ITAÚ UNIBANCO HOLDING S.A.

CNPJ 60.872.504/0001-23 Publicly Listed Company NIRE 35300010230

CORPORATE POLICY FOR PREVENTION AND FIGHT AGAINST ILLEGAL ACTS

OBJECTIVE

This policy for Prevention of Illegal Acts consolidates the principles and guidelines of Itaú Unibanco Holding S.A. (Itaú Unibanco) for the prevention and fight against money laundering, terrorism financing, fraud, and casualties, in line with the current legislation and regulations, and with the best Brazilian and international market practices.

TARGET AUDIENCE

This policy applies to Itaú Unibanco and its subsidiaries and affiliates, in Brazil and abroad.
In case of conflict between this policy and local legislations of jurisdictions where the overseas representations are located, the stricter standard shall prevail, provided it does not violate the local legislation.

INTRODUCTION

Financial institutions play a key role in Preventing and Fighting against Illegal Acts, i.e. all human actions or omissions that are conscious and intended to the practice of criminal misconduct notably to money laundering, terrorism financing, corruption, fraud and casualties.
Money laundering is the concealment or disguise of the nature, source, location, disposition, transfer or ownership of property, rights or values arising, directly or indirectly, from criminal offense.
Terrorism financing is when someone, directly or indirectly, by any means, provides financial support, provides or collects funds with the intention to use them for or knowing that they will be used, wholly or partially, by terrorist groups for the practice of terrorist acts.
Corruption consists in suggesting, offering, promising, granting, requesting, demanding, accepting or receiving, directly or indirectly, whether demanded or otherwise, to/from persons or companies from the public and private sectors, and third sector organizations, as well as between persons, companies and organizations from different countries, undue advantages of any nature (financial or otherwise) in exchange for the performance or omission of acts inherent in their attributions, operations or activities for the Conglomerate, or aiming at benefits for themselves or for third parties.
Fraud refers to any unlawful activities, attitudes or actions that are intended to mislead or deceive someone, in bad faith and for their own benefit or that of others. Example: omission/manipulation of information, allocation of amounts, adulteration of documents, records and financial statements.
Casualty refers to atypical events that result in losses or damages to Itaú Unibanco, such as robbery to branches and customers, extortion by kidnapping, theft, accident, break-in, among others.
Embargo is the total or partial prohibition of commercial transactions with a particular country, established by a jurisdiction or an international organization to retaliate certain actions adopted by the embargoed jurisdiction, of an economic, political, social or warlike nature, which are contrary to the principles established by the jurisdiction or international body imposing the embargo. Some jurisdictions or international organizations also establish restrictions on certain individuals or companies that engage in illicit activities.
The biggest challenge is to identify and restrain increasingly sophisticated transactions that seek to conceal or disguise the nature, person responsible, origin, location, disposition, transfer or ownership of assets, rights and/or values arising directly or indirectly from illegal activities.
Itaú Unibanco has established this policy in order to avoid its intermediation of illegal activities, and to safeguard and protect its name, reputation and image before employees, customers, strategic partners, suppliers, service providers, regulators and society, through a governance structure based on transparency, strict compliance with rules and regulations, and cooperation with law enforcement and judicial authorities. The institution also seeks to continually align itself with the best Brazilian and international practices for prevention and fight against illegal acts, through investments and continuous training of its employees.

ROLES AND RESPONSIBILITIES

Board of Directors

Approve the Institution's guidelines for prevention of illegal acts and any amendments thereto.

Audit Committee

Supervise the Corporate Program for the Prevention of Illegal Acts based on information compiled and presented by the functions, as well as other mechanisms at its disposal.

High Operational Risk Committee (*Comissão Superior de Risco Operacional* - CSRO)

- Define and propose to the Board of Directors the Institution's guidelines for prevention of illegal acts;
- Analyze the results of processes and activities of the program to prevent illegal acts;
- Deliberate on situations not provided for in this Policy.

Credit Risk, Modeling Department and Preventing Laundry Money and Fighting Terrorist Financing (*Diretoria de Risco de Crédito, Modelagem e Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo (DRCMPLD*)

- Manage the Anti-Money Laundering and Counter Terrorism Financing Program of Itaú Unibanco in Brazil and abroad;
- Improve the quality and effectiveness of its processes and responsibilities over Itaú Unibanco's Anti-Money Laundering and Counter Terrorism Financing processes;
- Perform a prior assessment of the risks of money laundering and terrorism financing in products and services;
- Define guidelines and minimum criteria for risk rating relating to money laundering and terrorism financing of customers, employees, business partners, suppliers, and service providers;
- Monitor and diagnose different types of money laundering, in order to anticipate trends and propose preventive and countering solutions;
- Validate the Itaú Unibanco's Anti-Money Laundering and Counter Terrorism Financing procedures mentioned in the business units' documents;
- Periodically report to the Audit Committee material facts relating to Anti-Money Laundering and Counter Terrorism Financing of Itaú Unibanco.

