



# PCG\_005 Preventing and Combating Money Laundering, Terrorism Financing, Proliferation Financing, Fraud Financing and Anti-Bribery

Effective since August 9<sup>th</sup> 2024

## Purposes

This policy establishes guidelines for the companies of the Votorantim Financial Conglomerate (hereinafter "The Conglomerate") related to fighting against money laundering and terrorism financing, the proliferation of weapons of mass destruction, fraud and anti-bribery, in line with the Code of Conduct and the Integrity Program, formalizing Senior Management's commitment to the effectiveness and continuous improvement of this policy, procedures and controls presented here.

## Guidelines

### 1. General Attributes

- 1.1. Repudiates acts of corruption, bribery, extortion, kickbacks, fraud, money laundering money, terrorist financing and weapons of mass destruction, or any other illicit acts.
- 1.2. Adopts procedures, in relationships with public entities, to inhibit the practice of acts of corruption.
- 1.3. Prevents the practice of money laundering, terrorist financing, proliferation of weapons of mass destruction and corruption in carrying out business in the country and abroad, in accordance with national legislation and the one in force in each country where it operates.
- 1.4. It acts in line with the international commitments assumed by the Brazilian Government with regards to preventing and combating crime money laundering, terrorist financing, proliferation of weapons mass destruction and corruption, in compliance with the legislation in force in the country.
- 1.5. The Conglomerate adopts procedures in the development of products and services, to inhibit their use for illicit practices linked to money laundering money, terrorist financing, proliferation of weapons of destruction mass and corruption.
- 1.6. Stimulates and participates in joint actions within the scope of the Brazilian Financial System, to prevent and combat money laundering, to finance the terrorism, proliferation of weapons of mass destruction and corruption.
- 1.7. Use settings established by law for recording transactions and identification of those saved with money laundering fraud, regulation of weapons of mass destruction or funding for terrorism. To do so, invests in the development or acquisition of systems automation of monitoring of transactions carried out.
- 1.8. Uses specific parameters for transaction monitoring financial institutions that could constitute signs of corruption.
- 1.9. Adopts due diligence procedures to mitigate the risks of money laundering, terrorist financing, proliferation of weapons mass destruction and corruption, depending on the activity, jurisdiction and agents involved.

1.10. Adopts restrictive measures regarding the conduct of business and maintaining business relationships with customers, suppliers and partners when circumstances reveal evidence of involvement in acts linked to money laundering, terrorist financing, proliferation of weapons mass destruction or corruption, in compliance with current legislation.

1.11. Conditions the hiring and maintenance of banking correspondents and non-banks, to provide customer service services to our customers and users, the absence of administrative or judicial conviction in the sanctions of the Law 12,846/2013 and verification of the provisions of Laws 9,613/1998 and 13,810/2019.

1.12. Requests that banking correspondents who provide services for the Bank carry out training in preventing and combating money laundering and to terrorist financing.

1.13. Conditions the maintenance of a correspondence relationship with other banks to the existence, within those banks, of mechanisms to prevention of money laundering, terrorist financing, proliferation of weapons of mass destruction and corruption.

1.14. Considers, in maintaining business relationships with partners and suppliers, the existence, within those third parties of mechanisms to corruption prevention and acculturation on money laundering prevention and terrorist financing.

1.15. The Conglomerate has specific jurisdiction (Controls and Risks Committee - CCR) to deal with and deliberate on matters of greater risk, relating to preventing money laundering and combating terrorist financing, and corruption.

1.16. Adopts procedures to monitor the prevention process and combating money laundering, proliferation of weapons of destruction in mass and terrorist financing by senior management, ensuring its commitment to the effectiveness and continuous improvement of policy, procedures and internal controls required.

1.17. Adopts a procedure for closing activities when throughout the relationship, a client presents atypicalities related to money laundering, terrorist financing, proliferation of weapons mass destruction and corruption.

