Prevention of Money Laundering and Financing of Terrorism Policy

Circular Nº 3.978 from BACEN, of January 23, 2020, and CVM Resolution 50, of August 31, 2021.

The present policy of Anti Money Laundering, Countering the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction was developed aiming to formalize the established guidelines with the purpose of mitigating the risks of operations that configure signs of money laundering, thus preventing the utilization of BOCOM BBM for purposes of activities related to the crimes provided for in Law Number 9.613 of March 3, 1998 ("Law 9.613") and in Law Number 13.260 of March 16, 2016 ("Law 13.260") ("Policy" and "AML/CFT", respectively).

1. Concepts relevant to this Policy:

1.1. What is Money Laundering?

Money laundering is the concealment or dissimulation of the nature, origin, location, disposal, movement, transaction or ownership of goods, rights or values coming, directly or indirectly, from criminal violation under terms of Article 1 of Law 9.613/98, c/w Law 12.683/12.

The money laundering process can be broken down into three stages:

- Placement – The first stage of the process is the placement of the money within the economic system. Aiming to conceal its origin, the criminal attempts to move the money in countries with more permissive rules and those having a liberal financial system. Such placement occurs by means of deposits, purchase of negotiable instruments or purchase of goods. In order to make difficult the identification of the money origin, the criminals apply sophisticated techniques and increasingly more dynamical, such as fractioning of the amounts moving through the financial system and utilization of commercial establishments that usually work with cash.
- Concealment – The second stage of the process consists in making difficult the accounting tracking of illegal funds. The purpose is to break the chain of evidence before the possibility of conduct of investigations on the origin of the money. Criminals attempt to move it in electronic form, by transferring the assets to anonymous accounts – preferably in countries

supported by bank secrecy laws – or making deposits in accounts opened in the name of "stooges" or using fake or shell companies.

- Integration – In this last stage, the assets are formally incorporated to the economic system. The criminal organizations seek to invest in concerns that facilitate their activities – such companies being able to provide services between one another; once the chain is formed, it becomes increasingly easier to legitimate the illegal money.

In order to disguise the illegal profits without compromising those involved, the money laundering is made by means of a dynamic process requiring: first, the distancing of the funds from their origin, thus avoiding a direct association thereof with crime; second, the disguise of their different transactions to avoid tracking of such funds; and third, the provision or availability of the money again to the criminals after having been sufficiently moved around in the laundering cycle and can be considered "clean".

1.1.1. Tactics used by criminal organizations:

The tactics used by "money launderers" are several comprising different sectors such as:

- Financial System – This is one of the most targeted sectors by criminal organizations that conduct money laundering operations. The new Technologies and the globalization of financial services favor the fast circulation of the money in complex transactions so that the "dirty" money is mixed with legally moved amounts.
- Real State Market – By means of transactions of purchase and sale of real estate and false real estate speculations, which consist in the acquisition of major valued assets with declaration of purchase for a much lower value to the market and the consequent sale of such assets at market value. This activity allows the criminals "to warm up" the money.
- Tax Havens and Offshore Centers – Both tax havens and offshore centers share a legitimate purpose and are commercially justifiable. However, in the last years we have seen a large occurrence of money-laundering crimes in this sector, bearing mind the facilities offered thereby. Attentive to the particulars of the financial legislation of each country, criminal groups internalize resources in countries with more permissive legislation, subsequently conducting illegal operations with countries of more rigid legislation via components of their groups installed in countries that do not monitor the international transactions of funds;
- Games and Lotteries – The main characteristics of the criminal processes are the manipulation of awards and conduct of high volume of bets in a certain mode of games,

aiming to justify the gain obtained. In some cases, the criminals do not care if they lose part of the funds, as long as they manage to finalize the money laundering process;

- Stock Exchanges – In Brazil, the control and monitoring of these institutions are under the responsibilities of the Securities Commission ("CVM"). Stock exchanges offer favorable conditions for the conduct of money laundering operations, bearing in mid that (i) permit the conduct of business with international characteristics; (ii) have high index of liquidity; (iii) the purchase and sale transactions can be carried out in a short period of time and (iv) most of the operations are carried out through a broker;
- Insurance Companies – The market of insurance, capitalization and open private pension is supervised by the Private Insurance Superintendence ("SUSEP"), being another sector vulnerable to the money-laundering crimes, bearing in mind that: (i) insureds can launder money through the presentation of false or fraudulent notices of claims / damages and (ii) the intermediation materialized through brokerage, also can propitiate the money laundering involving third parties or non-resident customers; and
- Business Structures – Many times the criminals act by means business structures in the sectors of retail, industry or provision of services of any nature. Such structures may be:

    - Shell Companies: Present legal existence and physical location, but do not produce anything and do not carry out commercial transactions.
    - Ghost or Phantom Companies: Present false documentation and have no physical location.
    - Legitimate Companies: Present legal existence, physical location and, together with their legitimate businesses, use funds coming from crime.

Ex: High volume of transactions and movements, inconsistent with the type of activity and declared invoicing; large quantity of deposits (small amounts), withdrawals and electronic transfers; frauds in issuance of import and export invoices (using under or over invoices, keeping the difference earned, thus legalizing that amount).

1.2. What is an "Beneficial Owner"?

Individual or individuals who, together, have control or influence significantly, directly or indirectly, a customer in whose name a transaction is being conducted or it benefits out of which, or yet, the representative, including the attorney and the agent, who exercise the actual command over the activities of the legal entity.

1.2.1. What defines an "Active Client"?

Active customer is the customer who, in the last twelve (12) months, has carried out transactions in his current account or in his custody position, carried out operation in the securities market and/or presented balance in his custody position.

Exclusively in relation to customers of the Corporate Credit segment, an active customer is the one who carried out any credit operation in the last 6 months, or having a contract in force.

1.3. What defines a Politically Exposed Person ("PEP")?

For purposes of enforcement of national standards on the topic, the following are considered PEP: public agents performing or having performed, in the last five years, in Brazil or in foreign countries, territories or dependencies, offices, jobs or relevant public functions as well as their representatives, family members and other persons of their close relationship.

BOCOM BBM should obtain, from its customers, information that allow to characterize them or not as PEP and identify the origin of funds involved in the transactions of customers characterized as such.

1.3.1. PEP Individual

Brazilian individuals in the following conditions are considered as PEP:

- Holders of elective offices of Executive and Legislative Branches of the Federal Government;
- Occupants of offices in the Federal Government Executive Branch:
    - Of state minister or equivalent;
    - Of special nature or equivalent;
    - Of president, vice-president and director or equivalent positions, of autarchies, public foundations, public companies or private-public joint stock companies;
    - Of DAS Level 6 – Higher Direction and Advisory or equivalent.
- Members of the National Justice Council, the Federal Supreme Court, higher courts, district courts, federal courts, labor and election courts, of the Higher Labor Court and the Federal Justice Council;

- Members of the National Council of Public Prosecutor's Office, the Attorney General of the Republic, the Assistant Attorney General of the Republic, the Labor Attorney General, the Military Courts Attorney General, the Assistant Attorneys General of the Republic and the States and Federal District Attorneys General;
- Members of the Federal Audit Court, the Attorney General and Deputy Attorneys General of the Public Prosecutor's Office with the Federal Audit Court;
- Presidents and national treasurers, or equivalent, of political parties;
- State and Federal District Governors and Secretaries, State and District Deputies, presidents, or equivalents, of state and district indirect public administration entities and presidents of Courts of Justice, Military Courts, Audit Courts or equivalents of the States and the Federal District;
- Mayors, Councilmen, City Secretaries, presidents or equivalent, of entities of the municipal indirect public administration and presidents of Audit Courts or equivalent of Municipalities; and
- High-level officers and directors of public or private international law entities.

