AML AND ANTI-TERRORISM FINANCING POLICIES

1. INTRODUCTION AND OBJECTIVES

This Policy is an extension of the FACILITAPAY Code of Conduct. Its objective is to establish the expected conduct of employees in preventing and combating money laundering and terrorist financing. FACILITAPAY has zero tolerance for money laundering and is committed to mitigating money laundering risks. FACILITAPAY will take the necessary preventive measures and promptly investigate any suspicion of money laundering.

The Policy for the Prevention and Fight against Money Laundering and the Financing of Terrorism is periodically reviewed in order to achieve best practices for FACILITAPAY. The review is carried out through:

- Periodic review of media reports relevant to the sector or jurisdiction in which FACILITAPAY is active;
- Periodic review of law enforcement alerts and reports;
- Pay attention to changes in terrorist alerts and sanctions regimes as soon as they occur;
- Review of thematic and similar publications published by the competent authorities;
- Review of national and international guidelines to define standards, policies and procedures. In the event that there is no guidance, the Compliance Committee will seek it through legal advice (internal or external) and will follow the formal opinions offered.

1.1 FACILITAPAY OVERVIEW

FACILITA INSTITUIÇÃO DE PAGAMENTO S/A (FACILITAPAY) is a digital financial services facilitation company established in Brazil. The company**,** together with all its subsidiaries, offers international payment facilitation products and services, as a non-financial institution, in Brazil.

As Brazil is a full member of the UN, FACILITAPAY adheres to the sanctions regulations imposed by the United Nations. These regulations consist of sanctions implemented in accordance with United Nations Security Council Resolutions (UNSCR). In addition, FACILITAPAY must adhere to the regulations imposed by national laws to prevent money laundering and the financing of terrorism (Laws No. 9,613/98; No. 12,683/12; No. 13,260/16 and No. 13,810/19). FACILITAPAY will not do business with entities included in the sanctions lists.

In addition, in Brazil, FACILITAPAY is an entity subject to the control mechanism provided for in Article 9 of Law 9,613/98, which provides for money laundering crimes. Therefore, it is the obligation of FACILITAPAY to communicate to the Financial Activities Control Council - COAF the financial operations referred to in Chapter VII of the aforementioned Law.

2. SCOPE OF APPLICATIONS AND USERS

This Code applies to all FACILITAPAY employees, regardless of the country they are renting. The employees are:

•Partners and shareholders
•Directors
•Collaborators
•Temporary
•Internal
•Minor apprentices
• Customers and / or natural / legal persons who are commercially related to FACILITAPAY.

3. APPLICABILITY AND REGULATION

FACILITAPAY operates in several jurisdictions worldwide. However, the subjection of FACILITAPAY's business activity to regulation depends on the laws and regulations of each jurisdiction on the institutions that facilitate cross-border payment. As such, where

applicable, FACILITAPAY will operate in accordance with the regulatory requirements of a jurisdiction.

4. DEFINITIONS OF APPLICABILITY AND REGULATION

Money laundering

Money laundering is the common term for the process by which an individual seeks to conceal the results of a crime by exchanging ownership of the crimes for so-called "clean" money. The following activities may be associated, but not limited to, money laundering:

- Acquire, use or possess property derived from crimes;
- Concealing, concealing, transferring or manipulating assets derived from crimes such as theft, fraud and tax evasion;
- Be knowingly involved in any way with property derived from crimes;
- Investing assets derived from crime, either in financial products, or through the acquisition of goods or assets;
- Transfer of criminal assets;
- Financing of terrorist activities.

The three stages of money laundering generally are:

- Placement: this is the first phase of money laundering. It implies the insertion, in the formal economy, of the asset derived from the illegal activity; Example: putting money into the conventional financial system.
- Concealment: This second phase involves separating illicit assets from their source by creating complex layers of financial transactions designed to disguise the auditable money trail and allow anonymity.
- Integration: the final phase is to give apparent legitimacy to assets derived from crimes. If the concealment phase was successful, integration schemes insert laundered money back into the economy so that these assets re-enter the financial system that appear to be regular funds.

Based on various laws, regulations and regulatory guidelines of the Financial Action Task Force (FATF) and other applicable international best practices, FACILITAPAY will ensure that the legal obligations resulting from international anti-money laundering regulations are complied with by all employees and third parties. In relation to these, FACILITAPAY must ensure that our business model is understood and respected by any new merchant or client, avoiding irregularities such as tax evasion and other crimes.

Where local regulations are stricter than those set forth in this Policy, the stricter standards shall prevail. In the event that the minimum standards established in this Policy cannot be applied in any country, because their application would be contrary to local legislation or because they could not be imposed for other legal reasons, FACILITAPAY will ensure that it will not initiate, continue or carry out commercial relations in that country. If a business relationship already exists in that country, FACILITAPAY will ensure that it is terminated, regardless of other contractual or legal obligations.

Financing of terrorism

The financing of terrorism is any involvement with funds or property that are certain or likely to be used for terrorist purposes, even if cleared at source. For the purposes of this Policy, money laundering also includes any activity related to the financing of terrorism.

5. GUIDELINES

5.1 ORGANIZATIONAL STRUCTURE

FACILITAPY establishes and maintains an effective AML Compliance program . In general, anti-money laundering programmes should be proportionate to the risks posed by the location, size, nature and volume of the financial services provided. An effective program is one created to prevent FACILITAPAY from being used to facilitate money laundering and terrorist financing. In addition, the Facilitapay Financial Intelligence Program incorporates the FACILITAPAY Financial Intelligence Program.

The program for the prevention and fight against money laundering and terrorist financing is formulated and managed by the Legal and Compliance Department:

The Compliance/Legal Department reports to the Chief Legal Officer (CLO). Local Money Laundering Reporting Officers (MLROs) report to the Directorate of Legal. The primary responsibility of the MLRO is to ensure that, where appropriate, information or other means leading to knowledge, suspicion or reasons for knowledge or suspicion of money laundering are properly disclosed and communicated to the competent authorities.

5.1.1. Financial Intelligence Program

FACILITAPAY's Financial Intelligence Unit (FIU) is a component of FACILITAPAY's global Financial Crime Risk and Money Laundering Prevention (AML) program. The purpose and work of the FIU allows FACILITAPAY to execute aspects of its AML Program, particularly in relation to financial crime investigations, regulatory reporting, law enforcement, and engagement. The purpose of this manual is to describe the functions governed by the FACILITAPAY Financial Intelligence Program, which applies to FACILITAPAY's global operations and customer base. The program aims to ensure that FACILITAPAY continues to comply with the relevant regulatory requirements around financial crime compliance reporting in all jurisdictions in which it operates.

In addition, the Financial Intelligence Program manages the entire scope and responses of FACILITAPAY to law enforcement agencies in relation to criminal investigations, including Compliance of subpoenas and any other type of legal request submitted to FACILITAPAY by international and national agencies. The FIU ensures that FACILITAPAY responds to criminal investigations in accordance with local laws.

The FACILITAPAY Financial Intelligence Program is responsible for monitoring and identifying all types of financial crimes potentially committed on the FACILITAPAY platform, including, but not limited to:

•money laundering, associated background crimes
•Financing of terrorism
•fraud
•Bribery and corruption
•Violations of sanctions
•Tax avoidance
•market abuse
•Anti-competitive practices

5.1.2. Mission of the FIU

FACILITAPAY's FIU mission is to provide an industry-leading investigation and analysis capability capable of identifying emerging financial crimes quickly and effectively. With a global perspective, coordinating and learning lessons across investigations, countries and regions, the FIU offers clear findings and recommendations that are shared to drive proactive and impactful risk management. The FIU facilitates the effective exchange of information with internal and external stakeholders, including regulatory, law enforcement and security agencies. The FIU leverages its findings to support the continued evolution of the regulatory landscape based on practical and proven innovations.

