenya			X	
Mali		X		
Mozambique			X	
Myanmar	Banned			
Namibia		X		
Nigeria		X		
Panama		X		
Philippines		X	X	
Russia				X

Senegal				X
South Africa			X	
South Sudan				X
Syria				X
Tanzania			X	
Turkey			X	
Uganda				X
United Arab Emirates			X	
Vietnam		X		
Yemen			X	

The columns in the table refer to:

State:

The verdicts of immediate disapproval to any potential customer or supplier based on the jurisdictions in question, marked as "Banned", as seen above.

Lower Risk:

1. Countries that have submitted a written high-level political commitment to address have identified high deficiencies and that have developed an action plan with the FATF, or -

2. Countries that have submitted a high-level written commitment to address identified policy deficiencies and that have developed an action plan with the FATF.

Medium risk:

Countries/territories with strategic weaknesses in their measures to combat ML/TF, but already subject to close monitoring by the FATF (having made, at the highest level, the commitment to adopt an action plan developed jointly with the FATF.

High Risk:

High-risk countries that currently have persistent and substantial money laundering and terrorist financing problems, having repeatedly violated the obligation to remedy the deficiencies identified under the FATF.

FacilitaPay may choose to conduct business with entities located in the jurisdictions presented above, provided that the appropriate level of due diligence is applied, directly proportional to the risk presented. However, it should be noted that FacilitaPay does not

encourage sales of its services to be directed to customers based in such jurisdictions. The entity in question must be able to provide a commitment plan to adhere to international compliance requirements, as part of the enhanced due diligence process. Prohibited jurisdictions will not be considered, and commercial discussions within them are expressly prohibited.

Sources:

https://facilitapay.com/compliance/

https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-february-2024.html

https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-february-2024.html