



Manual for Monitoring, Selection and Analysis Operations and Suspicious AML/CFT Situations

Responsible Area: Legal & Compliance

Director in Charge: Ricardo Reis

Approval Date: 07/31/2025

Internal Code: 04

Version: 1

Signature of Responsible Director:

Ricardo Reis

SUMMARY

1. OBJECTIVE	3
2. DEFINITIONS.....	3
3. SCOPE	5
4. RULES.....	5
4.1. MONITORING OF SUSPICIOUS OPERATIONS AND SITUATIONS	6
4.1.1. Monitoring Criteria for Prepaid Payment Accounts	8
4.1.2. Criteria for Monitoring Foreign Exchange Operations and eFX Services	9
4.1.3. Rules for Monitoring Restrictive Lists, Prohibited Sectors and Adverse Media	10
4.1.4. List of Red Flags	11
4.2. SELECTION AND ANALYSIS OF SUSPICIOUS TRANSACTIONS AND SITUATIONS	11
4.3. REPORTING OF SUSPICIOUS TRANSACTIONS AND SITUATIONS	13
5. ROLES AND RESPONSIBILITIES.....	15
5.1. FacilitatePay Collaborators.....	15
5.2. Compliance Area.....	15
5.3. Payment Desk Area.....	15
5.4. AML/CFT Director and/or Head of Compliance.....	15
5.4. Senior Management	16
6. LEGAL BASIS	16
7. APPROVAL HISTORY.....	16
ANNEX I.....	17
ANNEX II.....	19
ANNEX III.....	21
ANNEX IV	24

1. OBJECTIVE

Describe the internal criteria and processes used for continuous monitoring, selection, evaluation and communication of operations and situations that contain evidence of the practice of money laundering and terrorist financing crimes.

2. DEFINITIONS

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

AML/CFT: means the prevention of the practice of money laundering, terrorist financing and proliferation of weapons of mass destruction;

AML/CFT Officer: means the statutory officer responsible for complying with the obligations set forth in BCB Circular No. 3,978/20;

AML/CFT Policy: means FacilitaPay's current policy that deals with the prevention of the practice of money laundering, terrorist financing and proliferation of weapons of mass destruction;

BCB: means the Central Bank of Brazil;

Circular Letter No. 4,001/20: means Circular Letter No. 4,001, of January 29, 2020, issued by the BCB, as amended, which discloses the list of operations and situations that may constitute evidence of the occurrence of crimes of laundering or concealment of assets, rights and values, which is dealt with by the Money Laundering Law, provided for in Law No. 13,260, of March 16, 2016, subject to communication to COAF;

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 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;

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

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;

Communication: has the meaning given in section 4.3 below;

Customer: means the individuals or legal entities, as the case may be, that contract or use the products and services offered by FacilitaPay;

Dossier: has the meaning given in section 4.2 below;

eFX Services: means (i) the provision of payment services and international transfers to Clients, through foreign exchange operations or transactions in a non-resident's account in reais, enabling (i) the acquisition of goods and services, in Brazil or abroad, which occurs in (a) person; or (b) through a payment solution integrated with the e-commerce platform;

(ii) unlimited unilateral transfer; (iii) transfer of funds between an account in Brazil and an account abroad of the same unlimited ownership; and (iv) withdrawal in Brazil or abroad.

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

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

Family members: means relative, in the direct or collateral line, up to the second degree, the spouse, the partner, the stepson and the stepdaughter of PEP;

FATF means the Financial Action Task Force;

Final Beneficiaries: means (i) individuals who hold, directly or indirectly, twenty-five percent (25%) or more of equity interest in the Client; or (ii) 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 attorneys-in-fact or representatives;

Foreign Exchange Operations: means the operations of closing foreign exchange and converting international currencies, under the terms of foreign exchange regulations and in line with what is allowed by applicable laws and regulations;

Internal Risk Assessment: means the process adopted by FacilitaPay for risk assessment described and documented in a specific report;

Money Laundering Law: means Law No. 9,613, of March 3, 1998;

Manual: means this manual containing procedures for monitoring, selection and analysis of suspicious operations and situations approved by the Senior Management and updated by FacilitaPay;

