INSTITUTIONAL POLICY

OF PREVENTION AND COMBAT TO

MONEY LAUNDERING AND FINANCING OF TERRORISM

Rua Bispo Dom José, 2095 | 6th floor, District of Batel | Curitiba/PR | ZIP CODE 80.440-080 +55 (41) 3123-0100 +55 (41) 3123-0123 | CNPJ No. 19.307.785/0001-78

Summary

Version History

1st Version – Original Version - Prepared by the President of Braza bank, approved on 06/14/2015.

2nd Version – 1st Amendment – Periodic update, approved on 10/31/2017.

3rd Version – 2nd Amendment - Periodic update, approved on 09/28/2020.

4th Version – Inclusion of the list of prohibited countries and checking procedures in sanctions lists, approved on 06/15/2021.

5th Version – Inclusion of guidelines for internal risk assessment, New products, services and technologies, Hiring of employees and service providers and Monitoring and Control Mechanisms, approved on 08/24/2021.

6th Version – Update considering the provisions of BCB Resolutions 277, 278, 279, 280, 281 and 282, approved on 01/02/2023.

7th Version - Periodic update, including details of communication on UNSC sanctions and adequacy of responsibilities, approved on 04/01/2023.

8th Version – Change of the bank's corporate name to Braza bank S.A. Banco de Câmbio, considering the approval by the competent regulatory bodies, approved on 04/04/2023.

Normative Basis

This document includes, among others, guidelines on the Prevention of Money Laundering Crimes, Financing of Terrorism, Combating Corruption, Fraud and other Financial Malpractice. In this sense, the legal basis for implementing and implementing this institutional policy as well as its procedures is based, but not restricted, to the following laws/regulations:

- Act no. 9.613, of 03/03/1998.
- Act No 10.467, of 6/11/2002.
- Act No 12.683, of 7/9/2012.
- Act No 12.846, of 8/1/2013.
- Act No 13.260, of 3/16/2016.
- Act No 13.810, of 3/8/2019.
- Act No 14.286, of 12/31/2021.
- CMN Resolution No 3.426, dated 12/22/2006.
- COAF Resolution No. 31, dated 06/07/2019.
- CMN Resolution No 4.595, dated 08/28/2017.
- BCB Newsletter No. 3.978, dated 01/23/2020.
- BCB Resolution No 44, dated 11/23/2020.
- BCB Resolutions No. 277, 278, 279, 280, 281 and 282, dated 12/31/2022.
- BCB Newsletter No. 4.001, of 01/29/2020.
- Forty Recommendations of the GAFI (Financial Action Group), created in 1991, instituted in Brazil by the RFB Normative no. 1.571 of 07/02/2015.

- Nine Special GAFI Recommendations on Financing to Terrorism, created in 10/2001 - instituted in Brazil by the RFB Normative no. 1.571 of 07/02/2015.

Introduction

What is Money Laundering?

According to the provision of Law No. 9.613, of March 3, 1998, with wording amended by Law No. 12.683, of July 9, 2012:

“Article 1 Conceal or disguise the nature, origin, location, disposition, movement or property of assets, rights or values resulting directly or indirectly from a criminal infraction.”

Money laundering schemes can be very simple or highly sophisticated. Most of the more complex processes involve three phases:

Placement - placement of money in the economic system, which can be done through deposits, purchase of negotiable instruments, offshore companies or purchase of goods. Here, the fractioning of values is very common, as well as the use of commercial establishments that normally work with cash.

Concealment - consists of making it difficult to trace illicit resources in the accounts, aiming at breaking the chain of evidence to make it difficult to trace the origin of funds.

Integration - when assets are formally incorporated into the economic system, often in ventures that facilitate the activities of criminal organizations (even among them). Once the chain is formed, it becomes easier to legitimize illegal money.

What is Terrorism Financing?