The FIU is responsible for disseminating the results of its analysis to the competent authorities and for taking appropriate measures to mitigate internal risks. The financial intelligence program mitigates these threats through various operational functions, such as monitoring transactions, responding to law enforcement inquiries and investigations, among other methods described in this document.

The FIU reports to the Chief Compliance Officer, who has final responsibility and authority over the financial crimes program.

The FIU is responsible for disseminating the results of its analysis to the competent authorities and for taking appropriate measures to mitigate internal risks. The financial intelligence program mitigates these threats through various operational functions, such as monitoring transactions, responding to law enforcement inquiries and investigations, among other methods described in this document.

The FIU reports to the Director of Governance, who has final responsibility and authority over the financial crimes program.

5.2 RISKS

In order to develop a comprehensive and effective AML program, FACILITAPAY undergoes an AML risk assessment at least once a year. This risk assessment serves as a roadmap to guide the implementation of procedures and internal controls for comprehensive customer identification, customer due diligence, sanctions, customer monitoring for unusual activity, regulatory reporting, and record-keeping requirements. The risk assessment identifies the unique risk drivers of PLD for FACILITAPAY that arise from its specific business model, as well as several factors including: products, services, payment methods and gateways, types of target customers, partners and other relationships, geographical locations, internal controls and organization. The risk assessment includes a review of mitigation controls in all business areas exposed to the identified AML risks.

FACILITAPAY will adopt a risk-based approach to assess the most effective and proportionate way to manage and mitigate money laundering risks. The steps that FACILITAPAY will take to achieve this goal are:

- Identify relevant money laundering risks;
- Evaluate the risks present in customers, products, services, transactions, delivery channels and geographical areas of operation of FACILITAPAY,

Risk assessment is used for FACILITAPAY activities such as:

- Design and implement controls to manage and mitigate assessed risks;
- Monitor and improve the effective functioning of these controls.

FACILITAPAY's risk assessment uses the following sources when determining the risks of a jurisdiction:

•FATF
•BASEL
•Transparency International
•USDS (United States)
•HMT sanctioned countries/schemes*
•Countries/regimes sanctioned by OFAC*

** All regimes/areas where complex sanctions have been imposed are blocked due to the risk they pose.*

FACILITAPAY will evaluate the risk of each client, taking into account the purpose of the account or relationship, the level of assets or the size of the transactions to be executed and the regularity or duration of the commercial relationship. The risk assessment will also consider customer risk factors, products, services, transactions, delivery channels and geographic areas.

It is important to provide the customer's current risk level:

•Significant risk factors
•Negative news research about account managers, beneficial owners and control persons associated with the account
•Previous processes/presentations; If there is, provide an overview of the results.

Low-risk customer risk factors:

•Public companies listed on stock exchanges and subject to disclosure rules (either by market rules or by legal obligation) that impose requirements to ensure adequate transparency of final beneficiaries;
•Customers residing in low-risk geographic areas.

Risk factors of high-risk clients:

•Business relationship carried out in unusual circumstances;
•Customers residing in high-risk geographic areas.
•Legal persons established by natural persons for the specific purpose of managing assets for investments (personal asset holding vehicles);
•Companies that have registered shareholders or bearer shares;
•Persons who are politically exposed persons and companies that have such individuals as shareholders and/or legal representatives;
•Companies whose significant share of income is in cash;

•Companies whose corporate structure appears to be unusual or too complex, given the nature of the company's business.

The customer risk score is the foundation of KYC requirements. FACILITAPAY implements a risk-based approach when performing risk rating. This process consists of evaluating the customer's risk factors with a numerical value during the integration process.

The risk of the product is equivalent to 25%. The risk of the product includes the services that FACILITAPAY offers to a client and the services / products that a corporate client can perform or offer to its users. With a weighting of 25%, the product risk factor takes into account a customer's transaction risk, looking at anticipated transaction volume and type of activity, as well as trading expectations. Several high-risk products and services are measured in the product's risk scoring methodology. There are additional services that customers may offer that present a higher risk. A complete list can be found in the risk score matrix.

Risk factors for low-risk products, services, transactions or delivery channels:

•Financial products or services that offer defined and limited services to certain types of customers in order to increase access for financial inclusion purposes;
•Products where the risk of money laundering and terrorist financing is managed by other factors, such as transparency in the corporate structure.

Risk factors of high-risk products, services, transactions or delivery channels:

•Private banking;
•Products or transactions that may promote anonymity;
•Business relationships or virtual transactions without safeguards, such as digital signatures;
•Payments received by unknown or unassociated third parties;
•New products and new business practices, including new delivery mechanisms, and the use of new technologies for new and pre-existing products.

Low-risk geographic risk factors:

•Countries with effective anti-money laundering systems;
•Countries that have a low rate of corruption and other criminal activities, according to reliable sources;
•Countries that, according to reliable sources, have requirements to combat money laundering and terrorist financing and that effectively implement them.

High-risk geographic risk factors:

•Countries that do not have effective anti-money laundering systems;
•Countries that have a significant rate of corruption and other criminal activities, according to reliable sources;
•Countries subject to sanctions, embargoes or similar measures applied, for example, by the United Nations (UN);
•Countries that finance or support terrorist activities or that have organizations considered terrorist on their territory.

Customers will be classified into risk categories: high, medium or low. Those classified as "high risk" will have to go through an Enhanced Due Diligence (EDD) process.

5.2.1. Risk Level Section (Assessment and Categorization):

In the process of evaluation and verification of the client and its level and risk, FACILITAPAY will evaluate the documents and information provided in order to evaluate the category of risks, and the following actions may be carried out:

a) After reviewing the information, an "Alert" or "Non-match" decision must be made using criteria defined by the Compliance Committee.

b)The following reason code should only be used if approved by management and properly documented:
-Paired, but irrelevant

c)If any of the following reason codes are used, you must add escalation:

-Insufficient information (requires scaling)

-No location match (requires a note detailing at least one other data point used for denial)

-No longer associated (requires a note detailing the steps taken to ensure the relationship no longer exists)

-It is not a correspondence (requires a note detailing two reasons for the refusal)

-Unrelated to PLD (requires a note detailing the reason for the denial)

-Pre-corrected (requires a note detailing the previous alert and any new information)

When a positive match is identified, it is marked as an alert and requires escalation. The escalation process will vary depending on the type of alert.

(d)Sanctions alert

Sanctions matches present significant regulatory risk and require immediate action. Therefore, once a positive match is confirmed, it should be immediately sent to a Compliance Manager or a designated person for the next steps. Matches must be tracked in the sanctions tracking log.

5.2.2. Red flags (RED FLAGS)

The main focus of FACILITAPAY is to report suspicious activity to determine if transactions are in fact linked to money laundering, market abuse, terrorist financing or a specific crime. The following examples are warning signs of RED FLAGS that, when found, may warrant further analysis. This is not an exhaustive list and the mere presence of a red flag is not, in itself, evidence of criminal activity. Closer scrutiny should help determine if the activity is suspicious or if there does not appear to be a reasonable business or legal purpose.

Examples of red flags:

•The identification documents provided to FACILITAPAY appear to be fraudulent or modified.

•IP address ranges do not match the associated IP ranges correlated with the account location.

•The user's name appears on a sanctions watch list.

•The user is the subject of news indicating possible criminal, civil or regulatory violations.

•Funds derived from illegal activities or the intention to hide funds derived from illegal activities.