PEPs or Politically Exposed Persons: means (i) holders of elective mandates of the Executive and Legislative Branches of the Union; (ii) 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; (iii) 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; (iv) 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; (v) 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; (vi) the presidents and national treasurers, or equivalent, of political parties; (vii) the Governors and the Secretaries of State and of the Federal District, the State and District Deputies, the presidents, or equivalent, 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; (viii) the Mayors, Councilors, Municipal Secretaries, the presidents, or equivalent, of entities of the indirect municipal public administration and the Presidents of Courts of Accounts or equivalents of the Municipalities; (ix) 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 (x) the directors of senior levels of public or private international law entities;

Products and Services: means any and all products and/or services offered and provided by FacilitaPay, which includes, but is not limited to: (i) eFX Services; (ii) offering prepaid payment accounts; (iii) issuance of prepaid payment instruments; and (iv) Foreign Exchange Operations;

Red Flags: has the meaning given in section 4.1.4. of this Manual;

Senior Management: means the senior management of FacilitaPay, which is currently represented by a Board of Directors composed of three (3) statutory officers;

Suspicious Operations and Situations: means any operations or situations that present evidence of the use of FacilitaPay or its Products and Services for the practice by third parties of the crimes of money laundering, terrorist financing and proliferation of weapons of mass destruction, with emphasis on the operations and situations indicated in Circular Letter No. 4,001/20;

UNSC: means the United Nations Security Council; and

User/End User: an individual or legal entity that, as a final recipient, uses the products and/or services offered by the Client. It is responsible for making the payments that are processed through the institution.

3. SCOPE

This Manual is applicable to all FacilitaPay Employees and Customers, as applicable, and must, however, be executed by the Compliance and Payment Desk areas.

4. RULES

Through the application of the appropriate criteria, controls and monitoring and selection processes, FacilitaPay is able to decide on the execution of Reports of Suspicious Operations and Situations to COAF.

FacilitaPay conducts the processes of monitoring, selection, analysis and communication of Suspicious Transactions and Situations in line with the best market practices, with the international guidelines of the FacilitaPay Group, with the provisions of Circular No. 3,978/20, the Money Laundering Law and Carta Circular No. 4,001/20. These processes are reviewed annually or whenever there are changes in the applicable laws and regulations, as well as in material changes in the products offered and/or services provided by FacilitaPay, always previously analyzed and approved by the responsible authorities, as described in this Manual.

The criteria for monitoring and selecting suspicious transactions and situations must be revisited at least annually, in order to ensure adherence to FacilitaPay's Risk-Based Approach.

4.1. MONITORING OF SUSPICIOUS OPERATIONS AND SITUATIONS

The analysis of transactions and operations executed by Customers is essential to detect changes in the transactional profile of Customers, as well as the possible use of Products and Services that may expose FacilitaPay to practices associated with money laundering and terrorist financing.

FacilitaPay conducts the procedures and internal controls associated with the continuous monitoring of suspicious Operations and Situations through software, which are responsible for monitoring transactions automatically, as well as generating instant alerts associated with the main scenarios, variables and flows previously parameterized by FacilitaPay, in order to detect and select Operations and Situations in disagreement with the established parameters.

Additionally, depending on the Client's risk classification, FacilitaPay may manually monitor the Client and its movements in order to confirm possible Suspicious Transactions and Operations.

In this way, alerts for Suspicious Transactions and Operations can be generated automatically or manually from the parameters used by FacilitaPay and must be checked later in light of the expected risk profile of the Client, pattern of transactions and/or operations executed by the Client, information obtained from restrictive lists or adverse media, among other criteria.