According to the provision of Law No. 13.260, of March 16, 2016 (“Anti-terrorism Act”):

“Article 2 Terrorism consists in the practice by one or more individuals of the acts provided for in this article, for reasons of xenophobia, discrimination or prejudice of race, color, ethnicity and religion, when committed with the purpose of causing social or generalized terror, exposing the danger person, property, public peace or public safety. "

Terrorist acts can be considered:

- Use or threaten, transport, store, carry or carry explosives, toxic gases, poisons, biological, chemical, nuclear or other means capable of causing damage or promoting mass destruction;
- To sabotage the operation or to take, with violence, a serious threat to the person or using cyber mechanisms, of total or partial control, even if temporarily, of means of communication or transportation, of ports, airports, railway stations or road stations, hospitals, nursing homes, schools, sports stadiums, public facilities or places where essential public services operate, power generation or transmission facilities, military facilities, oil and gas exploration, refining and processing facilities and banking institutions and its service network;
- Attempting the life or physical integrity of a person;
- Promote, constitute, integrate or provide assistance, personally or through an intermediary, to the terrorist organization;
- Carry out preparatory acts of terrorism with the unequivocal purpose of carrying out such a crime;

- Offering or receiving, obtaining, keeping, keeping in deposit, requesting, investing or in any way contributing to obtaining an asset, asset or financial resource, with the purpose of financing, in whole or in part, a person, group of people, association, entity, criminal organization whose main or secondary activity, even on an occasional basis.

Policy: Purposes, Establishment, Management and Target Audience

The purpose of this document is to inform all employees, national and international banking partners, foreign exchange correspondents, employees and relevant service providers regarding the Institutional Policy for Preventing Money Laundering and Combating the Financing of Terrorism ("PLDFT") that Braza bank has adopted and adheres to its daily operations.

Our basic principles are:

- Braza bank keeps its Institutional Policy for Preventing and Combating Money Laundering and Terrorism Financing up to date and in writing, as well as for combating Corruption. This policy is to be compatible with the "nature, size, complexity, structure, risk profile and business model" from the bank.
- Braza bank complies with the laws and regulations applicable to the Prevention and Combating of Money Laundering and the Financing of Terrorism, as established by local and international regulatory bodies.
- The Braza bank's Board is committed to the dissemination of its preventive organizational culture, at all levels and to third parties, when appropriate. The organizational culture of Braza bank aims to protect the institution's reputation and

image through the application, implementation, evaluation and improvement of the principles established in this document.

This Institutional Policy applies to all employees, direct or indirect at all levels, branches (if any), banking and/or foreign exchange correspondents, partners and service providers of Braza bank, receiving extensive internal disclosure.

Term and Periodicity of Review

This document comes into force on the date of its approval and will be revised every two (02) years or whenever there are significant changes in current laws or regulations, as well as significant changes in the risk profile of the institution's clients and businesses. The revisions and amendments will be approved by the Executive Board of Braza bank in Minutes, which will be available for consultation by regulatory/supervising bodies, as well as internal and external auditors, for a minimum period of five (5) years.

Governance and Responsibilities

It is the responsibility of all employees and collaborators (at all levels), branches (if any), banking and/or foreign exchange correspondents, service providers and partners to conduct their daily activities with honesty, ethics and integrity, being expressly prohibited the involvement or facilitation, in any way, in any suspicious or illegal activity that may result in money laundering and terrorist financing crimes.

The entire organizational structure of Braza bank has specific duties on PLDFT:

Executive Board

- Appoint the director responsible for the implementation and compliance with Law No. 9613/1988 and Newsletter No. 3978/2020, according to the provisions of its Chapter III;
- Review and approve the rules and guidelines for the process of preventing and combating money laundering and financing of terrorism - “Institutional Policy to Prevent and Combat Money Laundering and Financing of Terrorism”, as well as their subsequent changes;
- Promote the dissemination and adherence of the Institutional Policy for Preventing and Combating Money Laundering and the Terrorism Financing throughout the organizational structure of Braza bank.
- Review and approve the guidelines of “Know Your Customer”, “Know Your Employee/Collaborator”, “Know Your Partner/Service Provider”, “Procedures for Monitoring, Selection, Analysis and Reporting of Suspicious Transactions” and “Assessment of Effectiveness of PLDFT Policy” as well as its action plan;
- Be aware of the Institution’s “Internal Risk Assessment”, as well as its action plan and respective follow-up report;
- Ensure that the PLDFT Director has sufficient independence, autonomy and technical knowledge to fully perform his/her duties, as well as full access to all the information deemed necessary for the respective PLDFT risk governance to be carried out; and
- Provide a qualified organizational structure, as well as guarantee adequate and sufficient resources to carry out activities related to the PLDFT with efficiency and quality.

Director responsible for PLDFT

- Respond to Bacen for the implementation and compliance with this Policy, as well as for the necessary communications to Organs competent bodies;
- Ensure that the Institutional Policy for Preventing and Combating Money Laundering and the Financing of Terrorism is in compliance with applicable laws and regulations;
- Be accountable for the proper Governance of this Policy;
- Appreciate the reports and communications issued by Organs regulatory and self-regulatory bodies, the internal audit and the external audit, determining the actions and measures necessary to meet the demands;
- Comply with the determinations of Organs regulatory bodies to act in the PLDFT;
- Document and approve the Internal Risk Assessment and its due referral to the Executive;
- Provide information about contracts with financial institutions headquartered abroad;
- Provide information on the execution of contracts with third parties not subject to authorization to operate by Bacen, participants of a payment arrangement in which Braza bank also participates;
- Follow-up the updating of internal manuals and procedures that ensure adherence to this Policy;
- Implement the money laundering prevention program at Braza bank (systems, processes, procedures and training);
- Resolve on the hiring of specialized professional services and investments in control systems and technology, in PLDFT, when necessary;

- Determine the immediate unavailability of assets of natural or legal persons whose ownership, directly or indirectly, is included in the United Nations Security Council sanctions lists, as well as also arrange for the immediate communication of such unavailability to the Department of Asset Recovery and International Legal Cooperation of the National Secretariat of Justice of the Ministry of Justice and Public Security, to the Central Bank of Brazil, through the BC Correio system and to COAF, pursuant to the provisions of article 9 of Law 9613/1998, and
- Receive, analyze and decide on the formal communication to COAF of situation reports regarding suspected money laundering or terrorist financing.

Director Responsible for Risks

- Identify, evaluate, monitor the credit, market, operational, liquidity, social, environmental, climate and other risks and, if atypical situations are identified, report to the PLDFT Board or PLDFT Management;
- Receive and document internal communications about situations that may be classified as evidence of PLDFT from all employees in your area and forward them for evaluation by the Management or Board of PLDFT;
- Determine the immediate unavailability of assets of natural or legal persons whose ownership, directly or indirectly, is included in the United Nations Security Council sanctions lists, as well as also arrange for the immediate communication of such unavailability to the Department of Asset Recovery and International Legal Cooperation of the National Secretariat of Justice of the Ministry of Justice and Public Security, to the Central Bank of Brazil, through the BC Correio system and to COAF, pursuant to the provisions of article 9 of Law 9613/1998, and
- Contribute to the analysis of new products, services, or technologies.

Director Responsible for Foreign Exchange Transactions

- Comply with the determinations contained in Chapter VI, of Newsletter 3978/2020, for the registration of operations carried out, products and services contracted, including withdrawals, deposits, contributions, payments, receipts, transfers of funds and operations in the foreign exchange market, including if the operation occurs within the same institution,
- Receive and document internal communications about situations that may be classified as evidence of PLDFT from all employees in your area and forward them for evaluation by the Management or Board of PLDFT;
- Determine the immediate unavailability of assets of natural or legal persons whose ownership, directly or indirectly, is included in the United Nations Security Council sanctions lists, as well as also arrange for the immediate communication of such unavailability to the Department of Asset Recovery and International Legal Cooperation of the National Secretariat of Justice of the Ministry of Justice and Public Security, to the Central Bank of Brazil, through the BC Correio system and to COAF, pursuant to the provisions of article 9 of Law 9613/1998, and
- Contribute to the analysis of new products, services, or technologies.