Foreign individuals exercising or having exercised major public functions in a foreign country are considered PEP such as chiefs of state or of government, high echelon politicians, occupants of high level governmental offices, general officers and members of high level of the Judiciary Branch, high level executives of public companies or directors of political parties.

1.3.2. PEP Legal Entity

Legal entities being controlled, directly or indirectly, by a politically exposed person are considered PEP.

1.3.3. Related PEP

The persons in the following situations are considered as related to PEP:

- Family members of the PEP, considering relatives in straight line, up to first degree, the spouse, companion, partner, stepson and step daughter;
- Politically Exposed Person appointed as attorney or agent;
- Close collaborator of PEP:
    - Individuals who are known for having a partnership or joint property or ownership in private legal entities or in arrangements with no legal personality,

appearing as attorneys, although through a private instrument, or having any other type of close relationship of public knowledge with a politically exposed person; and

  - Individuals having the control of private legal entities or in arrangements with no legal personality, known for having been created for the benefit of a politically exposed person.

- Conducting regular transactions or movements of financial funds from or to a politically exposed person customer of the institution, not justified by economic events such as acquisition of goods or provision of services.

1.4. What are Tax Havens?

By design, "Tax Havens" are countries or dependencies that do not tax income (or tax it at a tax rate below 20%) or yet, have internal legislation that does not allow access to information related to the shareholding or corporate composition of legal entities or the ownership thereof, such as those jurisdictions listed in RFB Normative Instruction 1.037 of June 4, 2010 as subsequently amended.

The full listing of Tax Havens should be regularly consulted at the Brazilian Federal Revenue Office.

1.5. What is the definition of a Non-Resident Investor (NRI)?

The following are considered non-resident investors by CVM: individuals or legal entities, including funds or other collective investment firms with residence, headquarters or domiciled abroad and who invest in Brazil.

1.6. What are non-profit organizations?

Non-profit organizations are those whose company's activity has not the purpose of accumulation of capital with consequential distribution of profit to its directors.

Such organizations are characterized for gathering several persons having the same purpose; they have no profitable ends, and their equity is formed by their associates.

1.7. What is the RBA – Risk-Based Approach?

BOCOM BBM adopts the risk-based approach as one of the main tools of AML/CFT, through the methodology described in Section 3.5, which optimizes human, material and informational resources, in order to enable an effective management of the activities developed in the processes of identification, monitoring, analysis, understanding and mitigation of AML/CFT risks.

1.8. What is the concept of "AML/CFT area"?

The AML/CFT area compromise AML area of BOCOM BBM Bank.

1.9. Who is "Senior Administration "?

The Senior Administration of Banco BOCOM BBM is composed by the statutory directors who make up the Compliance Committee, being responsible for the Governance of AML/CFT.

2. Objective

Financial institutions may be inadvertently used as intermediaries to conceal the true origin of funds from illegal activities, configuring money-laundering. In response to the increasing world concern facing this problem, several countries approved and reinforced their legislations in connection therewith.

The AML/CFT process is formed by a set of control actions which should be adopted in organized and integrated manner for greater effectiveness:

- Internal Risk Assessment;
- Risk-Based Approach;
- Identification, registration, qualification and classification of Customers, as described in the Customer Registration Policy and in the Operating Procedures of Know Your Customer;
- Know Your Customer (KYC), as described in the Operating Procedures of Know Your Customer.
- Know Your Employee (KYE), as described in the Operating Procedures of Know Your Employees;
- Know Your Service Provider and Supplier (KYS), as described in the Operating Procedures of Know Your Supplier.

- Know Your Partner (KYP), as described in the Policy of Selection of Brokers and in the Operating Procedures of You're your Partner;
- Assessment of new products, services and technologies, as described in the Product Approval Policy and in the Operating Procedure of Analysis of new products, services and technologies;
- Monitoring of Operations, as described in the Operating Procedure of Monitoring and Communication of Suspicious Operations and Situations;
- Communication of Suspicious Operations, as described in the Operating Procedure of Monitoring and Communication of Suspicious Operations and Situations; and
- Training, as described in the Ongoing Qualification and Training Policy.

The non-utilization of these controls may enable the relationship with criminals, thus entailing the following risks:

- Reputational: Risk of damage to the organization reputation which may be caused from a simple rumor;
- Legal: Risk of violation to current and applicable laws and regulations; and
- Operational: Risk of losses generated by improper systems and controls, failures of management and human errors.

Furthermore, this Policy reinforces the Financial Conglomerate BOCOM BBM ("BOCOM BBM") commitment to observe and enforce the current laws, by communicating suspicious cases to the proper authorities, as applicable, as well as setting forth functions and responsibilities related to the enforcement thereof.

3. Guidelines

3.1. Principles:

The principles synthetizing the guidelines described in this Policy are:

- Ethics and Legality - BOCOM BBM shall act in compliance with the legislation and regulation in force, within the highest ethical and conduct standards.
- Cooperation with Public Authorities - BOCOM BBM, in its position of institution watching over the regularity of the financial system, shall adopt strict policies of governance and enforcement of rules, oriented to the prevention and combat of money laundering.

- Ongoing Improvement – BOCOM BBM hereby undertakes to continuously improve standards of conduct, raising the quality of products, the security levels and efficiency of services.

BOCOM BBM's Board of Directors And Senior Administration are committed with the effectiveness and continuous improvement of the policy, of internal procedures and controls related to the Anti Money Laundering and Countering the Financing of Terrorism.

3.2. Exchange of Information among the members of Conglomerates BOCOM BBM

Aiming to gain efficiency and effectiveness, including in the Internal Risk Assessment, in the procedures destined to know your Customers and Procedures of Monitoring, selection and analysis of suspicious operations and situation, BOCOM BBM hereby elects to adopt a unique policy of AML/CFT, as well as of enforcement of procedures established in the regulation in centralized manner.

BOCOM BBM should have mechanisms for the exchange of information between its members aiming to avoid that failures in the communication between the internal control units would prevent the fulfillment of obligations related to AML/CFT. Such exchange of information should consider the relevance of the risk identified in each case, always in line with the Internal Risk Assessment.

3.3. Information's Confidentiality

Confidential Information is understood as that owned by BOCOM BBM or by third parties destined to the restrict use by BOCOM BBM, which should not be disclosed to any third parties, except in cases expressly provided for by the law or upon authorization by the owner of the information.