Corporate Security Department (*Diretoria de Segurança Corporativa* - DSC)

- Manage the Itaú Unibanco's Program for the Prevention of Illegal Acts in Brazil and abroad;
- Improve the quality and effectiveness of its processes, ensuring the integrity, availability and confidentiality of information; the physical security of employees, customers and executives, and property; and the responsibilities for the processes for the Prevention of Illegal Acts;
- Performs a prior assessment of the risks of fraud in products and services;
- Define guidelines and minimum criteria for risk rating relating to fraud of customers, employees, business partners, suppliers, and service providers;
- Monitor and diagnose different types of illegal acts, in order to anticipate trends and propose preventive and countering solutions;
- Validate the procedures for the Prevention of Illegal Acts mentioned in the documents of the business units;
- Periodically report to the Audit Committee material facts relating to illegal acts;
- Manage extreme, unique and rare events that threaten the organization's strategy, goal and viability, its image and/or reputation.

Business Units

- As the first line defense, define and implement procedures and controls compliant with this policy, with the guidance of DRCMPLD and DSC, considering the risk assessment at the beginning and during maintenance of a relationship with natural and legal persons, in those processes that are performed by them and are under their direct responsibility;
- Ensure that employees conduct training on prevention and fight against money laundering, terrorism financing, fraud, and casualties.

Legal Department

- Analyze the legal and regulatory requirements on Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF) and their impact on the business;
- Assist business managers in developing action plans for the implementation of AML/CTF controls;
- Support the assessment of risks and measures required to address transactions suspected of involving money laundering, fraud and casualties, from a legal perspective.

Operational Risk Directorate

Certifies the efficiency of the control environment through Monitoring Programs, control tests, reporting residual risk independently as defined in internal policy.

Internal Audit

As the third line defense, annually assess the effectiveness of the Program for Prevention and Fight Against Illegal Acts and propose measures to improve it.

5 CORPORATE PROGRAMS FOR PREVENTION AND FIGHT AGAINST ILLEGAL ACTS

Customer Identification

Set of actions to be adopted for customer identification purposes, which includes capturing and confirming information, periodical updating and storage of registration data.

Itaú Unibanco does not allow the opening and maintenance of anonymous accounts.

Know Your Customer - KYC

A set of actions that shall be taken to ensure the identity and financial activity of customers, as well as the origin and making of their net worth and financial resources.

The more accurate the information collected and registered at the beginning of the relationship, the greater the ability to identify illegal acts.

For cases that require Special Attention, such as the relationship with Politically Exposed Persons (PEPs) and customers where it was not possible to identify the final beneficiary, specific rigorous analysis procedures are adopted.

It is mandatory to have a higher clearance for the beginning of the relationship with natural persons or legal persons classified as PEPs and for the maintenance of the existing relationship when the client becomes part of this situation, as defined in internal policy.

Know Your Partner - KYP

Partners are the Legal Entities that enter into business agreements or arrangements with one or several companies of the Itaú Unibanco conglomerate and that meet the requirements established in the internal policy.

Know Your Partner is a set of rules, procedures and controls that shall be adopted for identification and acceptance of business partners, including correspondent banks in the country and abroad. Its purpose is to prevent business with unreliable counterparties or counterparties suspected of involvement in illegal activities, as well as to ensure that they have adequate AML/CTF procedures as specific internal policy, where applicable.

Itaú Unibanco does not allow relationship with the so-called Shell Banks, that is, banks incorporated in a jurisdiction where there is no physical presence and which are not integrated with any regulated financial group.

Know Your Supplier - KYS

Set of rules, procedures and controls that shall be adopted to identify and accept suppliers and service providers, in order to provide adequate employee awareness so as to prevent the engagement of unreliable companies or companies suspected of involvement in illegal activities.

For those customers, partners, suppliers, and service providers who present greater risk associated with illegal acts, stricter identification and due diligence criteria shall be applied, and the relationship shall be approved by a higher hierarchical level.

Know Your Employee - KYE

Set of rules, procedures and controls that shall be adopted for selection, hiring, and monitoring of any situations that may characterize any type of risk or deviation, for the purpose of preventing money laundering, terrorism financing and other illegal acts.

Evaluation of New Products and Services

New products and services shall be evaluated in advance, from the AML/CTF perspective, according to the guidelines established in the internal policy.