The minimum criteria, applicable to all operations conducted by the institution, must be considered for the purposes of monitoring and selecting Suspicious Operations and Transactions:

- a) non-compliance with the guidelines provided for in FacilitaPay's AML/CFT Policy;
- b) the Client's risk classification, especially those mapped as "High Risk", and criteria provided for in FacilitaPay's Internal Risk Assessment;
- c) PEP condition of the Client, its representative, its Family Member or Close Collaborator;
- d) request by the Client for proposals for atypical Foreign Exchange Operations;
- e) performance by the Client of atypical transactions or operations, especially those listed in Circular Letter No. 4001/20 or denominated by FacilitaPay as "*Red Flags*" (item 4.1.4. of this Manual);
- f) Need to present additional documents during the legal relationship, if the established operating limits are exceeded — US\$ 3,000 per operation and US\$ 20,000 in the last 12 months;

The Compliance and Payment Desk areas are responsible for monitoring and selecting Suspicious Operations and Situations and must have access, through internal monitoring systems, to detailed information on the operations carried out by Customers and situations that occurred, including all Customer identification, qualification and classification information.

The analysis carried out by the areas must consider the above criteria in view of the procedures for identifying, qualifying and classifying the Client and its consequent risk classification, considering, at least:

- a) purpose and nature of the business relationship with the Client;
- b) Customer's transactions and operations history;
- c) history of the Customer's location, identified through a mobile device;
- d) the Customer's consumption pattern;
- e) Client's appearance on restricted lists;
- f) difficulty in identifying the final beneficiaries.

Customers who are classified as "high risk" based on the Know Your Customer (KYC) procedure have special attention given by FacilitaPay. Additional continuous monitoring procedures applied are as follows:

- a) Annual consultation on restrictive lists, on behalf of the legal entity and/or its final beneficiaries, including negative media searches.
- b) Consultation of the presence of the legal entity and its final beneficiaries as a passive pole of criminal or sanctioning proceedings, to be carried out annually.
- c) Complete reassessment of the corporate structure presented in the Know Your Customer (KYC) process, annually, taking into account the geolocation of any companies that own/hold companies in the chain that holds the corporate Customer, including consultation of software for validating the geolocation of the company's headquarters and analysis of images related to the address of the headquarters/place of operation indicated during the registration procedure.
- d) Requirement to provide a robust Money Laundering Prevention Manual, informing adopted contingencies and the responsible signatory board.

When performing the monitoring and selection of Suspicious Transactions and Transactions, the responsible analysts and members of these areas must prepare internal reports containing the details of the transaction, the reasons for atypicality, and the possibility of communication to the regulatory bodies responsible.

Reports must be submitted to the director responsible for approval and communication decision.

The period for the execution of the procedures for monitoring and selection of Suspicious Operations and Situations may not exceed a period of forty-five (45) days, counted from the date of knowledge of the operation or situation to be analyzed.

Depending on the Suspicious Operation and/or Transaction reported to COAF and identified internally, FacilitaPay's Head of Compliance and/or AML/CFT Director may, at his discretion, and based on the high risk of setting up the practice of money laundering, terrorist financing or proliferation of weapons of mass destruction:

- a) suspend the Client's account and freeze its funds temporarily; or
- b) terminate Client's account and return the funds in accordance with applicable law.

4.1.1. Monitoring Criteria for Prepaid Payment Accounts

In addition to the minimum criteria listed in item 4.1., the following are factors for monitoring prepaid payment accounts of FacilitaPay's Clients:

- a) accounts opened less than 30 days old and that have moved funds above R\$ 1,000.00 within such period;
- b) accounts that have not moved any type of financial transaction in the last 12 (twelve) months;
- c) occurrence of Red Flags described in this Manual;
- d) payment method used to operate payment accounts (i.e., PIX, prepaid payment instrument, TED);
- e) transaction executed in sanctioned, border or port region;
- f) repeated registration changes;
- g) repeated requests for changes in the transactional limit;
- h) amount moved in disagreement with the customer's profile;
- i) time of movement in disagreement with the customer's profile;
- j) transaction with a suspicious counterparty, classified as PEP or located in a sanctioned region; and
- k) history of occurrences or accusations of fraud in the DICT.

The factors mentioned above are integrated with continuous monitoring tools, with the purpose of being promptly analyzed as soon as they occur, allowing a quick and efficient response to the variations identified.

