CORPORATE POLICY FOR PREVENTION OF ILLEGAL ACTS

OBJECTIVE

This policy for Prevention of Illegal Acts consolidates the principles and guidelines of Itaú Unibanco Holding S.A. Conglomerate. (Itaú Unibanco) for the Prevention and Fight Against Money Laundering, Terrorism Financing, including Proliferation of Weapons of Mass Destruction (AML/CTF), fraud and casualties, in line with the current legislation and regulations and with the best national and international market practices.

TARGET AUDIENCE

This policy applies to Itaú Unibanco Conglomerate and its companies 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 Illegal Acts, including 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. Weapons of Mass Destruction Proliferation Funding, on the other hand, is constituted when someone, directly or indirectly, by any means, renders financial support, provides or collects funds with the intention of being used for the proliferation of weapons of mass destruction, which can be biological, chemical, and nuclear.

Corruption consists of 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. 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, outsourced 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.

RESPONSIBILITIES

Board of Directors (Conselho de Administração - CA)

Approve the Institution's guidelines for prevention of illegal acts and amendments thereto, with the commitment to the effectiveness and continuous improvement of the theme. In addition, the Board receives for its awareness the Internal Risk Assessment, the Effectiveness Assessment Report, as well as the action plans prepared to remedy deficiencies, and their respective Follow-up Report.

Audit Committee (Comitê de Auditoria - CAUD)

Supervise the Corporate Program for the Prevention of Illegal Acts based on information compiled and presented by the funcions, as well as other mechanisms at its disposal. Additionally, the Committee receives for its awareness the Internal Risk Assessment, the Effectiveness Assessment Report, as well as the action plans prepared to remedy deficiencies, and their respective Follow-up Report.

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.

Risks and Capital Management Committee (CGRC)

Support CA in the performance of its duties related to risks and capital management at Itaú Unibanco. Additionally, the Committee receives for its awareness the Internal Risk Assessment.

Credit Risk, Modeling and Anti-Money Laundering Department (DRCMPLD)

- AML/CTF Officer: Manage AML/CTF risks through information received from committees and, depending on the risk, cases submitted to its approval level; Approves Itaú Unibanco's Internal Risk Assessment; Approve the rules of procedure related to know your customer, employees, partners and outsourced service providers, as well as those for monitoring, selection and analysis; and Receive for awareness the partnership agreements with foreign-based financial institutions, as well as with third-party participants in payment arrangements in which Itaú Unibanco also participates, as set forth in current regulations;

- Ensure the implementation of the Anti-Money Laundering and Counter-Terrorism Financing Program of the Itaú Unibanco Conglomerate and its companies in Brazil and abroad;

- Prepare Itaú Unibanco's Internal Risk Assessment;

- Improve the quality and effectiveness of its processes and the responsibilities for the processes of Anti-Money Laundering and Combating Terrorism Financing at Itaú Unibanco, checking compliance with the policy, as well as remedying any verified deficiencies;

- Carry out a prior assessment of the risks of money laundering and terrorist financing in new products and services, including the use of new technologies;
- Define the guidelines and minimum criteria for classifying the risks of money laundering and terrorist financing for customers, employees, business partners, suppliers and outsourced service providers;

- Prepare and monitors the implementation of the risk-based approach in the processes, formalizing them in internal procedures, together with the criteria established for the generation of effectiveness indicators

- 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 (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;
- Perform a prior assessment of the risks of fraud in products and services, including the use of new technologies;
- 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 and support Units in Brazil and abroad

- As first line defense, define and implement procedures and controls in compliance with this policy and with the guidance of DRCMPLD and DSC, considering the risk assessment in the beginning and during maintenance of the relationship with individuals and legal entities, 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 Department

Certify the effectiveness of the control environment, through monitoring programs, assessment of effectiveness tests of controls, reporting the residual risk and monitoring of deficiencies independently verified, as defined in internal policy and prepare an Effectiveness Report as well as a Follow-up Report, submitting for approval and awareness of those responsible, following up on, at least, the deadline established by the regulation.

Internal Audit

As a third line of defense, the scope of internal audit covers the examination and assessment of the adequacy and effectiveness of the governance, risk management and internal controls of the organization, the quality in the execution of the responsibilities assigned to achieve the goals established by the organization, as defined in internal policy.

INTERNAL RISK ASSESSMENT

Itaú Unibanco will annually prepare its Internal Risk Assessment, a document aimed at identifying, measuring, and mitigating the risk of using its products and services in money laundering and terrorist funding practices.

Based on this Assessment, a risk-based approach is applied, a methodology that ensures that measures to prevent and mitigate money laundering and terrorist financing are proportionate to the risks identified, given that where the risks are higher, enhanced measures will be adopted to manage and mitigate such risks, and where the risks are lower, simplified measures will be used.

The detailing of the guidelines that underpin the risk-based approach is formalized in internal rule.

EFFECTIVENESS ASSESSMENT

Itaú Unibanco will prepare an annual Effectiveness Report to assess the effectiveness of AML/CTF policies, procedures, and internal controls. Action plans addressing the deficiencies identified through this Assessment shall be accompanied through the Follow-up Report. Additionally, the Effectiveness Assessment shall contain at least information describing the methodology adopted; the tests applied; the qualification of the evaluators and the deficiencies identified.