It is essentially important that the information on suspicions of crime of money-laundering is confidential, and it should only be directed to AML/CFT Area, for analysis and adoption of applicable actions. The identity of the employee pointing out the suspicion shall be equally kept confidential.

Additionally, the communications reported to regulatory bodies, as applicable, have a strictly confidential nature, and the knowledge of the parties involved is strictly prohibited.

BOCOM BBM is responsible for safeguarding and continuous maintenance of information and documents obtained from its customers and watches over their security and confidentiality, following the legal and regulatory principles as well as the rules set forth in its procedures related to the matter.

3.4. Customer Registration

The registration of customers is the pillar of identification of the Know Your Customer (KYC) process.

This process should attest the quality of information in order to enable the proper identification of customers and it should be conducted based on the calculation of the risks of occurrence of the practice of money laundering crime.

The customer's registration should be updated within periods not longer than:

- Five (5) years for customers classified as lower risk; and
- Two (2) years for customers classified as higher risk.

BOCOM BBM adopts procedures enabling the collection of registration information described in the Customers Registration Policy and in the Operating Procedures of Know Your Customer.

In general, the following registration information should be obtained from the customers, as a minimum:

- Identification:
    - Individuals: Full name, parents' name, nationality, date and location of birth, gender, marital status, name of spouse if married, occupation, identification document (type, number, date of issue and issuing body), number of enrollment in the Ministry of Treasury National Individual Taxpayers' Roll ("CPF/MF"), name and CPF/MF (as applicable) of their representatives and attorneys;
    - Legal Entities: Corporate name, core activity, form and date of organization, number of enrollment in the Ministry of Treasury National Corporate Taxpayers' Roll ("CNPJ/MF"), name and CPF/MF (as applicable) of its

representatives, directors, attorneys and corporate participation chain until reaching the individual, characterized as final beneficiary;

- Legal Entities (publicly-held companies or non-profit entities): corporate name, core activity, form and date of organization, number of enrollment in the CNPJ/MF, name and CPF/MF (as applicable) of its representatives, attorneys, controllers, directors and officers, if any; and
- Persons Non-Resident in Brazil (INR's):
  - Individuals: Full name, parents' name, nationality, date and location of birth, gender, marital status, name of spouse, if married, occupation, identification document (Passport), name and passport (as applicable) of its representatives and attorneys; and
  - Legal Entities: Corporate name, core activity, form and date of organization, number of enrollment in the Ministry of Treasury National Corporate Taxpayers' Roll ("CNPJ/MF"), name and identification document (Passport) of its representatives, directors (including Executive Board and Board of Directors), attorneys and corporate participation chain until reaching the individual, characterized as final beneficiary.

- Residential address (for individuals), main address (for legal entities), mail address (for individuals and legal entities), telephone number and area code;
- Amounts of monthly income and equity, in the case of Individuals, and average monthly invoicing of the twelve previous months in case of Legal Entities;
- Signed statement on the purposes and nature of business relationship with the institution; and
- Characterization as PEP, as applicable.

Customers are responsible for the veracity of the stated information and for the documents submitted in the retaining of products and services provided by BOCOM BBM, under penalty of personal accountability under terms of the current legislation.

Nevertheless, in the process of registration update and in the verification tests, it is extremely important that the missing registration data are collected, and the inconsistent registration data of existing and active customers are corrected, if any.

BOCOM BBM may resort to publicly available information or to databases to form the missing registration data or to correct inconsistent registration data of its existing customers.

It is prohibited to start a business relationship without the completion of the procedure of identification and qualification of customers.

It is allowed, for a maximum period of thirty days, the beginning of the business relationship in case of insufficient information regarding the client's qualification, as long as there is no damage to the procedures of monitoring and selection of operations and situations.

3.5. Risk-based Approach and Internal Risk Assessment

The continuous threat of money laundering through banks is fought in the most efficient form through the knowledge and treatment of potential risks associated with the customers and the transactions.

The conduct of an Internal Risk Assessment enables to identify and measure the risk of utilization of its products and services in the practice of money laundering and terrorism financing, and for that, the potential risks associated with the following dimensions of activity are observed:

- Customers;
- Institution, including the business model and the geographic area of activity;
- Operations, transactions, products and services covering all distribution channels and utilization of new technologies; and
- Activities performed by employees, partners and outsourced service providers.

The risk assessment should be reviewed each two years, as well as on the occurrence of significant changes in the above risk profiles.

The application of the Risk-based Approach, in turn, enables BOCOM BBM to prevent and combat the risk of money laundering in an efficient manner, safeguarding its own and its customers' reputation with the strict compliance with the laws and rules in force.

3.5.1. Risk Rating

As part of the Risk-based Approach methodology, diligence procedures are performed on the following relationships:

- Customers;
- Employees;
- Partners; and
- Service providers.

According to specific procedures those will be classified as Low, Medium and High risk, according to specific criteria that will provide the definition of the treatment of monitoring and revision of diligence of knowledge thereon. Besides the classification of the relationship segments, the new products, services and Technologies offered will also be classified.

Customers should be classified two groups:

- Prospective Segments: Segments subject to prospection, listed at levels of risk of involvement with activities of money laundering and terrorism financing.
- Prohibited Segments: Segments whose risk associated with the activity performed exceeds the institution's risk appetite or those connected to illegal lines and activities, which should be excluded from the universe subject to prospection.

In order to mitigate the AML/CFT risks associated with the relationships with customers, employees, service providers and partners, BOCOM BBM should adopt appropriate procedures and steps for those classified as higher risk, including, but with no limitation:

- Application of in-depth diligence at the start and during the relationship;
- Approval by higher competence for start or continuation of the relationship;
- Reinforced monitoring (special attention);
- Revision of KYC (Know Your Customer) with differentiated time lapses according to the assigned degree of risk;
- Revision of KYP (Know Your Partner) with differentiated time lapses according to the assigned degree of risk;
- Revision of KYS (Know Your Supplier) with differentiated time lapses according to the assigned degree of risk; and
- Revision of KYE (Know Your Employee) with differentiated time lapses according to the assigned degree of risk.

3.6. Politically Exposed Person - PEP

BOCOM BBM is concerned with movements and transactions involving PEP for the risk of image and legal risk which may be associated with the institution. This type of customer may have involvement with certain wrongdoings, including, but with no limitation, passive corruption, collusion, extorsion by public employee, embezzlement (misappropriation by public employee of public or private money of which he has the possession due to his office or deviation of money in his or third party's advantage) and influence peddling, situations which could render questionable the origin of resources.

For the identification of politically exposed persons, BOCOM BBM can adopt the following actions:

- To request an express declaration from the customer, beneficiary, third party or other related parties on the classification thereof;
- To resort to publicly available information; and
- To resort to databases on politically exposed persons.

The PEP identification process is detailed in the Operating Procedure of Identification of Politically Exposed Persons.

It is worth mentioning that the PEP condition is not a restrictive element, but it should be subject of in-depth diligence for assessment of money-laundering risks in the start or during the relationship, including the validation of information, analysis of origin of financial resources transacted and the financial capacity, among others.

BOCOM BBM will start a relationship or continue an already existing relationship with the customer classified as PEP only upon the Board's approval.