4.1.2. Criteria for Monitoring Foreign Exchange Operations and eFX Services

In addition to the minimum criteria mentioned in item 4.1., the monitoring of Foreign Exchange Operations and eFX Services executed by Clients must consider the following factors and parameters:

- a) economic basis of the operation;
- b) foreign currency used in the operation;
- c) volume executed in the last 60 days above average;
- d) Foreign Exchange Transactions with a suspicious counterparty, classified as PEP or located in a sanctioned region;
- e) Clients and counterparties located in a medium and high risk region, as per Annex III of this Manual;
- f) occurrence of Red Flags described in this Manual;
- g) repeated registration changes;
- h) repeated requests for changes in the transactional limit;
- i) Suspicious Transactions and Transactions previously identified based on the prepaid payment account used to contribute the funds subject to the Exchange Operations or receive such funds; and
- j) Suspicious Trades and Transactions previously identified when executing the Foreign Exchange Trade or performing eFX Services.

The factors mentioned above are integrated with continuous monitoring tools, with the purpose of being promptly analyzed as soon as they occur, allowing a quick and efficient response to the variations identified.

Users and/or Clients who exceed the transactional limit defined by the institution within a period of one year must present proof of income to the Client and/or FacilitaPay, preferably the Income Tax Return, in order to demonstrate their financial capacity and justify the transaction.

4.1.3. Rules for Monitoring Restrictive Lists, Prohibited Sectors and Adverse Media

As an integral and essential procedure for the continuous monitoring of operations and transactions, aiming to identify Suspicious Operations and Transactions, FacilitaPay must systematically carry out the analysis of signs of risk considering:

- a) the possible participation (future or eventual) of Clients in restrictive lists;
- b) appearance of Clients in adverse media; and
- c) execution of any transactions and/or operations carried out by Clients in the context of prohibited sectors and/or prohibited countries.

The frequency of monitoring of the aforementioned criteria will be defined according to the level of risk assigned to the client:

- a) Low Risk Client – every 3 years;
- b) Medium Risk Client – every 2 years;
- c) High-Risk Client – annually;

In addition, FacilitaPay's responsible areas must reassess the Client's risk classification whenever, during the course of the commercial relationship, relevant indications are identified that alter their risk profile, such as:

- a) Classification as a PEP, Family and/or Close Collaborator;
- b) Presence on national and/or international sanctions lists as listed in Annex I of this Manual;
- c) Execution of activities in prohibited sectors as listed in Annex II of this Manual;
- d) Carrying out activities in prohibited countries territories with strategic deficiencies in the implementation of the FATF recommendations, as per Annex III of this Manual; and/or
- e) Involvement with relevant and adverse media, which may be related to, but not limited to, the practice of financial crimes, money laundering, terrorist financing or proliferation of weapons of mass destruction, fraud, bribery and corruption.

If the client is classified as a PEP, family member or close collaborator of a PEP, or is identified in relevant adverse media, its classification must be adjusted to "high risk", with the application of improved due diligence procedures for its qualification.

4.1.4. List of Red Flags

In addition to the procedures and criteria described above aimed at monitoring operations, transactions and situations with the potential to be characterized as suspicious, FacilitaPay establishes a series of events that, when identified, must be treated internally as "Red Flags", and therefore, automatically classified as a Suspicious Operation and Situation.

All situations described in Circular Letter No. 4,001/20 of the Central Bank of Brazil (BCB) that are identified in the institution's operations are classified as suspicious operations. However, it is important to note that not all items of said regulation apply to the activities currently carried out by FacilitaPay. Thus, the situations described in Annex IV of this Manual are considered red flags.

4.2. SELECTION AND ANALYSIS OF SUSPICIOUS TRANSACTIONS AND SITUATIONS

After issuing alerts about possible Suspicious Operations and Situations, FacilitaPay's Compliance area must manually analyze the notifications and select the

transactions, operations and/or situations that qualify as Suspicious Operations and Situations.

The deadline for selection, analysis and communication of Suspicious Operations and Situations is up to 45 (forty-five) days, counted from the date of issuance of the alert or situation detected. The analysis procedure occurs at two levels, namely:

- a) The Compliance area evaluates the Suspicious Situation or Operation and prepares the Dossier with the main information and evidence, and must give its opinion on the need to carry out the Communication to the competent bodies; and
- b) the AML/CFT Director and/or Head of Compliance who acts individually as the decision-making authority for communication to COAF.