1.18. The Conglomerate maintains training and dissemination programs of a culture of preventing money laundering, of combating the financing of terrorism, proliferation of weapons of mass destruction and corruption, in accordance with legal requirements and best market practices. The program is applied to employees, bank correspondents and third parties relevant.

1.19. The Conglomerate maintains a specialized structure responsible for monitoring all customer transactions, with a focus on preventing money laundering, terrorist financing, proliferation of weapons mass destruction and corruption. Monitoring considers the profile, origin and destination of resources and the financial capacity of customers. Additionally, the Conglomerate maintains a communication channel designed to receive information or whistleblow, including anonymous ones, from any employee or third party, regarding suspicious operations or proposals, identified in the conduct of business.

1.20. Investigates signs and reports of acts of corruption carried out by agents direct or third parties for the benefit or interest of the Bank, against the administration public, in accordance with current legislation.

1.21. Investigates signs and reports of acts of corruption committed by clients, partners and suppliers, against the assets, principles and commitments assumed by the Bank, in accordance with current legislation. At the institutional level, the treatment of cases of signs/reports of corruption is carried out by the areas competent authorities, being the prerogative of the Integrity Program.

- 1.22. Preserves the identity of anonymous whistleblowers.
- 1.23. Repudiates any acts of reprisal or retaliation attempted against whistleblowers in good faith, who choose to identify themselves.
- 1.24. Adopts protection measures for employees who report in good faith, in relation to facts arising from the whistleblowing.
- 1.25. Evaluates, in the analysis of operations, the instruments used, the way of completion, frequency, parties and amounts involved, financial capacity and the customer's economic activity and any indication of irregularity or illegality involving the client or its operations, with a view to detecting evidence of money laundering, terrorist financing or corruption.
- 1.26. The Conglomerate keeps copies of the documentation of the customers, as well as recording operations and laundering prevention analyzes of money made, the financing of terrorism, the proliferation of weapons of mass destruction and corruption, maintained in accordance with the standard's internal regulations, laws and regulations of the countries where it operates.
- 1.27. The Conglomerate strictly observes the recommendations of the Financial Action Task Force – FATF/GAFI which specifies the list of countries with controls insufficient measures to prevent money laundering and the financing of terrorism, as well as restrictive lists issued by other bodies international crime prevention agencies, in addition to not maintaining a relationship, nor carry out financial transactions with entities or people designated, as well as taking steps to carry out, timely and without prior notice, the unavailability of assets of individuals and legal entities sanctioned by the United Nations Security Council.
- 1.28. The Conglomerate does not accept transfers of funds by way through anonymous bank accounts or those linked to holders fictitious.
- 1.29. We do not authorize any type of facilitation payment.
- 1.30. We cooperate with public authorities in investigations related to acts harmful to government administration, which arise from our activities, observed to current legislation.
- 1.31 The Conglomerate adopts the best practices for fighting against corruption in relationship with its parties, customers, suppliers, employees, and government, and not admits any types of activities carried out by them against the government administration, national or foreign.
- 1.32. The Conglomerate provides for the application of a policy of consequences (among which, application of disciplinary measures and/or administrative removal) to all employees, including Senior Management, when applicable, in cases of non-compliance with regulations and internal policies, including but not limited to those relating to the commission of practices considered illicit acts, such as: acts of corruption (within the scope of the relationship with the public administration and/or private entities), money laundering, proliferation of weapons of mass destruction and terrorist financing.
- 1.33. Performs internal risk assessment with the aim of identifying and measuring the risk of using our products and services for illicit practices money laundering, terrorist financing, proliferation of weapons of mass destruction and corruption, considering the risk profile: of customers; of the Conglomerate, including the business model and the geographic area of operations, transactions, products and services, covering all distribution channels and the use of new technologies; and activities carried out by employees, partner institutions, suppliers and correspondents. Through compliance with the provisions of the matrix of products and services, and sequentially regarding the provisions in the ABR matrices AML (customers, suppliers, and partners), the guidelines are presented necessary for

the implementation of specific procedures for collection, verification, validation and updating of registration information for customers, employees, partners and relevant third parties.