A reinforced monitoring should also be conducted of the customers considered as PEP through the adoption of more rigorous procedures for the determination of suspicious situations.

The communications made by BOCOM BBM to the regulatory bodies of suspicious operations of money laundering related to a customer identified as PEP should specifically include such information.

3.7. Beneficial Owner

The facility with which legal entities are created and dissolved allows that they may be used not only for legitimate ends but for the integration, in the financial market, of funds of illegal origin, as well as for the concealment of their Beneficial Owner.

The proper identification of the Beneficial Owners of customers legal entities is an important process for mitigation of risk of money laundering by the banks.

BOCOM BBM adopts the following procedures to identify the Beneficial Owners of its customers legal entities:

- To analyze the corporate structure, knowing and understanding who the shareholders / partners / owners of the company are, by obtaining the name, CPF/MF (as applicable) and percentage of shareholding in the capital stock (and in case of control by another legal entity, open the path until reaching the individuals);
- To analyze official documents of legal entities (e.g. company organizational acts – Articles of Incorporation, Corporate Bylaws and/or Power of Attorney, etc.): to know and understand who their representatives, directors are
- To resort to publicly available information or databases;
- To dedicate special attention to the cases in which it is not possible to conduct such identification;
- To maintain records of the analyses made; and
- To maintain the information updated.

3.8. Non-Profit Organizations

Non-profit organizations in Brazil are easily created and have no robust regulation, so that they may be used by persons with shady purposes for the practice of money-laundering crimes.

BOCOM BMM adopts the following procedures to analyze and monitor the relationship with non-profit organizations:

- To analyze the corporate structure: to know and understand who are the shareholders / partners, by obtaining the name, CPF/MF (as applicable) and percentage of interest in the capital stock (and in case of control by another legal entity, go through the path until reaching the individuals).

- To analyze the organization official documents;
- To resort to publicly available information or databases;
- To assign classification of Special Attention to all the customers / partners / suppliers with nature of non-profit organization; and
- In Approval Routine for start of relationship and/or monitoring, the analysis will occur in competence higher than that of the risk that will be assigned to the organization.

3.9. Non-Resident Investors (NRI)

Non-resident investors should be observed with more regularity for registration purposes, since, as they are not domiciled in the same country as the financial institution, the exchange of information between them and the latter may become more fragile than with a resident investor.

The Conglomerate BOCOMBBM meets all the regulatory and legal requirements for purposes of registration and maintenance of a non-resident in the list of customers, according to Procedures of Know Your Customer and the Customer Registration Policy.

3.10. Know Your Customer or "KYC":

The process of Know Your Customer ("KYC") is a set of actions aiming to assure, with accuracy and at any time, the identify (who it is), the activity (what it does) and the coherence in the origin and movement of resources of customers individuals or legal entities, and it is detailed in the Operating Procedures of Know Your Customer.

It is one of the most important pillars in the prevention of money laundering also recommended by the Basel Committee. The banks should establish a set of rules and appropriate procedures aiming to identify and know the origin and constitution of the customer's equity and financial resources.

The process of Know Your Customer is adopted by the banks aiming to provide direction and standardization to the start, maintenance and monitoring of the relationship with customers that use or intend to use the products and services, in order to prevent their involvement in illegal activities configuring crime of money laundering and protecting their reputation and image.

For application of the KYC principle, the customer's identification should be established prior to the start of the relationship with BOCOM BBM. Such identification should be standardized by means of registration forms and copies of documents required by law. The registration data of all customers should be duly updated; documents of inactive customers should be filed at the Institution for 10 years, at least.

It is extremely important to obtain information that allow the tracing of the customer's profile such as: income, equity, available and fixed, occupation, professional / economic activity, among others. Such information should be sufficient for identification of risks of occurrence of money laundering or terrorism financing and the verification of the compatibility between the movement of resources, the origin thereof and the customer's financial capacity.

Prior to the start of the relationship with the customer, the AML/CFT area should conduct analysis thereof and other parties involved in the requested operation, according to a previously defined research operating procedure.

3.10.1. KYC Analysis

Prior to the start of the relationship, the AML/CFT Area should conduct the analysis (according to pre-defined scope of searches in websites of public bodies, search websites and national and international databases) of customers and their representatives, if any. Besides, in the case of individual customer, the spouse should also be analyzed. For legal entity customer, the corporate chain should be analyzed up to the individual characterized as Beneficial Owner, besides their directors and representatives, including the attorney and the agent who exercises the actual command over the legal entity activities.

The KYC process as well as the scope of the analysis are detailed in the Operating Procedures of Know Your Customer.

For customers of Wealth Management and Institutional Funding, the documentation proving the respective financial capacity should also be analyzed, and requesting additional documentation proving the origin of applied funds with BOCOM BBM, according to the risk associated with the customer.

For Credit customers, the Credit Analysis area is responsible for the analysis of the customer's financial capacity.

After conducting the analyses, the AML/CFT Area should issue an opinion reporting, as applicable, the relevant facts worthy of attention and which may serve for subsequent discussion at the Compliance Committee.

All evidence related to the above procedure should be filed by the AML/CFT Area.

The AML/CFT area shall carry out the monitoring of the customer base according to the risk assigned to the customer, in order to enable an eventual reclassification of risk, in case of change in the customer's information table.

3.11. Know Your Employee ("KYE")

The institution's constant fear of money laundering is increasingly more notorious in the market. Companies are adopting procedures aiming to prevent the entrance of money from criminal activities.

As the "money launderers" use the most varied forms in their attempt to "clean" their illegal funds, employees can be considered another means for such attempt definitively to be carried out. For that, the criminals do not hesitate to offer bribes aiming to circumvent the institution internal controls.

BOCOM BBM is concerned with the quality of its staff and it is aware of the risks that poor hiring may cause; therefore, operating routines are required to provide the proper hiring of persons and their continuous monitoring.

3.11.1. KYE Analysis

The KYE process aims to provide the institution with greater knowledge of its employees, by preventing future occurrences that may configure frauds or acts that may adversely affect the institution image.

The KYE process as well as the scope of the analysis are detailed in the Operating Procedure of KYE.

The AML/CFT Area:

- To analyze employees at the time of hiring, according to the pre-defined research scope;
- To forward Opinion to the Persons' Area with the result of the searches;
- To conduct monitoring of the employee base according to the assigned risk;

- To define the criteria and procedures for selection and training, together with the Persons' Area and for the follow up of the economic-financial situation of employees, together with the Managers of each area.

3.11.2. HR

The HR Area shall:

- Forward listing of employees being hired to AML/CFT Area;
- File the Opinions forwarded by AML/CFT Area;
- Re-forward the relevant information to the contracting area and to the Persons' Committee, as applicable; and
- It is extremely important that the information searched by AML/CFT Area be maintained in absolute confidentiality, and it should not be disclosed to third parties or printed for any other purpose.

3.11.3. Managers of Areas

The area managers should also monitor the behavior of their respective employees by paying special attention to the following cases:

- Unusual change in standards of life and behavior of employee or representative with no visible cause;
- Unusual modification of the employee's or representative's operating result with no visible cause;
- Conduct of any business in different manner from the institution formal procedure by employee or representative; and
- Supply of assistance or information paid or not, to customer in prejudice to the institution AML/CFT program, or for assistance to structure or fraction operations, circumventing or defrauding regulatory or operating limits.