PLDFT Management

- Monitor the activities of the PLDFT areas in order to ensure that all demands, if they are met within the established deadlines by providing the team with the necessary resources to carry out their work;
- Assess the team's knowledge of the rules to be followed and activities to be performed and, when necessary, provide the necessary training.

- Act and monitor the implementation of the action plans presented to meet legal requirements and improve internal processes.
- Forward to the PLDFT Board relevant issues that require changes or improvements in processes of which solution depends on greater authority;
- Review and, when necessary, update manuals and submit proposals to change internal policies so that they are in compliance with the legislation, rules, regulations, and internal policies that govern the prevention and fight against money laundering and financing of terrorism;
- Develop and implement tools and processes to support strategies for the corporate program to prevent money laundering and financing of terrorism;
- Plan and ensure compliance with periodic training programs for employees and, when applicable, foreign exchange correspondents.
- Meet and monitor internal and external audits and inspections related to PLDFT area, according to the proposed;
- Submit proposals to the PLDFT Board for adoption or changes in policies applicable to the topic;
- Receive, analyze and decide on the formal communication to COAF of situation reports regarding suspected money laundering or terrorist financing;
- Determine the immediate unavailability of assets of natural or legal persons whose ownership, directly or indirectly, is included in the United Nations Security Council sanctions lists, as well as also arrange for the immediate communication of such unavailability to the Department of Asset Recovery and International Legal Cooperation of the National Secretariat of Justice of the Ministry of Justice and Public

Security, to the Central Bank of Brazil, through the BC Correio system and to COAF, pursuant to the provisions of article 9 of Law 9613/1998, and

- Evaluate the interest in initiating or maintaining relationships with customers who qualify as a politically exposed person, when necessary.

Customer Registration Area

- Comply with what is described in the internal procedures regarding the "Know Your Customer" process, as well as the provisions of the procedures for identifying, maintaining and updating customer records;
- Communicate to the General Supervisor of the area if any Conflict of Interest is identified, in order to ensure that the employee performs his duties independently
- Communicate immediately to the General Supervisor of the area when and if there is any client or potential client included in the resolutions of the United Nations Security Council, so that this Supervisor immediately reports to the PLDFT Board, Risk Board, Foreign Exchange Operations Board or to the PLDFT Management, for the immediate unavailability of assets and the due communications, provided for in current regulations;
- Communicate to the General Supervisor of the area when identified the reluctance to provide required information or any unusual information that is verified in the "know your customer" process, as evidence of document fraud;
- Define specific procedures for obtaining registration data and documents, when and if necessary, with a view to identifying, verifying, validating, qualifying and classifying the client, as well as ensuring regulatory compliance, and

- Prepare report suggestions if and when situations are identified that may be classified as evidence of PLDFT and forward them to the General Supervisor of the area, who will forward them to the PLDFT Management or Board.

Analysis Area and Foreign Exchange Operations Registration (BackOffice)

- Communicate to the General Supervisor of the area if any Conflict of Interest is identified, in order to ensure that the employee performs his duties independently;
- Communicate immediately to the Supervisor of the area when and if there is any client or potential client listed in the resolutions of the United Nations Security Council;
- Communicate immediately to the Supervisor of the area when and if there is any client or potential client contained in the resolutions of the United Nations Security Council, so that the Supervisor immediately reports to the PLDFT Board, Risk Board, the Foreign Exchange Operations Board or the Management of PLDFT, for the immediate unavailability of assets and the due communications, provided for in current regulations;
- Assess whether the operations are in accordance with the operational modality and technical qualification of the customer;
- Define specific procedures, with the purpose of observing the correct classification of the operations, considering the economic rationale and the document support presented, when and if necessary;
- Prepare report suggestions if and when situations are identified that may be classified as evidence of PLDFT and forward them to the General Supervisor of the area, who will forward them to the PLDFT Management, and

- Define a procedure for the maintenance of operation dossiers based on documents that prove their legality, if and when required.