•Funds made in a manner that indicates structuring-like activity in an attempt considered by that transactor to avoid record-keeping or reporting requirements.

•Transaction with no apparent legitimate purpose.

•Activity that is not consistent with the consumer's normal activities.

•The volume of user transactions has a large increase that cannot be explained.

•The user deposits and withdraws funds without trading.

•Sudden spikes in activity after long periods of inactivity.

•Police citations indicating that a user may be involved in a financial crime.

• A user demonstrates changes in features, for example, luxurious lifestyles.

•Significant trading inconsistent with market fundamentals.

•A particular trade caused an exceptionally large profit or loss for the user.

5.3 DUE DILIGENCE

A customer is any individual or company (user or merchant) to whom FACILITAPAY offers, intends to offer or has offered in the past a service and / or a product. Therefore, potential customers are also included in this concept. Anonymous customers or transactions from anonymous individuals or companies will not be accepted.

A partner is any individual or company (supplier, financial institution, agent, referral, independent professional) that provides products and / or offers services to FACILITAPAY.

Before incorporating any new Merchant, user or partner, FACILITAPAY must perform the Due Diligence process. Some third parties will offer a higher risk than others. In order to determine the level of risk offered by a third party, all of them will go through an implicit Due Diligence process and will have their risk defined through the Risk Assessment plan.

The Risk Matrix is based on criteria related to geographical, financial and business risk factors of the third party, among others. These criteria will be classified as low, medium and high, and a different score will be assigned to each risk level. The set of criteria will allow defining the risk that each third party represents for FACILITAPAY. Third parties assessed as "medium risk" will undergo a standard due diligence process. Those evaluated as "high risk", from Enhanced Customer Due Diligence.

5.3.1. Simplified due diligence

Simplified due diligence involves gathering information and documents
that allow:

•Identify the third party and verify their identity;
•Establish the nature of the business relationship;
•Conduct a check to identify whether the third party is a Politically Exposed Person (PEP) and/or is subject to sanctions;
• Ensure that any person acting on behalf of the third party is authorized to do so, as well as identify and verify that person;

Once this process is completed, the Risk Assessment will be conducted to determine the level of due diligence required.

5.3.2.Standard Due Diligence

For each client and user, FACILITAPAY will make an overview, which includes the relationship with the client, the document containing the start date of the relationship, the level of risk, the purpose of the account, the authorized account administrators and the associated accounts.

In addition to the checks carried out in the Simplified Due Diligence process, third parties whose level of risk is medium must go through the Standard Due Diligence process, which involves:

•Full identification and verification of any beneficiary owning 25% or more of the company (in case the beneficial owner is another company, verification should be done only in relation to the shareholder company, and not to its directors);

•Negative media verification of all involved.

The overview shall also include the following information:

•Name

•Client type

• Legal structure, if applicable (Limited Liability Company, Public Limited Company, etc.)

•Unique identifier (CNPJ, etc.)

•Embedding information (country, state, date, etc.)

•Physical location (Google Map search) countries of operation

•Description of the shareholding

•Brief description of the nature of the business, products and services

•Website (if available)

In summary, when opening the account, FACILITAPAY obtains certain identifying information about all customers and users through a risk-based approach, indicating: The classification of the client as a natural or legal person, the determination of the owner or final beneficiaries for legal entities, the identification of politically exposed persons and the type of product or service to be used. This allows FACILITAPAY to understand whether the customer or transactions pose a financial crime risk, and whether certain customers, such as those identified as high risk, require further customer due diligence.

A review process is also conducted to complete due diligence on these requests. Once the review is complete, it will be scaled for approval.

5.3.2.1Selection of sanctions and watch lists

Sanctions selection and watch lists are performed by a third-party provider. This includes the detection of sanctions, politically exposed persons (PEP) and negative news. The selection will be made on all customers and users (includes account name, authorized

accesses and beneficial owners). Screening will take place during onboarding and from there on a daily basis using a risk-based approach.

All evaluations correspond to the jurisdictions in which FACILITAPAY operates.

During the course of selection, if a possible combination cannot be decided, additional documentation may be requested.

5.3.2.2. Control of sanctions

FACILITAPAY reviews customers against all sanctions lists required for the jurisdictions in which it operates. Additional comments by Governments are considered under various global and targeted sanctions.

Any entity that has obtained licenses, exemptions, authorizations or certificates from the relevant authority to conduct business with sanctioned jurisdictions or activities will be escalated and reviewed by Compliance. These can then be escalated to a compliance administrator for review on a case-by-case basis. In addition, senior management approval is required before allowing any activity.

5.3.2.3 Politically exposed persons

Existing customers will have a retention decision made during the review. The source WBS alert is tracked in the trace log.

5.3.2.4. Negative news/media alert

New customers determined to be associated with negative news/media will be denied registration upon boarding. The existing customer associated with negative news will be escalated to a review of the EDD, which when completed will determine the risk it presents and whether FACILITAPAY will proceed with the closure of the account. Negative news alerts are tracked in the trail.

FACILITAPAY scans customers (including account managers and beneficial owners) for negative news. Customers associated with negative news will be analyzed by the Compliance team to determine the risk presented to FACILITAPAY. Negative news detection will include the following:

- False acts or statements with the intent to obtain or deprive money, goods or services in error; includes fraud, scams, Ponzi schemes, pyramid schemes, wire fraud, charity scams, decoys and barter schemes;
- Offences related to concealment or concealment of the source of proceeds of crime; includes money laundering, illicit financing schemes, stratification of funds, laundering of criminal proceeds, money smuggling, structured currency transactions;
- Crimes related to organized crime groups/gangs; includes organized crime, criminal association, extortion;
- Crimes related to terrorist groups or individuals;
- Listed entities under government surveillance.

5.3.2.5. Office of Foreign Assets Control (OFAC):

FACILITAPAY will evaluate customers (including users, account administrators and beneficial owners) to ensure that they do not appear on the list of Specially Designated Nationals (SDN). FACILITAPAY will also ensure that it does not engage in transactions or activities prohibited by economic sanctions and embargoes administered and applied by OFAC. All OFAC sanctions will be applied globally within the corporate structure of FACILITAPAY.

As the SDN list and economic sanctions and embargo lists are updated frequently, we will check with them regularly to ensure that automatic updates to the list are accurate and timely on our third-party provider.

5.3.3.Enhanced due diligence

This manual will be used to supplement the requirements of the PLD program by applying EDD to the identified high-risk functions. This document details the procedures by which the Compliance team will be responsible for the fulfillment of each function. These

improved processes and procedures will be used to assess and mitigate risk, ensuring the implementation of an effective risk-based approach.

The role of the Enhanced Due Diligence (EDD) sub-team is to implement enhanced processes and procedures for clients and activities that present a higher than normal risk of money laundering and terrorist financing, or other inherent compliance risk. The areas identified as having the highest level of risk will be defined in this document, along with the controls in place to mitigate these risks. The EDD Compliance team has the role and responsibility to conduct initial and periodic EDD reviews of higher-risk clients.

There are categories for each type of user account. The Pro account level is for high-volume individuals and all corporate accounts. Professional accounts go through due diligence, including all the requirements from the previous level along with additional documentation, financial statements, anticipated activity, open source research, and more.

In addition to the checks carried out in the Simplified and Standard Due Diligence processes, third parties classified as high risk must undergo the following checks:

•Source of income of the company's partners – in the case of PEP, evidence is required through documents;
•Full identification and verification of all beneficiaries, including verification of company directors;
• Identification of the final beneficiary, when applicable, verifying their identity and seeking to understand the control structure of the company, when applicable.