Any change of behavior observed within such scope should be informed to the Manager of AML/CFT Area.

3.12. Know Your Supplier / Service Provider (KYS)

BOCOM BBM adopts internal rules, procedures and controls for the identification and acceptance of suppliers and service providers according to the risk of money laundering, by preventing the retaining of dishonest companies or suspected of involvement in wrongdoings.

The expense managing area should forward to the AML/CFT Area the corporate name and CNPJ/MF of involved companies in order to start the searches according to scope of the Operating Procedure of Know Your Supplier / Service Provider. AML/CFT Area may request additional documentation of the company, such as, for instance, Consolidated Articles of Incorporation / Corporate Bylaws as subsequently amended, Minutes of Electoin of the Executive Board with current term of office and Power of Attorney.

For suppliers and service providers classified as higher risk complementary procedures and in-depth diligence of assessment and specific competence of approval should be adopted according to the criticality of annotations or exceptions, following a risk-based approach.

3.12.1. KYS Analysis

Prior to the start of the relationship, the AML/CFT Area should conduct the analysis (according to pre-defined scope of search in websites of public bodies, search sites and national and international databases) of the Service Providers and Suppliers.

The KYS process as well as the scope of the analysis are detailed in the Operating Procedure of Know Your Supplier / Service Provider.

After conducting the analyses, AML/CFT Area should issue an opinion reporting, as applicable, the relevant facts worthy of attention and which may serve for subsequent discussion in the Compliance Committee.

All evidence related to the above procedure should be filed by AML/CFT Area.

AML/CFT Area shall be responsible for conducting the monitoring of the service provider/suppliers base according to the assigned risk.

3.13. Know Your Partner (KYP)

BOCOM BBM adopts internal rules, procedures and controls for the identification, analysis and acceptance of start of relationship with partner institutions such as Banks, Managers and Brokers.

By means of the Know Your Partner Procedures, it is possible to conduct an analysis aiming to prevent the execution of agreements with dishonest institutions or those that are suspected of involvement in wrongdoings.

The area responsible for the relationship with the partner shall forward to the AML/CFT Area the required information, depending on the activity subject of the partnership, so that the searches can start as described in the Operating Procedures of Know Your Partner.

For Partners classified as Higher Risk complementary procedures and in-depth diligence of assessment and specific competences of approval should be adopted, according to the criticality of annotations or exceptions, according to the risk-based approach.

3.13.1. KYP Analysis

Prior to the start of the relationship, the AML/CFT Area should conduct the analysis (according to pre-defined scope of searches in public bodies websites, search sites and national and international databases) of potential Partners.

The scope of documental analysis and search made will vary according to the nature of the partnership made, and each of them can be verified in the Operating Procedures of Know Your Partner.

After conducting the analyses, the AML/CFT Area should issue an opinion reporting, as applicable, the relevant facts worthy of attention and which may serve for subsequent discussion in the Compliance Committee.

All evidence related to the above procedures should be filed by the AML/CFT Area.

The AML/CFT Area shall be responsible for the monitoring of the partners base according to the assigned risk.

3.14. New Products, Services and Technologies

The AML/CFT Area should conduct a previous analysis of new products, services and Technologies, according to the Operating Procedure of Analysis of new products, services and Technologies, under the optics of AML/CFT and vote at the Product Committee meeting that will deliberate on the approval of any new product or service, observing the Product Approval Policy.

The Product Area should consult the AML/CFT Area by mail on the analysis under the AML/CFT optics prior to the holding of the Committee meeting in which the approval of the new product or service will be assessed.

3.15. Monitoring of Operations

BOCOM BBM adopts, under terms of the Procedure of Monitoring and Communication of Suspicious Operations and Situations, such rules and procedures for monitoring of proposals and operations carried out by its customers.

3.15.1. Customers of Wealth Management and Institutional Funding

All transactions and movements of the customers' current accounts, either of Wealth Management or Institutional Funding, should be monitored by AML/CFT Area. The purpose of such monitoring is to highlight atypical movements which may configure signs of money laundering.

Such monitoring is based on the setting of several rules of customers' behavior which are supported by a system of control of signs of money laundering operations.

The rules are applied to all transactions carried out in the customers' accounts and take into account parameters such as equity, income, registration information, frequency of transactions, among others.

At the end of the monitoring process, AML/CFT Area will have a listing containing the customers who may have been classified within any of the indicator parameters of atypical operations.

Possible de-classifications should be justified and analyzed by AML/CFT Area, observing the period of 45 days from the alert generated by the transaction, based on the customer's registration information and the parameters that generated the suspicion.

If AML/CFT Area understands that certain operation is atypical configuring sign of money laundering, the operation should be referred for discussion and analysis by the Compliance Committee. If the Compliance Committee will deem that such operation is indeed suspicious of configuring crime of money laundering, such fact will be informed to the proper regulatory body.

3.15.2. Credit Customers

The monitoring of operations of credit customers is under the responsibility of the Corporate Credit Control; this area should pay special attention to the following situations:

- Performance of credit operations in the Country settled with funds apparently inconsistent with the customer's economic-financial situation;
- Request of granting of credit in the Country inconsistent with the customer's economic activity or financial capacity;
- Performance of credit operation in the Country followed by remittance of funds abroad, with no economic or legal grounds, and with no relationship with the credit operation;
- Performance of credit operations in the Country, simultaneous or consecutive, settled in advance or in a very short time;
- Settlement of credit operations in the Country by third parties with no apparent justification;
- Granting of guarantees of credit operations in the Country by third parties not related to the borrower;
- Performance of credit operation in the Country with offer of guarantee abroad by customer with no tradition of operations abroad; and
- Acquisition of goods or services incompatible with the purpose of the legal entity, especially when the funds come from credit in the Country.

The Corporate Credit Control area shall inform the AML/CFT Area, if it identifies any atypical operation, so that such operation may be referred for discussion and analysis by the Compliance Committee, observing the period of 45 days from the generated alert. If the Compliance Committee will deem that such operation is indeed suspicious of configuring crime of money laundering, such fact will be informed to the proper regulatory body.

3.15.3. Monitoring of operations, clients or assets related to sanctions imposed by United Nations Security Council (UNSC) resolutions.

The beginning or maintenance of relations with individuals or entities mentioned on the sanction lists imposed by United Nations Security Council (UNSC) resolutions is prohibited. As a result of any identification of registry on sanction lists imposed by United Nations Security Council (UNSC) resolutions, in case of confirmation of the client's identity, BOCOM BBM must block the account and deliberate regarding the termination of the relationship.

Communication to regulatory agencies precedes the blocking and/or termination of the relationship.

3.16. Communication of Suspicious Operations

The AML/CFT Area should inform the Brazilian Financial Activities Control Council (COAF) and other regulatory bodies, according to the Procedure of Monitoring and Communication of Suspicious Operations and Situations, all operations or proposals of operations which may configure the existence of signs of crime of money laundering within 24 hours from the determination of existence of operation subject to communication.