1.34. The Conglomerate has specific regulations that establish the roles and responsibilities for compliance with the obligations concerning the prevention of money laundering, terrorist financing, proliferation of weapons mass destruction and corruption.

1.35. The Conglomerate evaluates, at least annually, the effectiveness of the policy, procedures, and internal controls to prevent money laundering and records in a specific report. This report is sent to both the Auditing Committee and the Board of Directors for appreciation.

## **2. Know Your Customer – KYC**

2.1. The Conglomerate establishes mechanisms for identification, classification, and qualification, in addition to validating and updating customer registration data, as well as the origin and constitution of its financial capacity. The collection of this information should allow the customer to evaluate it as part of the procedures relating to the “Know Your Customer” principle and transactional monitoring.

2.2. Conglomerate adopts restrictive measures regarding the carrying out of business and maintaining a business relationship with the customer when circumstances reveal evidence of money laundering, financing of terrorism, proliferation of weapons of mass destruction and corruption.

2.3. The Conglomerate holds no ties with corporations belonging to any financial institution established in places where a physical presence is inexistent, and which is not integrated to a financial group subject to actual local supervision.

2.4. The Conglomerate follows specific rules for the purpose of authorizing the start and continuation of any business relationship with any Person Politically Exposed – PEP, as well as analysis of the chain of corporate participation until the identification of the natural person characterized as the ultimate beneficiary owner, in accordance with the legal requirements.

2.5. We condition the initiation and maintenance of the business relationship with clients Politically Exposed Persons to authorization of a higher authority than that which indicated the relationship.

## **3. Know Your Partner – KYP**

3.1. The Conglomerate defines and maintains standards and mechanisms for due identification, classification, qualification and grounded knowledge of its partners and its activities, conditioning the existence of mechanisms relating to the prevention of the crime of money laundering, financing of terrorism, proliferation of weapons of mass destruction and the corruption, in the control environment of these partners, when applicable.

## **4. Know Your Employee – KYE**

4.1. The Conglomerate defines and maintains standards relating to knowledge of its employee, with a focus on preventing and combating money laundering, financing of terrorism, proliferation of weapons of mass destruction and the corruption, which include criteria for hiring, identification, classification, qualification, and verification of the conduct of these employees and relevant third parties.

## **5. Know Your Supplier – KYS**

5.1. The Conglomerate defines and maintains standards and mechanisms for due identification, classification, qualification, and grounded knowledge of its suppliers and service providers in accordance with the purpose of the relationship.

5.2. Instructs our suppliers to adopt criteria for hiring and monitoring employee conduct, focusing on prevention and combat money laundering and terrorist financing, weapons proliferation of mass destruction and corruption.

## **6. Know your Banking Agent**

6.1. The Conglomerate defines and maintains standards and procedures for identification, classification, qualification, and approval of banking agents, national and international, with the aim of preventing carrying out business with un reputable institutions or those with suspected activities illicit.

6.2. Adopts practices and controls to prevent and combat money laundering, proliferation of weapons of mass destruction, and the financing of terrorism in line with the Wolfsberg Group principles for correspondent banks.

## **7. Fraud Prevention**

7.1 The Fraud Prevention Strategy Area is responsible for implementing strategies and rules, to prevent and detect atypical transactions, mitigating financial damage to customers and the financial institution. Adopts a structure that aims to support and ensure integrity and confidentiality in business areas in its product and service offerings. It is the responsibility of all employees to prevent and combat fraud.

7.2 The Fraud Prevention Strategy Area adopts best fraud practices market and controls, with parameters established in accordance with laws and current regulations, through a model based on the 4 main pillars of fraud prevention: prevention, detection, recovery, and repression. The pillars applied aim to ensure security and monitoring in the following items: evaluations of new products and services, due diligence of partners who contract BaaS (Banking as a Service), access/login to the application and in My BV (internet banking), onboarding (account, card, and loan products), financial and non-financial transactions (account and card), recovery and dispute.