The flow of the analysis of Suspicious Operations and Situations should occur as follows:

- a) the monitoring alert is generated through FacilitaPay's own software, or assisted by additional software contracted, and/or manually by a FacilitaPay Employee, especially those allocated in the Payment Desk, Commercial and Business areas;
 - The areas mentioned are periodically trained to identify suspicious operations and situations, both at the beginning and during the relationship with the Client.
 - Once a possible suspicious operation or situation is identified, the aforementioned areas must prepare a written report with the reasons for uncertainty, and submit it to the Compliance area.
- b) the alert is assigned to an analyst in the Compliance area, who indicates the existence of atypical behavior or if such behavior is within the usual parameters established by FacilitaPay. The analysis must include the relevant information and justifications that support the understanding about the communication, or not, of the Operation and Suspicious Situation to COAF. Subsequently, the analyst must generate a report indicating whether the alert constitutes a "false positive" or "positive", based on this Manual, Circular No. 3,978/20, the Money Laundering Law and Carta Circular No. 4,001/20;
 - if the alert is "false positive", the case must be taken to a member with greater seniority in the Compliance area for confirmation about the closure of the analysis and archiving of the demand; or
 - if the alert is "positive", the case must be documented in a specific and detailed dossier, containing the information associated with the demand in question, the conclusion of the analysis and the express indication of the reasons why the COAF must be communicated ("Dossier");

- c) the AML/CFT Officer and/or Head of Compliance must analyze the Dossier and determine whether the Suspicious Operation and Situation is subject to Communication, as well as whether there is a possible need to include additional information in the document prior to sending it to COAF.
- if the AML/CFT Officer and/or Head of Compliance understands that the Suspicious Operation and Situation should not be communicated to COAF, the latter must expressly indicate the reasons why the hypothesis is not subject to communication. Even so, the Compliance area must place the Client in continuous monitoring, for a minimum period of 6 (six) months; or
 - if the operation or situation is subject to communication to COAF, it must be carried out within a period not exceeding 24 (twenty-four) hours.
 - The AML/CFT Officer and/or Head of Compliance must take the report that motivated the communication to the regulator to Senior Management, in order to assess necessary improvements to FacilitaPay's procedures and internal controls.

4.3. REPORTING OF SUSPICIOUS TRANSACTIONS AND SITUATIONS

As indicated in the analysis flow described above, the Communication of Suspicious Operations and Situations to COAF is made by the AML/CFT Director and/or Head of Compliance within 24 (twenty-four) hours of decision-making, based on the Dossiers prepared by the Compliance area.

Communication is carried out through access to the specific portal made available by the regulatory agency (SISCOAF), observing the procedures and requirements established for this purpose.

FacilitaPay must keep a record of the Dossiers, regardless of their communication to COAF, in addition to the Communications made by the AML/CFT Officer and/or Head of Compliance. The information must be stored in specific folders within the scope of the internal systems of the Compliance area.

These Dossiers shall contain, at a minimum:

- a) name or company name of the Client;
- b) CNPJ or Tax ID, for other jurisdictions;
- c) Identification of final beneficiaries;
- d) details of the information obtained through the diligences carried out within the scope of the procedure for identifying, qualifying and classifying Customers, including verifying whether the Client or its final beneficiaries qualify as a PEP, Family Member or Close Collaborator;

- e) if it is a person who is known to have committed terrorist acts or participated/facilitated their practice;
- f) transactional summary of the Client and description and detailing of the characteristics of the operations carried out by the Client;
- g) the date of the beginning of FacilitaPay's relationship with the Client involved in the Transaction and Suspicious Situation;
- h) reasoned explanation of the warning signs of money laundering and terrorist financing risk identified; and
- i) analysts' opinion.

The decision to report a suspicious transaction or situation to COAF, taken by the AML/CFT Director and/or the Head of Compliance, must be duly substantiated by the information contained in the corresponding Dossier. Additionally, the grounds on which such a decision is based must be clearly and objectively recorded in the document itself.