The above communications should mention the participation or the involvement of PEP, as applicable.

The AML/CFT Area should also inform the regulatory bodies, in the frequency, form and conditions established thereby, the non-occurrence of proposals of operation or operations subject to communication, under terms of the current regulatory rules.

The AML/CFT Area should maintain the records of conclusions of their analyses about operations or proposals of operations which grounded the decision to make, or not, the communications referring to the signs of wrongdoing or crime of money laundering for five (5) years, or for longer period in case of determination by the regulatory bodies.

Good faith communications, as provided for in Paragraph Two of Article 11 of Law 9.613/98, will not cause civil, criminal or administrative liability to BOCOM BBM or its controllers, directors and employees.

3.17. Records of operations within the negotiation and registration environments, Products and Services Contracted

Operations carried out, products and services contracted, including withdrawals, deposits, contributions, provisions, payments, receipts and transfers of funds involving institutions of BOCOM BBM, should be duly recorded and the information stored for the period of 10 years.

The above records should contain, as a minimum:

- Type of operation carried out;
- Value of operation (as applicable);
- Date of holding;
- Name, CPF/CNPJ of the holder and beneficiary of the transaction;
- Channel used;
- Number of identification or registration of the company in the respective country of origin (in case of legal entity domiciled abroad);
- Type and number of travel document and respective issuing country; (in case of individual residing abroad); and
- International body of which it is a representative for the exercise of specific functions in the Country, as the case may be.

3.18. Treatment of Exceptions

Any exception to our Policies and Procedures should be analyzed and approved by the Manager of the AML/CFT area, by the Directors in charge of AML/CFT and by, at least, another Director being a member of the Compliance Committee, with subsequent remittance for acknowledgment by the Compliance Committee.

3.19. Training

BOCOM BBM has specific training program of qualification of its employees for the fulfillment of legal and regulatory requirements in force on AML/CFT.

Observing the rules appearing in the Continuous Qualification and Training Policy, the training program should be applied annually for, at least, the employees who:

- Have direct relationship with the customer;
- Are part of any stage of relationship or the flow of hiring and utilization of products and services;
- Participate in the development of new processes, products and services; and
- Act in the areas of AML/CFT, controls, compliance, risk management, audit and support to business.

3.19.1. Training Methods

Training may be held by means of presential interaction, at distance (e-learning), video-conference (audiovisual), audio-conference, press releases or publications, using clear and accessible language as well as other means that may be provided by BOCOM BBM.

3.20. Follow-up and Control Mechanisms

BOCOM BBM should have follow-up and control mechanisms in order to assure the implementation and adequacy of the policy, procedures and internal controls of AML/CFT, including:

- The definition of processes, tests and audit trails;
- The definition of proper metrics and indicators; and
- The identification and correction of eventual deficiencies.

Mechanisms should be subject to periodic tests by internal audit, as applicable, compatible with the institution internal controls.

3.20.1. Effectiveness Report

BOCOM BBM should perform an assessment of the policy effectiveness, of procedures and internal controls of AML/CFT, which should be documented in specific report.

3.21. Final considerations

- This document is for strictly internal use and should not be made available to third parties without consulting the AML/CFT Area manager.
- The accession to this Policy is mandatory to all employees and interns of BOCOM BBM.
- Employees or interns infringing the rules and procedures provided for herein shall be subject to applicable penalties.
- For clarification of any doubts related to this Policy, the AML/CFT Area should be consulted.

Situations not provided for herein shall be timely assessed by the Directors in charge of the AML/CFT activities, as applicable, and may be referred to the Compliance Committee at their sole discretion.

4. The responsibilities of this policy

Responsibility	Responsible
Area responsible for policy management	AML/CFT.
Who it applies to	This Policy covers all employees, interns, partners and third parties providing relevant services to the Financial Conglomerate BOCOM BBM ("BOCOM BBM"), according to the applicability thereof.
Who approves	Manager, Senior Manager of the AML/CFT area and the Senior Administration.

Concerning the enforcement of this Policy, it is important to emphasize that all the BOCOM BBM employees and interns have distinct functions and responsibilities varying according to area in which they are inserted.

It is the responsibility of the Board of Directors BOCOM BBM

- The Board of Directors of BOCOM BBM is responsible for approving the AML/CFT policy, as well as supporting its compliance, thus ensuring its effectiveness.

It is the responsibility of the Senior Administration

The Senior Administration is responsible for approving the AML/CFT Policy, the Internal Risk Assessment and the AML Operational Procedures. The Senior Administration should make sure that:

- It is timely aware of the risks of compliance related to AML/CFT;
- The directors in charge have Independence, autonomy and technical knowledge sufficient for the full performance of their duties, as well as the full access to all information they

may deem necessary so that the respective governance of risks of money laundering and terrorism financing may be carried out;

- The systems responsible for the collection, updating and safeguarding of information related to the procedures of Know Your Customer are appropriate to the purpose to which they are destined;
- The systems of monitoring of operations and atypical;
- Situations are aligned with the institution's risk appetite, as well as they can be promptly customized in the event of any change in the respective AML/CFT risk matrix; and
- Sufficient human and financial resources were actually allocated for the enforcement of the previously described points and issues.

It is the responsibility of the Commercial Areas

The commercial areas have the following functions and responsibilities:

- To obtain and record all information that enable to identify and qualify customers, as well as the origin of funds;
- To pay attention to behaviors considered suspicious and/or operations considered atypical, considering the customers' profile and their history of activities, including, with no limitation, the behaviors and operations listed in normative issued by regulatory bodies; and
- To notify the AML/CFT area when verifying the occurrence of a suspicious behavior, an atypical operation or proposal thereof.

It is the responsibility of the AML/CFT Area

The AML/CFT area have the following functions and responsibilities:

- To conduct the analyses of KYC, KYE, KYS and KYP;
- To analyze the operations considered atypical, by issuing a duly justified opinion and submitting it to the analysis by the Compliance Committee as applicable;
- To previously analyze new products, services and Technologies under the optics of prevention of crimes of money laundering and terrorism financing;
- To inform the proper authorities on the signs of money laundering, as applicable;
- To maintain filed the annotations made as well evidence of procedures carried out for purposes of AML/CFT;

- To hold periodic training, by maintaining evidence and records thereof; and
- To define policies and procedures to be followed, aiming essentially to prevent money laundering and terrorism financing.

It is the responsibility of the Compliance Committee

The Compliance Committee meets quarterly under the chair of the Director of Compliance and AML/CFT, to treat, among other topics, of matters related to AML/CFT. The Committee will discuss the cases indicated by the AML/CFT Area, by issuing an opinion on the following topics, among others that may be brought to the Committee's attention: (i) recommendation of reporting of atypical operations to the regulatory bodies, and (ii) as well as the start or maintenance of relationship in special cases.

The Committee is constituted in its own regulation available on the Intranet.