Enhanced due diligence measures also include:

•Increased frequency of review to verify that FACILITAPAY is still able to manage the risk associated with the business relationship and help identify any transactions that require further review;
• Increased frequency of review of the business relationship to verify whether the risk profile of the third party has changed and whether the risk remains manageable;
•Obtain approval from the local MLRO to initiate or continue the business relationship in order to ensure that senior management is aware of the risks to which FACILITAPAY

is exposed and to enable them to make informed decisions about how much we can manage these risks;

•Track transactions more frequently or in greater depth in order to identify any unusual or unexpected transactions that may raise suspicions of money laundering or terrorist financing. This may include setting the destination of the third party's funds or defining the reason for certain transactions.

The due diligence process must also be executed at any time when FACILITAPAY suspects or has reason to suspect money laundering or when it is believed that expired or inaccurate documents or information have been provided. Any business relationship with a merchant or user will be subject to constant monitoring, which may result in employees being asked at any time to perform due diligence or seek additional information about such individuals and companies. Commercial relationships and transactions must be consistent with the knowledge that FACILITAPAY has about the Merchant, the user or the partner, as well as about their business, risk profiles and sources of income.

When the risk exceeds the appetite of the business, the third party will not be integrated into FACILITAPAY. If the requesting area believes that the opportunity is important enough and that alternative controls can reduce the identified risk, formal exceptions may apply.

5.3.3.1 EDD Operating Procedures: Case Evaluations

As detailed in the previous sections, when a customer is first identified as high risk, an initial review of the EDD is required. This will happen at the time of detection during watchlist selection or once escalated to the Committee ofOmpliance during client onboarding. After an initial review, high-risk automated clients will maintain a semi-annual periodic review, while all others will maintain an annual review.

Once the review is complete, it will be escalated to a Compliance Manager or designee for approval.

The person who completes the EDD review is responsible for completing the EDD case selection. In the trace log, all case numbers are predetermined, and this unique number

will be used throughout the customer's high-risk lifecycle. If periodic reviews are required, the same trace entry is updated with the current information. Within the trace log, several columns were provided with set values to ensure consistency.

The next review date in the crawl is set using the end date of the current review, which is the date the EDD review is completed and scaled for approval. The EDD case tracking log will also maintain an approval date, which is the date a Compliance Manager or designee approves the review.

5.3.3.2. Risk scoring methodology

A)Types of high-risk clients

This factor includes higher risk types of customers, as well as products and services offered by customers who have been identified as being at high risk for money laundering and/or terrorist financing. These types of clients are determined through regulatory requirements or international guidance and may change throughout the lifecycle of this risk rating methodology. The risk scoring methodology is reviewed annually to ensure that the score is in line with current trends and practices.

B)Risk Watch List - Automatic High Risk

FACILITAPAY uses an external provider for the automated selection of politically exposed persons, sanctioned individuals and entities, and negative news. Any customer who returns as a positive match for these items is automatically considered high risk.

High-risk automated customers will be identified during the onboarding process based on the types of products and services offered. These specific types of customers will go through the normal risk scoring process to identify a risk score for each specific risk factor. However, your final risk score will be automatically set to the maximum risk score to align with the client's high-risk auto-escalation. These customers will require additional documentation and due diligence information during integration. In addition, they will be subject to periodic semi-annual reviews of the EDD, ensuring due diligence and ongoing

monitoring. The types of clients that will be considered automatic high-risk are as follows:

Client Type	Risks	Review schedule	Documentation/Information
Financial institutions / banking correspondents (excluding payment institutions, non-bank financial institutions and non-financial activities and professions designated (APNFD). Definition: Institutions Traditional finance and credit	High-risk automatic	Semiannual	Due Diligence Requirements: • Standard identification documents of the trading company; • Due Diligence Quesionário; • Copy of Compliance policies (AML and sanctions, if separate); EDD Review Guide: • Evaluate questionnaire, policies and procedures • Review of regulatory license, if applicable • Adverse means for the company, shareholders, shareholders, quotas, parents, subsidiaries and officers • Evaluation of: o Jurisdictions in which the company operates o Customer base o Products & Services o Correspondent banking activity
Politically Exposed Persons (PEP) Definition: the following are considered politically exposed persons: the holders of elective mandates of the Executive Powers and Legislature of the Union; the occupants of the office, in the Executive Power of the Union, of: Minister of State or equivalent; Special or equivalent nature; President and, Vice-President and Director, or equivalent, of entities of the indirect public administration; and Senior Management and Advisory Group - DAS, level 6, or equivalent; the members of the Federal Supreme Court, the Superior Courts and the Federal, Labour and Electoral Regional Courts; the Attorney General of the Republic, the Attorney General	High-risk automatic	Semiannual	Due Diligence Requirements: •The PEP assessment is done through an external provider and is reviewed by Compliance prior to integration. •Source of income •Source of wealth EDD Review Guide: •Position held •Official responsibilities •Specific role in relation to their authority in government •Access to government funds

of Labor, the Office of the Attorney General of Military Justice and the Office of the Attorney General of the States and the Federal District; the members of the Court of Accounts of the Union and the Public Prosecutor General of the Public Prosecutor's Office of the Court of Accounts of the Union; presidents and national treasurers, or equivalents, of political parties; the governors and secretaries of State and of the Federal District, the Deputies of State and Districts, the presidents, or equivalent, of entities of the state and district indirect public administration and of the presidents of Courts of Justice, Military, Accounts or equivalent of the State and the Federal District; the Mayors, Aldermen, Presidents of Courts of Accounts or equivalent of the Municipalities; Heads of State or Government; high-ranking politicians; occupants of government positions at higher levels; general officials and members of the senior levels of the judiciary; senior executives of public companies; or leaders of political parties; Leaders of higher levels of entities governed by public or private international law.			•Source of wealth oCountry/government risks oGlobal risks for countries oSpecifically address the risk of corruption and bribery established in the jurisdiction oAddress specifically whether financial crimes and political/government corruption have been criminalized •Associated relationships (for example, they maintain a corporate relationship, are a UBO of any company account maintained by FACILITAPAY, maintain any invoice, etc.) Elimination of Automatic High-Risk Monitoring: Individuals identified as PEP may be removed from automatic high-risk if they no longer meet PEP requirements and/or maintain their positions for a period of 5 years or more.
Other financial services Definition: • Trader or currency exchanger • Traveler's Check Issuer, Money Orders • Seller or casher of traveler's checks, money orders • Facilitators and payers or exchangers Virtual Currency Manager and Merchant • Virtual exchange platforms and • Fiat wallet providers	High-risk automatic	Semiannual	Due Diligence Requirements: • Standard identification documents of the trading company; • Due Diligence Quesionário; • Copy of Compliance policies (AML and sanctions, if separate); • EDD Regulatory License Review Guide: • Evaluate questionnaire, policies and procedures • Review of regulatory license, if applicable •Risk assessment of the products/services offered •Risk assessment of clients and jurisdictions served

Watchlist detection (excluding PEPs): Definition: Sanctions and adverse means will be immediately escalated for review by Compliance. Abolition of automatic high-risk surveillance of sanctions and The adverse means will be determined by an assessment of The risk presented	Automatic positive match/high risk	Semiannual	Due Diligence Requirements: •Standard integration requirements •Additional documentation may be requested to determine if customer risk can be mitigated.

C)Other types of high-risk clients:

Customers who do not meet the automatic high-risk criteria can still rate high-risk based on the combined risk factors. Once these clients are identified as high risk through the onboarding process, they escalate to EDD supervision of high-risk accounts.