Monitoring, Selection, Analysis Area and Reporting Suspicious Transactions (MSAC)

- Monitor the operations carried out by customers, especially those with higher risks, according to internal methodology;
- Observe whether the criteria necessary to guarantee the legality of the operations are being followed;
- Inform the Director responsible for PLDFT if any Conflicts of Interest are identified, in order to ensure that the analyst performs his duties independently;
- Communicate immediately to the Supervisor of the area when and if there is any client or potential client contained in the resolutions of the United Nations Security Council, so that the Supervisor immediately reports to the PLDFT Board, Risk Board, the Foreign Exchange Operations Board or the Management of PLDFT, for the immediate unavailability of assets and the due communications, provided for in current regulations;
- Preparation and application of consistency tests and adherence to internal policies;
- Write reports with suggestions for communications to COAF regarding the identification of evidence of money laundering, financing of terrorism or other financial offenses, as well as the maintenance of due files and forward these reports to the Management or Board responsible for PLDFT;
- Ensure compliance with this policy by conducting tests of controls, at least annually.

Business Areas and Products

- Being Braza bank's first line of defense, the relationship managers or their equivalents are responsible for direct customer relationships and transactions carried out by customers, mainly in relation to the assessment of risks related to PLDFT crimes;
- Follow the best practices regarding the "Know Your Customer" process, especially in the search of new customers, registration renewal, intermediation of foreign exchange operations, safeguarding supporting documents, when and if required;
- Communicate if and when situations are identified that may be classified as evidence of PLDFT and forward them to the General Supervisor of the area, who will forward them to the Management or Board of PLDFT, and
- Communicate immediately to the Supervisor of the area when and if there is any client or potential client contained in the resolutions of the United Nations Security Council, so that the Supervisor immediately reports to the PLDFT Board, Risk Board, the Foreign Exchange Operations Board or the Management of PLDFT, for the immediate unavailability of assets and the due communications, provided for in current regulations;
- Ensure that all foreign exchange correspondents are properly oriented and updated regarding their obligations and responsibilities under the regulation;
- Inform about the creation of new products, services or technologies to the areas of PLDFT, Risk Management, Compliance and Internal Controls for prior assessment of PLDFT risks and impact on the Internal Risk Assessment.

Foreign Exchange Correspondents

- Also being part of the first line of defense, they are responsible for the relationships and transactions prospected with customers, especially in relation to the initial assessment of risks related to PLDFT crimes;
- Follow the best practices regarding the “Know your Customer” process, especially in attracting and contacting customers, informing Braza bank Compliance about suspicious activities;
- Maintain controls to ensure that all its employees are trained in accordance with the training policy in force at Braza bank;
- Collect, verify and confirm the legitimacy of documents and customer registration information, in accordance with the established in the internal procedures manuals of Braza bank;
- Collect, verify and confirm the legitimacy of documents and information related to proposals for foreign exchange transactions, in accordance with the established in the internal procedures manuals of Braza bank;
- Report immediately to the Management or Board of the PLDFT team at Braza bank, when any evidence of money laundering or fraud in the financial system is found, such as proposals made or changes without apparent motivation to the “modus operandi” of customers.

Internal Audit

- Conduct tests of controls to monitor and ensure the implementation and adequacy of the PLDFT Policy;

Conduct control tests to monitor and ensure the implementation and adequacy of procedures and internal controls indicated in the Newsletter 3978/2020.