It is the responsibility of the Compliance Committee

The Compliance Committee meets quarterly under the chair of the Director of Compliance and AML/CFT, to treat, among other topics, of matters related to AML/CFT. The Committee will discuss the cases indicated by the AML/CFT Area, by issuing an opinion on the following topics, among others that may be brought to the Committee's attention: (i) recommendation of reporting of atypical operations to the regulatory bodies, and (ii) as well as the start or maintenance of relationship in special cases.

The Committee is constituted in its own regulation available on the Intranet.

It is the responsibility of the Employees, Interns and relevant Third Parties

Employees and interns of all areas as well as third parties providing relevant services to the Conglomerate BOCOM BBM, should comply with the legislation and regulations in force, as well as following the guidelines and procedures present in this Policy and in the Code of Ethics and Conduct.

All employees, interns and third parties have the responsibility to report to the AML/CLT Areas any suspicious situation which may configure sign of money laundering or terrorism financing of which they are aware.

It is the responsibility of the Client Registry

The Client Registry Area has the following functions and responsibilities:

- To receive and analyze the registration documentation of customers, in compliance with the Customer Registration Policy;
- To assure that the processes of collection and updating of registration information of customers consider all the requirements of the current regulation;
- To conduct periodic tests of registration verification according to the current regulation;
- To observe behaviors considered suspicious and/or operations considered atypical, considering the customers' profile and their history of activities, including, but with no limitation, the behaviors and operations listed in normative issued by regulatory bodies; and
- To notify the AML/CFT Area when verifying the occurrence of a suspicious behavior or atypical operation.

Parties responsible for maintenance of this Policy

The Managers of each of the areas subject to this Policy are responsible for the monitoring of the execution of the attributions herein established.

Parties responsible for maintenance of this Policy

The AML/CFT Area is responsible for the maintenance and updating of this Policy, at least, each 12 months.

5. Internal reference

- Code of Ethics and Conduct;
- Cyber Information Security Policy;
- Customer Registration Policy;
- Product Approval Policy;
- Contract Management Policy;
- Ongoing Training and Qualification Policy;
- Corruption Prevention Policy;
- Compliance Policy;
- Gift, Gratuity and Entertainment Policy;

- Denunciation Reception and Treatment Policy;
- Adverse Reputational Information Reporting Policy;
- Sanctions Policy;
- Brokers Policy and Selection;
- Operating Procedure of Identification of Politically Exposed Persons;
- Operating Procedures of Know Your Customer,
- Operating Procedures of Know Your Supplier;
- Operating Procedures of Know Your Partner;
- Operating Procedures of Know Your Employee; and
- Operating Procedure of Monitoring and Communication of Suspicious Operations and Situations.

6. Control of versions and policy effectiveness

This policy is valid for 1 year.

Version	Date	History	Authors
1.	19/04/2004	Document Creation	Compliance
2.	03/07/2006	Document Update	Compliance
3.	08/08/2006	Document Update	Compliance
4.	01/08/2008	Document Update	Compliance
5.	01/02/2010	Document Update	Compliance
6.	26/07/2011	Document Update	Compliance
7.	28/08/2012	Document Update	Compliance
8.	22/02/2013	Document Update	Compliance
9.	25/09/2013	Document Update	Compliance
9.	22/09/2014	Document Update	Compliance

10.	09/12/2014	Document Update	Compliance
11.	05/05/2015	Document Update	Compliance
12.	30/06/2016	Document Update	Compliance
13.	20/03/2018	Document Revision and Update	Compliance
14.	30/09/2020	Document Revision and Update	AML/CFT area
15.	16/10/2020	Document Revision and Update	AML/CFT area
16.	16/10/2021	Document Revision and Update	AML/CFT area and Corporate Compliance
17.	21/10/2022	Document Revision and Update	AML/CFT área
18.	22/01/2024	Document Revision and Update	Área de PLDCFT
19.	22/01/2025	Document Revision and Update	Área de PLDCFT

7. Approvals

DocuSigned by:
BFF28ABC55CE453...

Yan Mannarino – Manager of AML/CFT

DocuSigned by:
Luiz Augusto Maffazioli Guimarães
8797F7E2FBFC427...

Luiz Augusto Maffazioli Guimarães – Senior Manager of Compliance and AML/CFT

8. Annexes

8.1. Related legislation / Regulation

- 2021

CVM Resolution No. 50 of August 31, 2021: Provides for the Anti Money Laundering, Countering the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction – AML/CFT within the securities market and revokes CVM Instruction No. 617 of December 5, 2019 and the Explanatory Note to CVM Instruction No. 617 of December 5, 2019.

- 2020

BACEN Circular Letter 3.978 of January 23, 2020: It provides on the policy, procedures and internal controls to be adopted by the institutions authorized to operate by the Brazilian Central Bank, aiming at the prevention of utilization of the financial system for the practice of money-laundering crimes or concealment of assets, rights and valuables, addressed in Law 9.613 of March 3, 1998, and terrorism financing, provided for in Law 13.260 of March 16, 2016.

B3 External Communiqué 003/2020 of September 22, 2020: - Risk-Based Approach ("RBA") and Simplified Registration of Non-Resident Investor (NRI) – Minimum Requirements to be observed by BSM in the supervision of CVM Instruction 617/2019

- 2019

CVM Normative Instruction 617 of December 6, 2019: It provides on the prevention of money-laundering and financing of terrorism – AML/CFT within the scope of the securities market.

- 2017

COAF Resolution 29 of December 7, 2017: It provides on the procedures to be observed by persons regulated by COAF, under Paragraph 1 of Article 14 of Law 9.613 of March 3, 1998, related to politically exposed persons.

Circular Letter 3.858 of November 14, 2017: It regulates the parameters for application of administrative penalties provided for in Law 9.613 of March 3, 1998.

Law 13.506 of November 13, 2017: It provides on sanctioning administrative proceeding within the scope of the Brazilian Central Bank and the Securities Commission; it amends Law 6.385 of December 7, 1976, Law 4.131 of September 3, 1962, Law 4.829 of November 5, 1965, Law 6.024 of March 13, 1974, Law 7.492 of June 16, 1986, Law 9.069 of June 29, 1995, Law 9.613 of March 3, 1998, Law 10.214 of March 27, 2001, Law 11.371 of November 28, 2006, Law 11.795 of October 8, 2008, Law 12.810 of May 15, 2013, Law 12.865 of October 9, 2013, Law 4.595 of December 31, 1964, Decree 23.258 of October 19. Decree 9.025 of February 27, 1946, and Executive Order 2.224 of September 4, 2001; it revokes Decree 448 of February 3, 1969, and provisions of Law 9.447 of March 14, 1997, of Law 4.380 of August 21, 1964, of Law 4.728 of July 14, 1965, and of Law 9.873 of November 23, 1999; and other provisions.

Circular Letter 3.839 of June 28, 2017: It amends Circular Letter 3.461 of July 24, 2009 which consolidates the rules on the procedures to be adopted in the prevention and combat of the activities related to the crimes provided for in Law 9.613 of March 3, 1998.

- 2016

Circular Letter 3.780 of January 21, 2016: It provides on the procedures to be adopted by financial institutions and other institutions authorized to operate by the Brazilian Central Bank in compliance with Law 13.170 of October 16, 2015, which governs the action of non-availability of assets, rights or valuables as a result of resolution by the United Nations Security Council (UNSC).