The following are all other types of customers:

Client Type	Risk	Review schedule	Documentation/Information

Non-bank financial institutions, excluding payment institutions and stock exchanges. Definition: An entity that performs financial services other than a traditional bank. • Entities providing services in the capital market, including security and commodity firms, brokers, investment advisers, mutual funds, hedge funds, commodity traders, etc. • Insurers • Credit and financing companies • Trust Companies • Dealers in precious metals, stones or jewelry; Lenders • Financial advisors • Financial services companies • Dealers in precious metals, precious stones or jewellery • Jewelries • Scalpers • Luxury goods seller Casinos or equivalent gambling establishments.	High Medium Low	Annual None None	Due Diligence Requirements: •Standard integration requirements •AML and KYC Program •Regulatory license, if applicable EDD Review Guide: •Owner, controller, and director searches •Jurisdictions in which the entity operates •Customer base •Risk of products and services •Risks associated with regulatory news, if applicable.
Private ATM operators Definition: Entities that own or operate ATMs, and may or may not include cryptocurrencies.	High Medium Low	Annual None None	Due Diligence Requirements: • Standard integration requirements; • ATM questionnaire; • PLD/KYC Program, where applicable; • Regulatory license, if applicable; • ATM Contract; • Required ATM Due Diligence Questionnaire: • How many ATMs do you own and operate? • In many places, do ATMs work electronically? Provide addresses for all locations. • Do ATMs offer shopping and selling services?

			• If you offer vending services, who is responsible for replenishing the ATM with coin? Are you a trustworthy person? • For the purchase of services, is an instant messaging service used to deliver currency to a financial institution? • What currencies are accepted at the ATM? • What are the dollar transaction limits for buying and/or selling? • What identity verification procedures does the ATM offer? • What is the expected volume of daily/monthly ATM transactions in your account? EDD Review Guide: • Evaluate ATM questionnaire; • Evaluate Compliance policies and procedures; • Comply with the regulatory requirements of the country; • Analyze the location risk with the services provided.
Third Party Payment Processors Entities that provide payment processing services to their customers, such as Internet-based entities, Internet gaming companies, credit card payments, etc.	High Medium Low	Annual None None	Due diligence requirements: -Standard integration requirements: • AML/KYC program, if applicable; • Details about the Commercial Customer base ; • Details about the client's business activities; • Top 10 client list; • A copy of the marketing materials; EDD Review Guide:

			• Evaluation of controls; • Policies and procedures; • Search for complaints; • Use of open source searches, including surveys on consumer protection sites.
Professional Service Providers (PSPs) and Designated Non-Financial Activities and Professions (DNFBPs). Definition: PSPs and DNFBPs receive an additional risk value based on the type of activity. These companies and professions include the following: • Corporate service providers; • Companies; • Fiduciary; • Real estate agents; • Lawyers/legal professionals; • Counters; Tax advisors, auditors	High Medium Low	Annual None None	Due Diligence Requirements: - Standard integration requirements: • Active Professional License with the regulatory body; • Monitoring log; • LDP Policy; • Structure of the organization. EDD Review Guide: • Services and products; • Jurisdictions; • Active license registration.
Other Definition: All other types of customers that qualify as high risk based on the combined risk factors in the matrix. Example: A customer gets a high-risk score based on their activity, no activity is reported on the customer's account. If the risk factors do not correspond to the actual risk presented, the client can be eliminated.	High Medium Low	Annual None None	Due Diligence Requirements: - Standard integration requirements: Additional documentation may be requested to mitigate customer risk. Elimination: Customers who obtain a high-risk score based on their combined risk factors may be removed from high-risk monitoring if it is determined that their risk score does not match the actual risk presented.

5.3.3.3 High-risk client approval process

Because high-risk customers present significant risks, they must be approved by various levels of seniority within the organization. The overall customer approval process begins during onboarding and verification. During this process, identified high-risk customers must comply with the customer due diligence requirements set forth herein. Once all CDD requirements are met, they will escalate to Compliance.

High-risk clients will have an initial EDD review completed by the Compliance Department, which will further assess the client's risk score and any other relevant risks that may be present. The EDD review will also contain a review of all mitigating factors, conduct open source research, and transactional analysis. Compliance will make a recommendation based on its findings and the customer's overall risk.

Once per fiscal quarter, a list of all high-risk clients will be sent to the Chief Compliance Officer for approval by Senior/Executive Management. This list will accurately reflect our high-risk customer profile to ensure our risk profile and tolerance levels are aligned across the organization.

5.3.3.4. Continuous risk scoring and removal from the high-risk category

PAY continuously reviews clients using a risk-based approach. If it is identified that changes have been made to a client's business model, structure or overall business, this may warrant requesting additional documentation and a reassessment of their risk score. The Compliance Committee can identify such changes during the regulatory course of business by conducting EDD analyses of high-risk clients. If identified, the customer will be sent to the Customer Engagement (EC) team to perform a new customer risk score assessment. The EC can also perform a continuous customer risk score based on various triggering events that result in a potential change in the customer's overall risk. These triggers include the following:

•A change in ownership structure resulting in significant changes (e.g. a company that was once owned by a single individual is now identified as owned by a holding company with the UBO being owned by the holding company).

It can be identified that a client does not meet the risk factors presented when establishing the account or does not maintain significant activity to justify the inherent risk. Examples of these situations can be found in the table of high-risk customers (point 5.3.3.2). If such a situation occurs and the client does not disclose the risk, several results can be obtained. For example:

•If the customer's account is inactive with no activity for a period of one year. The customer's account can be blocked until the customer initiates contact. The client can be removed from high-risk supervision if the account is blocked. If the client wishes to unblock the account, the client's relationship will be evaluated later to determine if there is still justification for high-risk monitoring;
•If risk is not present, such as an integration error or PEP removal, the customer's risk score is updated and the customer can be removed from high-risk supervision.

5.3.4. Facilitapay will not do business with:

•Persons or companies suspected of money laundering and/or terrorist financing;
• Shell banks;
•Individuals or companies for whom the required level of Due Diligence has NOT been performed;
•Users listed as not acceptable by FACILITAPAY's Policies;
•Companies based in sanctioned countries.

In relation to the specific incorporation of Merchants, some types of businesses are not accepted by FACILITAPAY. Please refer to our lists of restricted and prohibited products and services in the appendix to this manual.

5.3.5. Possible recommendatory actions

The results of the comprehensive analysis should be documented by a general recommendation. This should include reasons to support one of the following recommendations:

• Retain the client at the existing risk level with periodic review;

•Retain the client and refer him for FIU investigation;

•Forward the client to the FIU with a recommendation to close the account;

•Remove the client from the automatic high-risk category in the wakeof the case review;

• Recommend the closure of the account based on the risk presented by the client.

5.3.6.Penalties

FACILITAPAY will block Merchants, users and / or entities originating from countries that do not respect the sanctions programs, in order to ensure that the company does not do business with sanctioned persons and organizations, combating, financing and proliferation of weapons of mass destruction.

Some jurisdictions pose an exceptional risk in relation to money laundering and financial crime. These jurisdictions are identified by the FATF as having weak controls or requiring action or are regimes sanctioned by the United States of America or the United Kingdom. The geographical risk shall be reviewed and updated annually. Traders, users and partners are verified for sanctions through a global database with access to over hundreds of thousands of sanctions list sources.

Analytically, FACILITAPAY analyzes all individuals, companies, entities and beneficial owners, including customers already registered, against various lists of prohibited transactions to confirm that FACILITAPAY does not authorize a transaction with any prohibited person or entity. These individuals and legal entities are identified on publicly available lists that require compliance with targeted financial sanctions based on United Nations Security Council resolutions or the U.S. Office of Specially Designated Nationals Foreign Assets Control (OFAC) list.