Monitoring of Transactions

Financial transactions and transactions conducted by customers, whether employees or not, shall be monitored for situations that may imply money laundering or terrorism financing. For cases that require Special Attention, such as relationship with Politically Exposed Persons (PEP) and customers for which it is not possible to identify the final beneficiary, stricter analysis procedures are adopted. Monitoring considers the profile, origin and destination of funds and the customers' financial capacity.

Communication of Suspicious Transactions to Regulatory Agencies

Transactions, situations or proposals containing evidence of money laundering or terrorism financing shall be reported to the relevant regulatory agencies, where applicable, in compliance with legal and regulatory requirements. Communications submitted in good faith do not entail civil or administrative liability to Itaú Unibanco, nor to its management personnel and employees.

Information about these communications is restricted and shall not be disclosed to customers and/or third parties.

Training

The AML/CTF training program is continuous and shall be applied to all eligible employees, in order to:

- deepen the knowledge that management personnel and employees have of legal and regulatory requirements and responsibilities, as well as of the corporate AML/CTF guidelines;
- enable administrators and employees to identify, prevent, address and communicate situations of risk or with indications of money laundering or terrorism financing in the businesses conducted.

The program shall be applied through institutional actions and in the business units, including in-class and distance learning (e-learning), lectures, teleconferences, audio conferences, campaigns, communications, publications, among others.

Prevention and Fight Against Fraud and Casualties

The prevention and fight against fraud is the responsibility of all employees. Fraud can be classified as:

a) Disciplinary Breach and Violation of the Itaú Unibanco Code of Ethics and the Corporate Integrity and Ethics Policy, committed in group or separately:

- Adoption of practices not authorized by the company;
- Misconduct;
- Breach of secrecy and conflict of interest.

b) Non-compliance with Legal and Regulatory Rules:

All situations identified relating to non-compliance with legal and regulatory rules that put at risk the image, net worth or continuity of the Organization.

c) Illegal Acts of Any Nature:
All forms of illegal acts (crimes or criminal offenses) provided for in the Brazilian Criminal Law and which may cause direct or indirect losses to the Bank, its employees, customers or third parties. Example:
- Forgery;
- Adulteration;
- Embezzlement (in all its forms);
- Fraudulent opening of an account (fraudulent accounts) or acquisition of products;
- Misappropriation;
- Theft;
- Robbery;
- Burglary;
- Break-in;
- Social Engineering;
- Extortion by kidnapping;
- Fraud through electronic and non-electronic channels;
- Scams.

Model of Actions for the Prevention and Fight Against Fraud and Casualties
Risk Assessment at the Beginning of Relationship
Service and product acquisition processes shall include procedures to prevent and mitigate the risk of fraud at the beginning of a relationship with the proponents.

Prevention and Fight Against Internal Fraud
Itaú Unibanco adopts specific measures to prevent fraud involving its employees, through guidelines and control procedures intended to prevent and detect irregular activities.

Prevention and Fight Against Accounting Fraud
Itaú Unibanco adopts measures to safeguard the quality and integrity of its financial statements, through internal controls, Internal and External Audits, and supervision by the Audit Committee.

Risk Assessment for New Products and Services
New products and services shall be evaluated in advance, from the fraud prevention perspective, according to the guidelines established in internal Policy.

Monitoring of Transactions
The products and services acquired by customers shall be monitored for detection and verification of atypical situations or suspected fraud or other illegal acts.
Treatment of Incidents
Suspicious or confirmed situations shall be addressed in order to determine responsibilities and required measures.
The procedures and decisions made during treatment of incidents shall be formalized in order to generate subsidies to legal proceedings.
Training and Awareness
The Fraud and Casualty Prevention training program is continuous and shall be applied to all eligible employees, in order to:
- deepen the knowledge that management personnel and employees have of external and internal rules on prevention and fight against fraud and casualties;
- enable management personnel and employees to identify, prevent, treat and report suspicious situations related to fraud and other illegal acts.
The program shall be applied through institutional actions and in the business units, and it may include in-class and distance learning (e-learning), lectures, teleconferences, audio conferences, campaigns, communications, publications, among others.

MAINTENANCE AND SAFEGUARDING OF INFORMATION AND RECORDS
The information and records on transactions and services shall be kept in their original form or in electronic files, according to deadlines and responsibilities established by current legislation.

TRANSPARENCY IN RELATIONSHIPS WITH CUSTOMERS
Itaú Unibanco's customers have access, through various channels, to their financial information, including invested funds, products acquired, and limits granted. Thus, the customers themselves are strong and active partners in preventing and fighting Illegal Acts.
Furthermore, Itaú Unibanco alerts its customers on an ongoing basis, through relationship channels, about the possibility of Illegal Acts and the actions and measures that must be taken to prevent them.