- 2015

CVM Instruction 560 of May 30, 2015: It provides on the registration, operations and disclosure of information of investor non-resident in the Country.

- 2014

CVM Instruction 553 of October 16, 2014: It amends provisions of CVM Instruction 301.

- 2013

Circular Letter 3.654 of March 27, 2013: It amends Circular Letter 3.461 of July 24, 2009 which consolidates the rules on the procedures to be adopted in the prevention and combat of the activities related to crimes provided for in Law 9.613 of March 3, 1978

CVM Instruction 534 of June 4, 2013: It amends provisions of CVM Instruction 301.

- 2012

Law 12.683 of July 9, 2012: It amends Law 9.613 to make more efficient the criminal prosecution of money laundering crimes.

CVM Instruction 523 of May 28, 2012: It amends articles of CVM Instruction 301.

Circular Letter 3.584 of March 12, 2012: It amends the Regulation of International Exchange and Capitals Market.

Circular Letter 3.583 of March 12, 2012: It amends Circular Letter 3.461.

Circular Letter 3.542 of March 12, 2012: It announces the list of operations and situations which may configure signs of occurrence of crimes provided for in Law 9.613 subject to communication to the Financial Activities Control Council (Coaf).

- 2011

CVM Instruction 505 of September 27, 2011: It establishes rules and procedures to be observed in the operations carried out with securities in regulated securities markets.

CVM Instruction 506 of September 27, 2011: It amends the CVM Instruction 301.

- 2010

Circular Letter 3517 of December 7, 2010: It amends Circular Letter 3.461 of July 24, 2009 which consolidates the rules on the procedures to be adopted in the prevention and combat of activities related to the crimes provided for in Law 9.613 of March 3, 1998.

RFB Normative Instruction 1.037 of June 4, 2010: It lists countries or dependencies with favored taxation and privileged tax regimes.

Circular Letter 3430 of February 11, 2010: It clarifies aspects related to the prevention and combat of activities related to the crimes provided for in Law 9.613 of March 3, 1998, addressed in Circular Letter 3.461 of July 24, 2009.

- 2009

Circular Letter 3461 of July 24, 2009: It consolidates the rules on the procedures to be adopted in the prevention and combat of the activities related to the crimes provided for in Law 9.613 of March 3, 1998.

Circular Letter 3462 of July 24, 2009: It amends the Regulation of International Exchange Market and Capitals (RMCCI).

- 2008

Circular Letter 3342 of October 2, 2008: It provides on the communication of financial movements connected to terrorism and its financing.

CVM Instruction 463 of January 8, 2008: It amends Instruction 301/99 which regulates the provisions of Law 9.613/98, under the autarchy jurisdiction.

- 2007

Circular Letter 3339 of July 2, 2007 (Revoked by 3.461): It provides on the procedures to be observed by multiple banks, commercial banks, savings banks, credit cooperatives and savings and loans associations for the follow up of financial movements of politically exposed persons.

- 2006

Circular Letter 3234 of May 15, 2006: It announces recommendations referring to operations or proposals involving non-cooperating countries as to prevention of money laundering.

COAF Circular Letter 014 of November 22, 2006: Extinction of list of countries considered as non-cooperating in the fight against money laundering.

- 2005

BACEN Circular Letter 3280 of March 9, 2005: It announces, among other information and rules, the securities referring to Iraq, Afghanistan and Liberia, appearing in the Regulation on countries with special exchange provisions of the RMCCI – Regulation of International Exchange and Capitals Market.

BACEN Circular Letter 3157 of January 12, 2005: It announces recommendation for intensified monitoring of financial transactions with non-cooperating countries as to the prevention and repression of money laundering crimes.

- 2004

BACEN Circular Letter of December 1st, 2004: It announces instructions for communication, by means of transaction PCA 500 of SISBACEN- Brazilian Central Bank System, of operations and situations with signs of crimes of money laundering and informs that the responsibility of information provided shall be upon the appointed Director, in form of BACEN Circular Letter 2852.

- 2003

CVM Office Letter of October 30, 2003: It amends and adds provisions to Law 9613 of March 03, 1998 which provides on crimes of money laundering or concealment of assets, rights and valuables;

Circular Letter 3.100 of July 07, 2003: It announces recommendations referring to the operations or proposals involving non-cooperating countries as to the prevention and repression of money laundering;

Circular Letter 3098 of June 11, 2003: It establishes the need of records of deposits and withdrawals in cash, as well as requests of provisioning of withdrawals;

CVM Normative Instruction 387 of April 28, 2003 and respective amendments made by Normative Instructions 395 and 419: It establishes rules and procedures to be observed in operations carried out with securities, on the floor (trade) and in electronic negotiation systems and registration in stock exchanges and commodities and futures exchanges and other provisions.

- 2002

Federal Revenue Office Normative Instruction 188: It publishes the countries or dependencies that are considered tax havens.

SUSEP Circular Letter 200: It provides on the identification of customers and maintenance of records, the list of operations and transactions denoting signs of money laundering in the security area.

BACEN Resolution 2953 of April 25, 2002: It amends rules related to the opening, maintenance and transactions of deposit accounts and provides on the retaining of correspondents in the Country by financial institutions.

- 2001

BACEN Circular Letter 3030;

- 2000

CMN Resolution 2747 of June 28, 2000: Ir amends rulesl related to opening and closing of deposit accounts, the rates and fees of services to checks (amends Articles 1, 2 and 12 of Resolution 2025).

- 1999

CVM Guidance Opinion 31 of September 24, 1999: It announces to the customers the need of veracity of information provided.

- 1998

CMN Circular Letter 3006 of December 5, 1998: It establishes complementary procedures and conditions for the opening, maintenance and closing of deposit accounts (it conditions the opening of deposit accounts to the enrollment in CPF/MF).

BACEN Circular Letter 2826 of December 4, 1998: It announces operations and situations that may configure signs of occurrence of crimes provided for in Law 9613, and it establishes procedures for communication thereof to BACEN.

BACEN Circular Letter 2852 of December 3, 1998 (Revoked by 3.461): It provides on the procedures to be adopted in the Prevention of activities related to the crimes provided for in

Law 9.613 and it regulates the obligations imposed on the financial institutions so that money-laundering cases may be duly identified:

Law 9613 of March 3, 1998: It typifies the crime of money laundering or concealment of assets, rights and valuables, and institutes actions that assign more responsibility to entities forming the financial system, also creating within the scope of the Ministry of Treasury, the Financial Activity Control Council ("COAF").

- 1996

Tax Adjustment Law 9.430 of December 27, 1996: It provides on the federal tax legislation, the contributions to social security, the administrative Consulting process and other provisions.

- 1993

BACEN Resolution 2025 of November 24, 1993 (amended by Resolutions 2953 and 2747): It amends and consolidates the rules and standards related to opening, maintenance and movement of deposit accounts.

8.2. Bibliography:

- "As Quarenta Recomendações", do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (FATF/GAFI);
- "As Nove Recomendações Especiais", do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (FATF/GAFI).