When appropriate, FACILITAPAY will block and / or freeze financial assets and report the incident to the competent authority.

The process of blocking funds varies depending on the funds involved. If FACILITAPAY maintains custody of securities, it will block the funds and place them in an interest-bearing account established in a corresponding institution. The account will be labeled

as "Blocked Funds" until OFAC or another competent authority issues guidance regarding the required action.

FACILITAPAY will record all rejected and blocked transactions through compliance tracking and audit logs to ensure a clear audit trail of the process.

5.3.7. Compliance Review

A) An overview

An overview of the client's relationship with FACILITAPAY will be carried out containing: start date of the relationship, level and purpose of the account, authorized account administrators and associated accounts. The overview should also include the following information:

•Name
•Client type
•Legal structure, if applicable (Unipersonal, Limited, S/A, etc.)
• Unique identifier (CNPJ)
• Embedding information (country, state, date, etc.)
•Physical location (Google Map search) countries of operation
•Description of the corporate structure
•Brief description of the nature of the business, products and services
•Website (if available).

B) Transaction analysis

In addition to the overview, it is imperative that FACILITAPAY performs a transaction analysis that provides: type of customer (personal / business), categorical level (Basic, Intermediate, Advanced), a review of the activity in the last 90 days or since the beginning of the relationship. In addition, the analysis should include:

• Total balance in the account
•An analysis of deposits and withdrawals
•Breakdown of fund usage, including margin trading, if applicable.

C)Notification of changes

When alerts are generated through initial or continuous classification, the Compliance team will be responsible for reviewing and deciding on alerts. If an alert cannot be decided based on the information held by FACILITAPAY, additional documentation may be requested from a customer. If a customer doesn't respond, the app, or the account, that fact may justify rejection or termination.

Any change in a Merchant's legal entity should trigger a review of Compliance at that Merchant.

It is the responsibility of the Merchant to notify FACILITAPAY whenever there are changes in relation to:

• Corporate structure and control of the company (directors and final beneficiaries);
•Company controller;
•other persons authorised to sign by the company;
• Negative media, at the time they are disclosed or known to the Merchant, and other relevant information.

D)Sanctions risk assessment

FACILITAPAY must carry out an annual assessment of the risk of sanctions. This will analyse the inherent risks associated with FACILITAPAY's business model, including products and services, jurisdictions andinternal controls. These factors will be analyzed along with the mitigation implemented to reduce the overall risk presented. The result will be the residual risk, which is the final risk presented to FACILITAPAY. Once all residual risks have been obtained, the average will be FACILITAPAY's overall sanctions risk.

E)Review of EDD cases

The EDD case review template outlines the sections that need to be completed and will be used to monitor high-risk EDD accounts.

EDD Case Review Determination: EDD case reviews will maintain predefined recommendations for selection to ensure a standardized approach to these recommendations and their subsequent procedures. The recommendations are set out in the following table:

1. Retain and monitor	Retain the client for periodic monitoring.
2. Retain and consult	Maintain monitoring for the client's newspaper and refer it to the FIU for investigation by the AML.
3. View and close account	Refer the client to account closure and an AML investigation at the FIU.
4. Elimination of high-risk monitoring	Remove the customer from EDD's high-risk testing and continuous monitoring.
5. Recommend account closure	Recommend account closure.
6. Wait for additional information	Await additional information/documentation to conclude the EDD review.

An EDD case is referred to the FIU when a possibly suspicious or unusual activity is identified. This can be determined when the reviewer has reason to suspect that the activity may be related to money laundering, terrorist financing, or another financial crime. The FIU shall investigate the referral on the basis of its internal procedures.

Confirmed PEPs will undergo an EDD review to determine the risk they present. This review must be completed before new customer onboarding is complete. The reader is responsible for adding the WBS to the EDD case review follow-up sheet.

5.3.8. Risk mitigation

The Committee must provide what mitigation measures are in place for the customer to fall within FACILITAPAY's risk tolerance. The indication shall include:

• Additional due diligence questions addressing factors such as source of funds/equity, business model, business activities, anticipated activity, purpose of account;
• Appropriate AML policy and/or other documentation;
• Regulatory environment;
• Federal and state license/registration/license;
• Bank statements;
• Tax return;
•Copy of lease agreements;
•Organization chart.

5.3.9.Due diligence for outsourced institutions and potential investors

FACILITAPAY will perform due diligence on customers for the use of third-party financing options, as well as on potential investors. They are not designated as high risk for continuous monitoring. This process is a unique assessment of the risk presented to determine if the action is within our risk tolerance or if additional mitigation controls are required.

5.4 DATA STORAGE

FACILITAPAY will store the data of all the data obtained in order to identify the Merchants, users and partners, as well as their documents, in accordance with the regulations.

In general, records related to the FACILITAPAY PLD Program must be kept for a period of five years from the date of the transaction. If a particular jurisdiction requires the retention of records for more than five years, the FIU will retain the records in accordance with local laws. This retention period includes allFIU-related documentation, including alert reviews, investigations, law enforcement inquiries, and more. Copies of all archived reports and the original or copies of any supporting documentation are retained for five years from the date of submission of such report. FACILITAPAY retains all necessary documents under all laws and regulations and is governed by its AML program in all jurisdictions in which it operates.

FACILITAPAY will store:

5.4.1. Customer Information

•All the steps to identify those interested in establishing business relationships with FACILITAPAY or the reasons why these steps were taken;

• Full name and date of birth of the people with whom FACILITAPAY does business;

•the form and origin of the funds and/or securities;

•the form and destination of funds paid or delivered to the client or another person on his behalf;

5.4.2. Transaction Information

•The financial transactions executed by FACILITAPAY with or for each client;

•Reports of suspicious internal and external activity, reasons for not reporting. These documents must be retained for 5 (five) years after the report is made.

5.4.3.Training

•Materials and tests;

• Test results;

• Training dates;

•Nature of training;

•Who was trained;

5.4.4 . Decision Making

Reports and reports to the Executive Level of actions and omissions, accompanied by the reasons for doing so;

Data and information can be stored in the following ways:

•Original documents;

•Copies of original documents;

• Scanned copies;

• Electronic formats;

At the end of the five-year period, FACILITAPAY will delete any personal data, unless the company is obliged to keep data containing personal data for legal reasons or due to a judicial process or the individual. To whom the data belongs has given its express consent for it to be retained.

5.5 MONITORING

FACILITAPAY will carry out regular monitoring of customers and transactions in accordance with its Risk Assessment. Monitoring should also be done to ensure that policies and procedures are implemented correctly.

Customer behaviors or problems with the customer's business may be alerts that further investigation by FACILITAPAY will be considered "Red Flags". Examples of red flags are:

•The customer is reluctant or evasive in providing information;
•The client's lifestyle is incompatible with their source of income;
•The client's business structure is unnecessarily complicated;
•There is participation of third parties without any valid reason;
•The client passes unusual instructions;
•There are repeated or unexplained changes in the instructions;
•Use of the bank account without valid reason;
•The client seems disinterested in prices, commissions, costs, etc.;
•There are transactions different from those expected of the client;
•Unexplained transfers of funds.

If red flags are identified in the Due Diligence or client monitoring processes, those responsible must notify the MLRO immediately.

FACILITAPAY uses an internal solution or deep monitoring to identify any unusual or unexpected transaction that may lead to suspicions of money laundering or terrorist financing.