Other Areas

- Ensure the compliance with this Policy and immediately report to the supervisor or equivalent any irregularities or atypicalities in the process;
- Prepare report suggestions if and when situations are identified that may be classified as evidence of PLDFT and forward them to the General Supervisor of the area, who will forward them to the PLDFT Management;
- Communicate immediately to the Supervisor of the area when and if there is any client or potential client contained in the resolutions of the United Nations Security Council, so that the Supervisor immediately reports to the PLDFT Board, Risk Board, the Foreign Exchange Operations Board or the Management of PLDFT, for the immediate unavailability of assets and the due communications, provided for in current regulations, and
- Attend the PLDFT trainings, which are mandatory.

Internal Risk Assessment (“IRA”)

The internal risk assessment aims to identify, analyze, measure, mitigate and monitor the risk of using its products and services, as well as the use of new technologies in the practice of money laundering and the financing of terrorism to which Braza bank is exposed to. The risk-based approach will be stipulated by checking categories and variables. This action ensures that the measures taken to prevent or mitigate money laundering and terrorist financing are proportionate to the risks identified in the process of accepting, monitoring and maintaining the relationship.

In this assessment, risk categories must be defined that allow the adoption of reinforced management and mitigation controls for situations of greater risk and the adoption of simplified controls in situations of lower risk.

The risks identified must be at least evaluated in terms of its probability of occurrence and the magnitude of the financial, legal, reputational and socio-environmental impacts for the Braza bank, within the profiles:

- Of customers;
- Of institution, including the business model and geographic area of operation;
- Of operations, transactions, products and services, covering all distribution channels and the use of new technologies; and
- Of activities performed by employees, partners and outsourced service providers.

The risk categories determine mitigating actions and controls for the mapped risks.

The IRA should be reviewed every two (02) years or when substantial changes occur in the risk profiles raised by the Institution.

New Products, Services and Technologies

Prior to the development of new products and services, as well as the decision to use new technologies, the possible risks arising from money laundering and financing of terrorism and its impacts must be assessed, among other aspects.

The participation of the PLDFT Board is mandatory in this process and its evaluation must consider, at least, compliance with legality, responsibility, identification of parties and economic basis of operations linked to new products, services or technologies, according to their nature, size, complexity, structure, risk profile and business model.

Training

Braza bank will periodically and properly train its employees and foreign exchange correspondents. The training can be in person or electronic ("online") and the person responsible for the area that received the training will keep a file with a history of individual tests applied (when applicable), as well as the training content and any certificates of participation, which will be maintained by the Braza bank for consultations with regulatory/supervisory bodies or auditors whenever necessary. The training agenda will be defined by those responsible for each demanding area and will have the necessary resources to achieve the desired results.

Evaluation of PLDFT Policy Effectiveness

The PLDFT Area will assess, on an annual basis, the effectiveness of this policy, procedures and internal controls of PLDFT and will be document in a specific report with a base date of December 31, sent to the Board for information by March 31 of the following year.

Based on this evaluation, an action plan must be prepared to solve eventual deficiencies identified, and its follow-up will be documented in a specific report, sent to the Board of Directors for acknowledgment and evaluation by June 30th of the following year.

The evaluation must contemplate the guidelines, procedures, and internal controls described in this Policy and in the other manuals referenced herein, related to the issues:

- Know your Customer Procedures, including the verification, validation and qualification of customer information and the adequacy of registration data;
- Procedure for monitoring, selection, analysis and reporting to COAF, including the assessment of the effectiveness of the parameters for selecting transactions and suspicious situations;

- Governance of this policy;
- Organizational culture development measures aimed at preventing money laundering and financing of terrorism;
- Training program for employees and foreign exchange correspondents;
- Know Your Employee and Know Your Partner/Service Provider Procedure, and
- Follow up of the notes of the Internal Audit and the supervision of Bacen.

It should also be considered:

- Result of the work carried out by the internal audit;
- Result of registration validation tests;
- Notes made by the supervision of the Central Bank, and
- The probability of occurrence and the magnitude of the impact, according to internal assessment, to determine the necessary levels of control and mitigation of risks.