Mandatorily, FacilitaPay must communicate to COAF the occurrence of operations related to payments, receipts and transfers of funds, through any instruments, against payment in cash of an amount equal to or greater than R\$50,000.00 (fifty thousand reais), pursuant to Circular No. 3,978/20.

Communications that have been made and changed or canceled after the 5th (fifth) business days following their realization will be accompanied by the justification of the occurrence.

All Communications are confidential and are restricted to the Compliance and Senior Management area. FacilitaPay undertakes not to inform any third party, including the Client, about the communication made to COAF.

If no Suspicious Transaction and Suspicious Situation is identified in the previous calendar year, FacilitaPay must send a communication to the BCB, within ten (10) business days after the end of that year, about the non-occurrence of proposals, operations and/or suspicions that can be communicated to COAF.

5. ROLES AND RESPONSIBILITIES

5.1. FacilitaPay Collaborators

- a) Carry out AML/CFT training promoted by the institution in a timely manner, keeping up to date on Operations and Suspicious Situations;
- b) Communicate to the Compliance Area about Operations and Suspicious Situations identified in the course of its activities;
- c) Maintain confidentiality of information regarding possible suspicious transactions;

5.2. Compliance Area

- a) Perform the monitoring and selection of Suspicious Operations and Situations;
- b) Evaluate the alerts received and prepare internal reports for the analysis of Suspicious Operations and Situations, giving its opinion on the need for communication to the regulatory body;
- c) Submit the reports to the responsible director for approval and communication decision.
- d) Maintain a record of the Dossiers in an internal system, regardless of their communication to COAF;

5.3. Payment Desk Area

- a) Perform the monitoring and selection of Suspicious Operations and Situations;
- b) Submit internal reports on alerts and identification of Suspicious Operations and Situations to the Compliance Area, for evaluation and possible escalation;

5.4. AML/CFT Director and/or Head of Compliance

- a) Approve or reject the internal reports prepared by the Compliance Area;
- b) Resolve on the communication of the facts narrated in the internal reports to COAF within 24 (twenty-four) hours;
- c) Communicate suspicious operations and situations to the regulatory body, whether mandatory or related to deliberation;
- d) Communicate to the BCB the non-occurrence of situations that can be reported to COAF in the last fiscal year, if applicable;
- e) Decide on the suspension or closure of accounts of Clients whose transactions are suspicious;
- f) Bring the Dossiers that can be communicated to COAF to the attention of Senior Management for evaluation of improvements in the institution's internal controls;

5.4. Senior Management

- a) To approve this Manual;
- b) Foster the culture of combating Money Laundering and Terrorist Financing;
- c) Evaluate the Dossiers presented by the AML/CFT Director and/or Head of Compliance, identifying improvements in the institution's internal controls;

6. LEGAL BASIS

- a) Law 9.613/98 (Money Laundering Law)
- b) Circular No. 3.978/20 – BCB

c) Circular Letter No. 4.001/20 – BCB

7. APPROVAL HISTORY

This Manual was duly approved by FacilitaPay's Senior Management.

Publication Date	Version	Nature of the changes	Responsible Board
19/07/2024	1.0	First publication	Ricardo Reis
15/07/2025	2.0	Changes the first version	Ricardo Reis

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

ANNEX I

ADVISORY LISTS IN THE FIELD OF CUSTOMER RISK CLASSIFICATION

- National Risk Assessment, carried out and published annually by the AML/CFT Interdepartmental Coordination Group.
- Financial Action Task Force (FATF) list: [https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc\(fatf_releasedate\)](https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)).
- Conselho de Segurança das Nações Unidas (CSNU): <https://www.un.org/securitycouncil/content/un-sc-consolidated-list>.
- World Bank: <https://www.worldbank.org/>.
- Organização Internacional de Polícia Criminal (INTERPOL): <https://www.interpol.int/How-we-work/Notices/View-Red-Notices>.
- UK Financial Conduct Authority (FCA): <https://register.fca.org.uk/s/>.
- Committee against Money Laundering, Illicit Resources and the Financing of Terrorism (MONEYVAL):