Based on FACILITAPAY's knowledge of the client, the monitoring will seek:

•Unusual behaviour: abrupt or significant changes in transaction activities, in value, volume or nature, such as change of beneficiary or destination of money;

•Connected relationships: common beneficiaries and senders in accounts and/or clients in which there is apparently no relationship;

•Geographic high-risk countries, regions and institutions: significant increases in activity or consistent high levels of activity with geographic high-risk countries, regions or institutions;

•Other typical money laundering behaviors: indications of possible money laundering, such as transactions below reported limits, in round or extremely complex numbers;

• Current relationships: FACILITAPAY will carry out retroactive and customer reviews to ensure that the ongoing business is consistent with what was agreed when the customer entered.

FACILITAPAY will carry out the monitoring of transactions, verifying their values, volumes and speed. The most intensive alerts will be linked to those that pose the greatest risk.

Alerts will be triggered to ensure we monitor transactions and report suspicious transactions.

All new products proposed by FACILITAPAY must undergo a compliance analysis. The analysis aims to identify specific financial risks and areas that need to be analyzed, so that these risks are mitigated.

5.5.1.Detection and Reporting of Suspicious Activities: Monitoring ofAlerts

FACILITAPAY uses a manual and automated surveillance method to monitor non-maliciousor suspicious activities; These surveillance methods are applied to all types of transactions and customers worldwide. The FIU is responsible for analysing alerts triggered by various sources, including market surveillance and transaction tracking. The FIU analyzes alerts regarding all types of transactions that occur on the payment platform, determines the financial crime risks posed by transactions, and takes measures to mitigate the risks (e.g. filing a suspicious activity report).

High-risk clients typically require additional documentation and/or information to mitigate some of the risk associated with their relationship. In doing so, the due diligence that was obtained during EDD reviews will ensure that this information and documentation remains up to date. By collecting this documentation, an EDD review may exceed the expiration date of a subsequent review by 30 days if approved by a manager. Such extensions should be rare and only if additional information or documentation is required.

5.6 CLOSURE

It is possible that FACILITAPAY must terminate a business relationship after identifying suspicious activities. Even if there is no suspicious activity, the local MLRO may still recommend that the relationship with merchants, partners, or other third parties be terminated based on the risk they present.

Account closure recommendations will be reviewed and approved. Additional information about account closure steps can be found in the Account Closure Referral Process described below.

5.6.1. Account Closure Process

Account closure recommendations will require approval from Compliance Management. Senior management and formermanagement shall be notified of the closure during normal reporting processes or directly in exceptional cases where additional risks, such as reputational risk, may arise. The approval will be in the form of electronic communication or documented in minutes of meetings.

Closures may be recommended based on the inherent and residual risk presented by a client. Such risks include the business model, professional activity, refusal to provide documentation or information, negative news associated with the client or other reason that places the client outside the risk tolerance of FACILITAPAY.

You will document a closure recommendation in the case review, which will detail the specific reasons behind the closure.

5.6.2. Account closure

FACILITAPAY will take measures to mitigate the risks associated with customer accounts involved in suspicious activities that cannot be mitigated and/or are above our risk tolerance. The FIU has the authority to close suspicious accounts and prohibit customers from using any FACILITAPAY account in the future. The accounts of customers involved in the following activities (illustrative list) will be closed and the future use of any account in FACILITAPAY will be prohibited:

•Customers who harass, threaten, intimidate, or attempt to coerce, persuade, or bribe an employee not to complete any required AML notification form.
•Customers who intentionally deceive FACILITAPAY employees regarding the identity or purpose of the account or transactions.
•Customers who are identified as subjects in the reports and the Compliance Officer or AMU makes a determination in order to close the account.
•Customers designated as prohibited customers under OFAC or sanctions detection programs.

5.7 TRAINING

FACILITAPAY will ensure that all employees are trained to ensure that they understand their obligations with respect to this Policy and the requirements to identify third parties. Specific training will also be offered for various areas, depending on yourspecific responsibilities and your exposure to risk.

Employees should be aware that failure to meet their responsibilities may result in disciplinary action and/or criminal sanctions.

5.8 INTERNAL AND EXTERNAL AUDIT

FACILITAPAY's financial crime controls will be audited.

Internal audit will report to senior management on the status of controls and areas for remediation. This report shall be transmitted to the regulatory authority and to third parties.

The Compliance/Legal Department will receive all audit reports to ensure that the necessary controls are implemented effectively.

5.9 DISCIPLINARY MEASURES

Any employee who violates this Policy may be subject to disciplinary action under the Disciplinary Measures Policy. Violations will be duly investigated, in accordance with the procedures of the Ethics Committee, ensuring the anonymity of those involved. All employees are required to cooperate with ongoing investigations.

5.10 REPORT SUSPICIOUS ACTIVITY

All customer transactions are subject to constant monitoring and review. When the local MLRO decides that a particular customer or transaction should undergo further investigation, including additional assistance, employees must execute it, providing information and requests.

Any director or employee who suspects money laundering must immediately report their suspicions to the local MLRO in writing, including full details.
All signs of suspected money laundering are reportable, even if they come to the employee's attention after the transaction has taken place, the account has been closed, or the transaction has been made by someone else. By making the report, the director or employee will have complied with his legal obligations. Disclosing to a suspicious person or third party that a report is made to the local MLRO or authorities, or that an investigation is ongoing, is a breach of conduct as it may prejudice investigations. Questioning a customer about a specific transaction to learn their identity or define their source of income does not constitute a violation. In the event that areport of suspicious activity has been made, great caution must be taken so that the client is not aware of it. If suspicious signs of money laundering are identified, the transaction should be blocked

and should not proceed without authorization from the local MLRO. The local MLRO will receive reports related to any suspicion of money laundering or real money laundering and will record, investigate and report the suspicion to the appropriate authorities if necessary.

The notification of suspected money laundering to the authorities does not constitute a breach of the obligation of confidentiality with the client and provides important safeguards to FACILITAPAY. In the event that the reports are not transmitted to the authorities, all the details of the making of this decision must be recorded. All notifications made will be processed with extreme confidentiality. However, there may be circumstances in which FACILITAPAY must disclose the identity of those involved in the suspicion, such as, for example, when required by law. In this specific case, anonymity cannot be guaranteed. Any employee who fails to report a transaction known to be suspected of money laundering or cash laundering will be subject to disciplinary and legal action unless they demonstrate reasonable grounds for not reporting to the local MLRO.

In this way, employees are informed that they must report these transactions to the MLRO, regardless of how superficial they may seem. The employee can discuss the situation in advance with his direct manager, who can accept responsibility for reporting to the MLRO. Listed below are examples of transactions that may raise suspicions of money laundering, but by themselves do not necessarily generate enough suspicion to make a report:

•Liquidation of large or unusual amounts of cash;
•Buying and selling transactions without a clear purpose or in unusual circumstances;
•Instructions to direct amounts to a current account other than the one previously agreed or in the name of a third party;
•Any transaction in which one of the parties is not known or which has an unusual volume or frequency;
• Transactions in which the investor is a foreign person and both are based in countries with high rates of drug production or trafficking.

It is not the responsibility of employees to know or establish the exact nature of any crime or that specific funds or property are definitely the result of a crime or terrorist financing.

FACILITAPAY is classified as an institution obliged to comply with the obligations of Law 9.613/1998, as well as the other regulations of the Central Bank of Brazil, the CVM and the COAF. All reporting requirements will be completed when FACILITAPAY obtains information during the normal course of business in which it knows or suspects that a person or entity is subject to an assets freeze, when a person suspects or is known to have committed a financial sanctions violation, or if the assets of a designated person or entity have been frozen.

The information to be reported will include the following:

•the information or other matter on which knowledge or suspicion is based
•any information one has about the designated person or the person by whom he or she can be identified
•the nature and amount of funds/assets held by FACILITAPAY.