ILLEGAL ACT COMMUNICATION CHANNELS

The management personnel and employees of Itaú Unibanco shall immediately communicate situations with indication or evidence of illegal acts, identified in the prospection, negotiation or during the relationship, using the following channels, by physical or electronic means:

Situations Related to Money Laundering or Terrorism Financing
In Brazil, communications shall be sent to the Supervising Department of Prevention of Money Laundering:
- Phone number: 0800-723-0010, Option 4;
- Retail Bank Phone: 0300 100 0341 say Money Laundering
- Internal email: MONEY LAUNDERING PREVENTION.

At the international units, the communications shall be sent to the local channels or Compliance Officers of the Unit.

Situations Related to Fraud and Other Illegal Acts
In Brazil, communications shall be sent to the Supervising Department of Fraud Investigation and Prevention:
- External phone number: 0800-723-0010
- Internal phone number: 0300 100 0341
- Website: www.itau.com.br/atendimento-itau/para-voce/denuncia;
- Internal email: inbox Inspetoria [Audit Dep.];
- External email: inspetoria@itau-unibanco.com.br and fornecedor_relatos@itau-unibanco.com.br;
- Courier: addressee: Investigation Manager/São Paulo;
- Address:
- C/O Investigation Office
- Rua Volkswagen, 10 Jabaquara, São Paulo – SP – CEP 04344-020

At the international units, the communications shall be sent to the local channels or Compliance Officers of the Unit.
These channels shall be disclosed and may also be used by customers, service providers and the general public.

Audit Committee:
- External email: comitê.auditoria@itau-unibanco.com.br
- Mail address:

A/C Comitê de Auditoria do Itaú Unibanco Holding S.A.
Praça Alfredo Egydio de Souza Aranha, 100
Torre Olavo Setubal – Piso PM
CEP [ZIP Code] 04344-902 – SP – São Paulo

In international units' communications can be sent to the channel established by the local Audit Committee, when it exists, or to the channel of the Itaú Unibanco Audit Committee detailed above.
These channels shall be disclosed and may also be used by customers, service providers and the general public.

PROTECTION OF WHISTLEBLOWERS
Management personnel and employees may not Retaliate those who, in good faith, denounce or express a complaint, suspicion, doubt or concern regarding possible violation of the guidelines of this Policy; and provide information or assist investigations relating to possible violations.
Management personnel and employees shall keep confidential any information on investigations of possible violations of the guidelines of this Policy.
The Whistleblower Channels accept anonymous reports and preserve the anonymity of whistleblowers.
Disciplinary sanctions shall be applied to the management personnel or employees who attempt to retaliate or retaliate those who, in good faith, communicate possible violations of the guidelines of this Policy.
Disciplinary sanctions shall also be applied to management personnel or employees who are known to have used bad faith to communicate possible violations of the guidelines of this Policy or have communicated facts that are known to be false.

SANCTIONS
Failure to comply with legal and regulatory provisions subjects the management personnel and employees to sanctions ranging from administrative penalties to criminal penalties for money laundering, terrorism financing, fraud, casualties, corruption, and other illegal acts.
Negligence and voluntary noncompliance are considered noncompliance with this policy, the Code of Ethics, and the Corporate Integrity and Ethics Policy, and may be subject to the disciplinary measures provided for in the Institution's internal regulations. Disciplinary Standards.

RELATED DOCUMENTS
This policy shall be read and construed jointly with the following documents:
Related External Rules
Decree-Law No. 2.848/40 - Brazilian Penal Code.

Circular Letter No. 3.430/10 of the Central Bank of Brazil.
Circular Letter No. 3.542/12 of the Central Bank of Brazil.
Circular Letter No. 3.461/09 of the Central Bank of Brazil.
Circular Letter No. 3.462/09 of the Central Bank of Brazil.
Circular Letter No. 3.517/10 of the Central Bank of Brazil.
Circular Letter No. 3.583/12 of the Central Bank of Brazil.
Circular Letter No. 445/12 of Brazil's Private Insurance Supervisory Office.
Circular Letter No. 3.654/13 of the Central Bank of Brazil.
Rule No. 301/99 of the Brazilian Securities and Exchange Commission and respective amendments.
Rule No. 18/14 of Brazil's Supplementary Pension Supervisory Office.
Federal Laws No. 9.613/98 and No. 12.683/12.
Anti-Corruption Law No. 12.846/13.
SARB Self-Regulatory Rule No. 011/2013 of the Brazilian Federation of Bank Associations.
Recommendations of the Financial Action Task Force (FATF).
Resolution No. 2.025/93 of the Brazilian National Monetary Council.
Resolution No. 2.747/00 of the Brazilian National Monetary Council.
Resolution No. 4.567/17 of the Central Bank
COAF Resolutions No. 006/99 and 021/12.
Wolfsberg Anti-Money Laundering Principles

Approved by the Board of Directors on October 31, 2019