[https://ec.europa.eu/transparencyregister/public/consultation/search.do?locale=pt&reset=.](https://ec.europa.eu/transparencyregister/public/consultation/search.do?locale=pt&reset=)

- U.S. Office of Foreign Assets Control (OFAC): [https://sanctionssearch.ofac.treas.gov/.](https://sanctionssearch.ofac.treas.gov/)
- 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.](https://siscoaf.coaf.gov.br/siscoaf-internet/pages/cadastroPO/tipoPO.jsf)
- Expulsions from the federal administration (CEAF): [http://www.portaltransparencia.gov.br/download-de-dados/ceaf.](http://www.portaltransparencia.gov.br/download-de-dados/ceaf)
- Disreputable and suspicious companies (CEIS): [http://www.portaltransparencia.gov.br/sancoes/ceis?ordenarPor=nome&direcao=asc.](http://www.portaltransparencia.gov.br/sancoes/ceis?ordenarPor=nome&direcao=asc)
- Impeded for-profit entities (CEPIM): [http://www.portaltransparencia.gov.br/sancoes/cepim?ordenarPor=nome&direcao=asc.](http://www.portaltransparencia.gov.br/sancoes/cepim?ordenarPor=nome&direcao=asc)
- Empresas punidas (CNEP): [http://www.portaltransparencia.gov.br/sancoes/cnep.](http://www.portaltransparencia.gov.br/sancoes/cnep)
- 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.](http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=16002)
- Complete international lists ([Shufti Pro AML Dataset December 2023.pdf](#))

ANNEX II

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;
- Medicines (whether sold exclusively on prescription or not) or any substances that are related to the miraculous cure of any disease or health condition, including any hospital equipment;
- 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 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:

- a. 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 -
- b. 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.php/>

<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>

ANNEX IV

LIST OF OPERATIONS AND SITUATIONS THAT MAY CONSTITUTE EVIDENCE OF THE OCCURRENCE OF CRIMES OF "LAUNDERING" OR CONCEALMENT OF ASSETS, RIGHTS AND VALUES, SUBJECT TO COMMUNICATION TO COAF.

Pursuant to BCB Circular Letter No. 4,001/20, considering the scope of FacilitaPay's commercial activities, the following are considered suspicious operations and situations:

- a) Situations related to the identification and qualification of customers:
- resistance to providing information necessary for the beginning of a relationship or for updating the registration;
 - offering false information;

- provision of information that is difficult or costly to verify;
 - opening, handling of accounts or carrying out operations by a holder of power of attorney or any other type of mandate;
 - occurrence of irregularities related to the procedures for identification and registration of operations required by current regulations;
 - registration of several accounts on the same date, or in a short period, with deposits of identical or approximate amounts, or with other elements in common, such as origin of funds, holders, attorneys-in-fact, partners, address, telephone number, etc.;
 - operations in which it is not possible to identify the final beneficiary, observing the procedures defined in the current regulations;
 - representation of different legal entities or organizations by the same attorneys or legal representatives, without reasonable justification for such occurrence;
 - information of the same residential or commercial address by natural persons, without demonstration of the existence of a family or commercial relationship;
 - incompatibility of the economic activity or billing reported with the standard presented by customers with the same profile;
 - registration of the same e-mail or Internet Protocol (IP) address by different persons, natural or legal entities or organizations, without reasonable justification for such occurrence;
 - information and documents submitted by the client that conflict with the publicly available information;
 - partners of companies without apparent financial capacity for the size of the declared business activity;
- b) Situations related to persons or entities suspected of involvement in terrorist financing and the proliferation of weapons of mass destruction:
- financial transactions involving persons or entities related to terrorist activities listed by the United Nations Security Council (UNSC);
 - transactions or provision of services, of any value, to persons or entities known to have committed or attempted to commit terrorist acts, or participated in or facilitated the commission thereof;
 - the existence of resources owned or controlled, directly or indirectly, by persons or entities known to have committed or attempted to commit terrorist acts, or participated in or facilitated the commission thereof;
 - movements with indications of terrorist financing;
 - financial transactions involving persons or entities related to the proliferation of weapons of mass destruction listed by the UNSC;
 - operations or provision of services, of any value, to persons or entities that have known to have committed or attempted to commit crimes of proliferation of weapons of mass destruction, or participated in or facilitated the commission thereof;