The FIU actively monitors employees and customers for suspicious activity. When FACILITAPAY knows, suspects or has reason to suspect that a transaction or pattern of transactions is suspicious, a case is opened and assigned to the FIU for further investigation.

5.10.1Regulatory Files/Disclosures

If FACILITAPAY has knowledge or suspicion of criminal activities by customers or employees, this must be reported immediately to the FIU. The FIU will coordinate the investigation, analyse the circumstances, gather supporting documentation and determine whether a suspicious activity report (SAR) should be submitted. If the investigation is determined to be suspicious, the case is referred to a RAS, which is submitted to the appropriate government authorities (depending on the jurisdiction). Suspicious activity reports form the basis of the financial crime reporting system. RAS provides financial information that is critical to the regulator's and law enforcement's ability to combat terrorist financing, money laundering, and other financial crimes.

5.10.1.1 RAS Archiving Responsibility

An FIU manager or compliance officer is responsible for making the final decision of whether or not a RAS will be filed. If, after investigation, the FIU determines that no SAR has been conducted, the reason for not completing the RAS must be documented, and all documentation related to the investigation is retained for five (5) years after the investigation.

5.10.1.2. RAS Reporting Schedule

FACILITAPAY will file a RAS 30 days from the determination that the transaction under review is suspicious in accordance with the RAS regulations (in the relevant jurisdiction). If no suspect was identified on the date of detection of the incident that requires presentation, in some cases FACILITAPAY may delay the presentation of a RAS for longer.

30 calendar days to identify a suspect. In no event shall reports be delayed more than 60 calendar days after the date of initial detection of a reportable transaction, unless otherwise specified and required by the applicable jurisdiction. In situations involving violations that require immediate attention, such as when a reportable violation is ongoing, the FIU shall immediately notify a competent law enforcement authority by telephone and submit a timely RAS.

5.10.1.3. Continuously unusual or suspicious activity

When suspicious activity of a FACILITAPAY customer is in progress, FACILITAPAY may register a RAS every 120 days, which includes a 90-day review of the activity from the date of the last RAS request, to update the activity and values. FACILITAPAY adds the dollar value of the previously reported activity and the dollar value of the recent activity in the most recent RAs.

5.10.1.4. Correction / modification of reports

In situations where FACILITAPAY has submitted a previous RAS with errors or has discovered new information, the Company will present a corrected / modified RAS if required by the regulatory requirements of the corresponding jurisdiction. If necessary, a corrected report will be archived in a previously archived RAS whenever errors are discovered in the data reported in that first RAS. A corrected report should be submitted in a previously archived SAR or its previous versions whenever new data on a reported suspicious activity is discovered and the circumstances do not warrant the completion of a continuous report.

5.10.1.5. Confidentiality of reports

All RAS registered by FACILITAPAY in all jurisdictions are confidential. No employee of FACILITAPAY may discuss a RAS record or the possibility of a record with a customer or other employee unless the employee is involved in RAS surveys or has another legal privilege and is not suspicious of the transaction. This obligation applies not only to the report itself, but also to the information that would reveal its existence.

5.10.2. Consultations on law enforcement agencies

FACILITAPAY may receive requests for formal legal investigations from government agencies around the world in connection with criminal investigations.
These investigations may generally require FACILITAPAY to provide internal information related to the accounts of customers, employees or other operational areas to government agencies, such as regulatory bodies and politicians. In cases that require direct contact with law enforcement authorities, the FIU is responsible for handling and complying with requests, including all communication, collection, and disclosure of requested information to law enforcement authorities.

The most common type of request is a subpoena or court order, which obliges FACILITAPAY to produce and disclose specific documents and records to an authorized government agency within a certain period of time.

In addition to subpoenas, FIU is also responsible for processing all other orders that FACILITAPAY may receive in connection with criminal and regulatory government

investigations (in all jurisdictions), including: asset forfeiture orders, freezing orders and requests, open maintenance, among others. Any person associated with FACILITAPAY who receives or is notified with a subpoena or court order related to the FACILITAPAY PLD Program must immediately contact the FIU.

5.11 REQUESTS FROM THIRD-PARTY PAYMENT INSTITUTIONS

Requests from third-party payment institutions occur when a customer chooses to use a third party for deposits/withdrawals into their FACILITAPAY account. This is due to legitimate reasons, such as gaining access to a fiat currency that your current bank does not offer. It can also occur on the basis of a lack of financial institutional acceptance based on risk reduction within specific jurisdictions. In these situations, the customer may request the use of a third-party payment processor, private bank or brokerage. Allowing such financing methods may increase FACILITAPAY's risk.

5.11.1 Applications section

This section refers to cases where a description of the customer's request must be provided.

Example: The client wishes to deposit into the account of a wholly-owned subsidiary OR the client requests the use of a third-party payment institution.

The description shall include:

• General description of the application;

•Detail the institutionof third-party payment and the reason for the use of a third party;

•Detail any information that requires more details of the risk assessment, such as negative news, regulatory licenses, etc.

Risk mitigation
Are the client and the outsourced institution regulated entities with a confirmed license? Yes = 0; No = 10
Is the client or outsourced institution located in a high-risk country? Yes = 10; No = 0

Has the client provided all AML documents, if any? Yes = 0; No = 10; Not applicable = NA
Does PAY understand the business model and raison d'être of an outsourced institution? Yes = 0; No = 10
Does FACILITAPAY keep updated information on the final beneficiary to comply with UBO requirements? Yes = 0; No = 10
Has the client provided a reasoned legal opinion detailing the relationship and/or AML obligations? Yes = 0; No = 10
Is the outsourced company owned by the client or vice versa? Yes = 0; No = 10
Negative news involved?fueron Identified for any part Yes = 10; No = 0
Did the customer provide proof of account (e.g., statement, bank notification, etc.)? Yes = 0; No = 10
Will transactions be displayed with the customer's name and account number? Yes = 0; No = 10
Is the client or outsourced institution incorporated or operating in an offshore financial center? Yes = 10; No = 0
Under the structure of the entity or jurisdiction in which the client is registered, has the client concealed its ultimate beneficial shareholders from its ultimate beneficial shareholders? Yes = 10; No = 0
The jurisdiction of the bank or financial regulator has a reputation or Track record of allowing the operation of shell corporations/banks or involvement in other illicit financial activities? Yes = 100; No = 0
Does the nature of the business declared in the application correspond to what appears in the analysis of FACILITAPAY? Yes = 100; No = 0
Punctuation: **0-30 = Low: Generally acceptable for approval** **40-60 = Medium: additional documentation may be required** **70-100 = High: additional documentation/analysis required** *** Specific answers to the above questions may require a additional analysis to ensure that KYC requirements are satisfactory.**

5.12 REQUESTS FROM POTENTIAL INVESTORS

Business relations with potential investors and FACILITAPAY require due diligence to ensure that we know their identity, source of investment funds and identify any warning signs that may be detrimental to FACILITAPAY. When reviewing these requests, the following information should be taken into account:

•Identity of the investor
•Source of wealth
•Other known trading company, if applicable
•Risks, if applicable
• Negative news

6. NORMATIVE REFERENCES

FACILITAPAY Code of Conduct.

7.PUBLICATION AND DISTRIBUTION

Any new policy or modification of an existing document should be made available to all interested parties.

Public documents can be found on FACILITAPAY's websites.

May 2023.

DocuSigned by:
Stephano Maciel
AA05FE84FFAE436...
Stephano Maciel, CEO

DocuSigned by:
Ricardo Reis
F148429D819247C...
Ricardo Reis, CLO

DocuSigned by:
Daniel Alves
7106FCC1366547B...
Daniel Alves, COO