Follow-Up and Control Mechanisms

The PLDFT area, together with the Compliance and Internal Controls area, must implement and maintain follow-up and control mechanisms that ensure compliance with the provisions of this Policy, Braza bank's internal Manuals and Procedures.

These mechanisms must include:

- The definition of processes, tests, and audit trails;
- The definition of appropriate metrics and indicators, and

- The identification and correction of eventual deficiencies.

These mechanisms themselves must be subject to periodic tests carried out by Internal Audit.

Know Your Customer ("KYC")

"Know your customer" refers to a set of actions that establish mechanisms to ensure due diligence in the identification, verification, qualification and classification of customers, also including specific procedures for identification of Final Beneficiaries and Politically Exposed Persons, carried out in line with the Internal Risk Assessment.

Politically Exposed Persons (PEP): Politically exposed persons are considered to be public agents who play or have played in the last five (5) years, in Brazil or in foreign countries, territories and dependencies, positions, jobs or relevant public functions, as well as their representatives, family members, close collaborators and others close to them.

Final Beneficiary: It is the person who ultimately, directly or indirectly, owns, controls or significantly influences a legal entity. It is also considered final beneficiary the representative, attorney-in-fact or agent, who actually exercises command over the activities of the legal entity.

Know Your Employee/Contributor ("KYE")

"Know Your Employee/Employee" is a set of rules, procedures and controls that must be adopted for selecting and monitoring the economic and financial situation and suitability of employees/contributir, in order to avoid links with people involved in illegal acts.

Know Your Partner/Service Provider ("KYP")

Know your Partner/Service Provider refers to a set of rules and procedures that must be adopted to identify and accept partners (Service Providers/Foreign Exchange Correspondent), preventing the hiring of unreliable companies or suspected of involvement in unlawful activities. For those who represent a higher risk, complementary procedures and in-depth assessment procedures and specific approval levels must be adopted, according to the criticality of the notes or exceptions.

Monitoring, Selection, Analysis and Reporting of Suspicious Transactions ("MSAC")

Monitoring, Selection, Analysis and Reporting of Suspicious Operations ("MSAC") is about the procedures and mechanisms that Braza bank uses to monitor, select, analyze and report atypical activities and evidence of money laundering and Financing of Terrorism. Operations, situations, or proposals with indications of money laundering or financing of terrorism must be communicated to the competent regulatory bodies, when applicable, in compliance with legal and regulatory provisions. Information about communications is restricted, not disclosed to persons involved or third parties.

Communications to COAF

Operations or situations suspected of money laundering and terrorist financing or any other situations with indications of illicit activities are communicated to COAF. The decision to report the operation or situation to COAF is based on the following:

Based on the information contained in the dossier prepared by the MSAC area;

- Be systematically recorded in a detailed manner.

- Occur until the end of the analysis period of forty-five (45) days, counted from the date of the selection of the operation or situation.

They will be specified when applicable if the person object of the communication is:

- Politically exposed person or representative, family member or close collaborator of that person.
- Person who, admittedly, has committed or has attempted to commit terrorist acts or participated in or facilitated their commitment, and
- Person who owns or controls, directly or indirectly, resources in the institution (final beneficiary).

Reporting the suspicious operation or situation to COAF is carried out until the business day following that of the communication decision, being justified according to the analysis dossier defined by the communication decision and is totally confidential, without informing those involved or the the third parties. Communications changed or canceled after the fifth business day following that of their realization must be accompanied by a justification for the occurrence.

If there is no communication to COAF in the calendar year, Braza bank will provide a statement attesting to the non-occurrence of operations or situations subject to communication, within ten (10) business days after the end of that year.

Braza bank is duly qualified in SISCOAF, and the records of unusual and/or suspicious activities are registered by employees in the MSAC area whose access to said system was authorized by the PLDFT Board, after approval of such communications by the PLDFT Board and/or Management.