- the existence of resources owned or controlled, directly or indirectly, by persons or entities that have known to have committed or attempted to commit crimes of proliferation of weapons of mass destruction, or participated in or facilitated the commission thereof;
 - movements with indications of financing the proliferation of weapons of mass destruction;
- c) Situations related to international activities:
- transactions with individuals or legal entities, including companies and financial institutions, located in countries that do not apply or insufficiently apply the recommendations of the Action Group against Money Laundering and Terrorist Financing (FATF), or that are headquartered in countries or dependencies with favorable taxation or privileged tax regimes, or in places where the persistent practice of the crimes provided for in Law No. 9,613 is observed, of March 3, 1998, not clearly characterized in their legality and economic basis;
 - complex operations with higher costs that aim to make it difficult to trace resources or identify the nature of the operation;
 - payments to third parties not related to import or export operations;
 - unilateral transfers that, due to their habituality, value or form, are not justified or present atypicality;
 - international transfers, including as availability abroad, in which the origin of the funds involved is not justified or which are incompatible with the financial capacity or profile of the client;
 - apparently fictitious exports or imports or with indications of overpricing or under-invoicing, or even in situations where it is not possible to obtain information about the customs clearance of the goods;
 - existence of information in the letter of credit with discrepancies in relation to other documents of the international trade operation;
 - payments abroad after credits in reais made in the deposit accounts of the holders of exchange operations by individuals or legal entities that do not demonstrate the existence of a commercial or economic link;
 - movements resulting from a program for the repatriation of funds that present inconsistencies related to the identification of the holder or final beneficiary, as well as the absence of reliable information on the origin and economic or legal basis;
 - payments for freight or other services that present indications of atypicality or incompatibility with the activity or economic and financial capacity of the customer;
 - international transfers by one or more individuals or legal entities with signs of fragmentation, as a way of hiding the real origin or destination of the resources;
 - transactions on the same date, or in a short period, of identical or approximate amounts, or with other elements in common, such as origin or destination of

- funds, holders, attorneys-in-fact, address, telephone number, which constitute an artifice to circumvent the maximum operating limit;
- transfer via payment facilitator or with the use of a credit card for international use, which, due to their habituality, value or form, are not justified or atypical;
 - transfers related to non-conventional investments that, due to their habituality, value or form, are not justified or present atypicality;
 - payment of international freight without support in documentation that evidences a link with a commercial operation;
- d) Situations related to employees, partners and third-party service providers:
- unusual change in the living standards and behavior of the employee, partner or outsourced service provider, without apparent cause;
 - unusual modification of the operating result of the partner's legal entity, including a corresponding one in the country, without apparent cause;
 - any business carried out in a manner different from the formal procedure of the institution by an employee, partner, including correspondent in the country, or outsourced service provider;
 - providing assistance or information, paid or unpaid, to a client to the detriment of the institution's money laundering and terrorist financing prevention program, or assistance in structuring or fractioning operations, circumventing regulatory or operational limits;
- e) situations related to the operation of current accounts in foreign currency (CCME):
- movement of resources incompatible with the economic activity and financial capacity of the client;
 - receipts or payments from/to third parties whose financial transactions do not have economic or legal basis or in which there appears to be no link between the declared activity of the CCME holder and the other parties involved in the transactions;
 - movement of funds, especially in accounts held by agents authorized to operate in the foreign exchange market, which denote non-compliance with limits due to foreign exchange operation or any other situation in which they are not justified or present atypicality, due to habituality, value, form or lack of adherence to foreign exchange rules;
 - atypical transactions in restricted movement CCMEs. Examples: travel agency accounts and credit card company accounts;
- f) Situations related to operations carried out in municipalities located in risk regions:
- atypical operation in municipalities located in border regions;
 - atypical operation in municipalities located in mineral extraction regions;
 - Atypical operation in municipalities located in other risk regions.