## **8. Notice to Authorities**

8.1. The Conglomerate conducts, with strict confidentiality, including in relation to customers, the registration, analysis, and communication processes to the authorities' competent authorities of financial operations with signs of money laundering, proliferation of weapons of mass destruction, or financing of terrorism, as well as processes relating to the investigation of suspected acts of corruption.

8.2. Communicates, to the competent authorities, the operations, or proposals for operations that, in accordance with current legislation, indicate evidence of money laundering, financing terrorism, proliferation of weapons of destruction mass and corruption.

8.3. Submits the program to prevent and combat money laundering, to the financing of terrorism, financing of the proliferation of weapons of mass destruction and corruption, audit firm assessment independent and internal audit. The frequency of reviewing the processes of combating money laundering and terrorist financing, by auditing internal, will be based on the risk map prepared by that area.

## **9. Maintenance and Storage of Information and Records**

9.1. The maintenance of records of services, financial operations, procedures for the identification of suitability, dossier of analysis of operations and suspicious situations is carried out for a minimum period of 10 years, counted from the first day of the year following that of the operation termination of the business relationship, or termination of the contractual relationship for suppliers, outsourced service providers, partners, employees, customers, and operations.

9.2 Records relating to prevention procedures and combating money laundering, terrorist financing, proliferation of weapons of mass destruction and corruption in accordance with the current legislation.

9.3. Records are kept of all operations carried out, products and services contracted, including withdrawals, deposits, contributions, payments, receipts, and transfers of funds.

9.4. The records of each operation contain the type, value, date of completion, origin, and destination of resources.

## **10. Responsibility**

10.1. Area responsible for preparation, updating and regulation: Executive Management of the AMLTFP Area.

## **11. Definitions**

11.1 Ultimate Beneficiary Owner: Is the natural person who ultimately holds control of the legal entity or on behalf of which a transaction is being carried out. The representative, attorney and agent who exercise de facto command over the activities of the Legal Entity are also considered final beneficiaries.

11.2. Conglomerate: Banco Votorantim S.A. and its controlled companies.

11.3. Corruption: Consists of offering, requesting, or receiving, directly or indirectly, upon request or not from people, public or private companies and third sector organizations, undue advantages of any nature in exchange for carrying out or omitting acts inherent to their duties, aiming to benefits for yourself or third parties. Law 12,846/2013 addresses this topic.

11.4. Suppliers: These are individuals or legal entities, public or private, national, or foreign, who provide products, services, or intermediary agents to the Conglomerate.

11.5. Financing the proliferation of weapons of mass destruction: Allocation of resources with the aim of providing financial support, providing, or gathering funds to be used for the proliferation of weapons of mass destruction, such as: nuclear, chemical, and biological or toxin weapons.

11.6. Terrorist Financing: Terrorist financing is considered the transfer of funds of any nature (legal or illicit) to people or groups that carry out acts of terrorism.

11.7. Money laundering: It is the practice used to hide or disguise the origin of money arising directly or indirectly from illicit activities.

11.8. Facilitation payment: Payment of small amounts of money or promises of other advantages for the personal benefit of a public agent, with the aim of speeding up a certain process.

11.9. PEPs - Politically Exposed People: People referred to as "Politically Exposed People (PEP)" are those who occupy public positions and functions listed in the AML/CTF rules published by regulatory and supervisory bodies, Resolution n°29 of 12/7/2017 Brazilian UIF deals with this topic.

11.10. AML/CTFP: Preventing and Combating Money Laundering and the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction.

11.11. Bribery: Consists of convincing a specific person to commit an illegal act by receiving an advantage, benefits, money or material goods for themselves or others.

1.12 Fraud: Act of cunning deception, bad faith, dishonest action with the intention of deceiving, corrupting, obtaining an advantage for one's own benefit, deceiving, subtract financial resources. It can also be characterized by fakes of documents, statements, resulting in loss to people and institutions.

*The guidelines contained in this policy are regulated and operationalized through normative instructions and procedures that define rules and processes for correct compliance with the policies.*