National and International Restrictive Lists (“Sanction Lists”)

Economic sanctions are a significant part of the global fight against financial crime and are used by governments around the world to restrict or prohibit trade with foreign persons or entities that are involved or suspected of being involved in illegal activities.

Sanctions Lists can include individuals, organizations, or entire countries involved in the criminal financing of activities such as:

- Terrorism and Financing of Terrorism;
- Money Laundry;
- Violation of Human Rights;
- Proliferation of weapons of mass destruction, among others.

The main international sanctions lists used by Braza bank are:

- Sanctions applied by the United Nations Security Council ("UNSC");
- Sanctions applied by the US Office of Foreign Assets Control ("OFAC");
- Sanctions applied by the Europe Union ("EU Sanctions"), and
- Sanctions applied by the United Kingdom ("HM Treasury").

Checks on these sanctions lists are made, but not limited, to the following occasions:

- In the initial registration of the client and all subsequent updates;
- In the process of continuous monitoring of registration and operations, including counterparties, and
- In a timely manner, in each event involving requests to transfer funds from clients and their counterparties, whether in national currency or foreign currency.

The aforementioned checks, and the respective timely unavailability of assets, when necessary, occur in all products offered by Braza bank, whether in the movement of values entering the country, or in the movement of values out of the country.

United Nations Security Council ("UNSC")

Braza bank, complying with the provisions of Law 13810/2019, immediately makes unavailable assets of individuals or legal entities whose ownership, directly or indirectly, appears on the UNSC sanctions lists. In addition, when blocking assets, Braza bank immediately communicates this action to the Department of Asset Recovery and International Legal Cooperation of the National Secretariat of Justice of the Ministry of Justice and Public Security, to the Central Bank of Brazil, through the system BC Correio (specifically for the "Deati/CSNU" folder) and COAF, as provided for in Article 9 of Law 9613/1998.

All employees, direct or indirect at all levels who have knowledge or suspicion of an act that is not compatible with the provisions of this Policy, in particular any direct or indirect link of individuals or legal entities that appear on the UNSC sanctions list, must report immediately to the Supervision of their area, which in turn must report in a timely and direct manner to the Management or to the PLDFT Board for immediate measures of unavailability of assets and their communication, under the terms of current regulations.

Braza bank is duly qualified in SISCOAF, and records of atypical and/or suspicious activities are recorded by employees in the MSAC area whose access to said system was authorized by the PLDFT Board.

Communication via BC Correio and the Ministry of Justice and Public Security is carried out by any member of the Statutory Board of Braza bank, with powers to answer for the Institution before these bodies.

Maintenance of Information and Records

The following documents must be kept for at least ten (10) years:

- Information and documents intended to know your customer;
- Information and documents intended to know employees/collaborators, partners (service providers and foreign exchange correspondents);
- Information about the registration of payment, receipt and transfer operations of funds (own or third party's), and
- Procedures for analysis of suspicious operations and situations.

Confidentiality of Information

All information related to evidence/suspicion of money laundering and combating the financing of terrorism is confidential, and under no circumstances should the parties involved be made available. Communications of suspicious cases dealing with Newsletter 4001/2020 are for the exclusive use of Regulatory Bodies for analysis and investigation.

Exceptions and Penalties Applicable

For cases of exception to compliance with the rules provided in this Policy, the applicant must submit an exception request to the PLDFT Board, or in the lack thereof, to the PLDFT Management, clearly explaining the reasons underlying it, and approval of the request must be made in writing by the PLDFT Director or Manager.

Expected Sanctions

Non-compliance with legal and regulatory provisions, subject to employees, partners and corresponding to sanctions ranging from administrative to criminal penalties, for Money Laundering, Financing of Terrorism. Negligence and voluntary failure are considered noncompliance with this Policy and the Code of Ethics and Conduct, subject to the application of disciplinary measures provided for in internal regulations.