CORPORATE PROGRAM FOR PREVENTION OF ILLEGAL ACTS

With the purpose of facilitating the compliance with the guidelines of this policy and preventing its products and services being used in illicit activities, Itaú Unibanco established the Illegal Acts Prevention Program. Such program shall be applied, independently and autonomously, by the AML/CTF area in Brazil and in the International Units, as defined in internal rule.

The program shall contain at least:

Anti-Money Laundering and Counter Terrorism Financing

Policies and Procedures

Itaú Unibanco has a structured policies, rules and procedures to determine the bank's guidelines for combating illicit acts, which are compliant with local laws and regulations, as well as with the risk profiles of customers; of the institution; of operations, transactions, products and services; and employees, partners and outsourced service providers. These documents are periodically reviewed and approved according to the previously established approval authority and are available to all employees.

Customer Identification
It is a set of actions that must be adopted for the identification and qualification of clients, as well as their administrators and representatives, contemplating the capture, verification and validation of their information, with the objective of knowing their true identity. The registration data obtained must be updated and stored according to the established deadlines.

In addition, in order to carry out a complete identification and qualification of the client, the procedures defined in internal policies must be followed to obtain information, which allows verifying his/her condition as a Politically Exposed Person (PEP), as well as the analysis of the corporate chain until the identification of the natural person characterized as the final beneficiary.

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

Know Your Customer - KYC

It is a set of actions that shall be taken to ensure the identity and financial activity of customers, as well as the origin and constitution of their net worth and financial resources. The collection of this information should allow the assessment of the financial capacity of the client. The more accurate the information collected and registered at the beginning of the relationship, the greater the ability to identify illegal acts.

Based on a ML/TF risk based approach, customers that pose more risk and cases that require special attention, such as the relationship with PEPs and customers where it was not possible to identify the final beneficiary, specific rigorous analysis procedures are adopted.

It is mandatory to assess the interest in the beginning or maintaining the relationship with individuals or legal entities classified as PEPs by a holder of a position or function at a higher hierarchical level than the person responsible for authorizing the relationship, as defined in internal rule.

Know Your Partner - KYP

Partners are the Legal Entities that enter into business agreements or arrangements between one or several companies of the Itaú Unibanco conglomerate and that meet the requirements established in the Business Partnership Governance Policy.

This pillar includes a set of rules, procedures and controls that must be adopted to identify and properly qualify the business partners, including correspondents in the country and abroad. These partners should be classified into risk categories considering the activities they carry out.

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 defined in internal rule.

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

Know Your Supplier - KYS
This is a set of rules, procedures and controls that must be adopted to identify and properly qualify suppliers and outsourced service providers. These agents should be classified into risk categories considering the activities they carry out.

The objective is to prevent doing business with insidious counterparties or suspected of involvement in illicit activities.

For those customers, partners, suppliers, and service providers who present a higher 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
Is a set of rules, procedures and controls that must be adopted to identify and adequately qualify the employees and/or candidates, in order to subsidize their selection and hiring, as well as monitor situations that may characterize some type of risk or deviation, for the purpose of preventing money laundering, financing terrorism and other illicit acts. These employees should be classified into risk categories considering the activities they perform.

Evaluation of New Products and Services

New products and services, including the use of new technologies, if applicable, shall be evaluated in advance, from the AML/CTF perspective, according to the guidelines established in internal policy.

Sanctions Compliance

It is a set of rules, procedures and controls related to sanctions, embargoes and political and economic restrictions that may be applicable to commercial operations with individuals, institutions and countries/regions involved in terrorism, drug trafficking, war conflicts, human rights violations or other improprieties and illegalities activities consistent with current legislation and regulations and best practices.

According to internal rule, Itaú Unibanco establishes guidelines for total embargoes on countries and follows restrictive lists imposed by sanction authorities.

Monitoring, Selection and Analysis of Suspicious Operations or Situations
All financial transactions and operations, including proposals, performed by customers, whether employees or not, shall be monitored to determine situations that may imply money laundering or terrorism financing. Monitoring considers the profile, origin and destination of funds and the customers' financial capacity.

According to the risk-based approach, for clients with higher ML/TF exposure a stricter set of rules or parameters should be applied or a more frequent or in-depth monitoring of their activities.

Additionally, the Monitoring, Selection and Analysis process must occur independently and autonomously in the AML/CTF Area, which must be segregated from the commercial department.

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 promotes continuous training and disseminates the culture of the subject, thus achieving learning and awareness of its importance, as well as the deepening and recycling of knowledge. Training should be applied to administrators, all employees, and eligible partners. This program aims to:
- deepen the knowledge of the legal and regulatory requirements and responsibilities, as well as the corporate AML/CTF guidelines;
- train on the best way to identify, prevent, treat and communicate situations of risk or with indication of money laundering or terrorism financing in the conducted business;

- promote an organizational culture of prevention of money laundering and terrorist financing, including proliferation of weapons of mass destruction.

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

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

a) Disciplinary breaches and violations of the Itaú Unibanco's Code of Ethics and 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;
- Embezzlement (in all its forms including by electronic means);

- Misappropriation;
- Theft;

- Breach of bank secrecy;
- Robbery;
- Extortion by kidnapping;

Operating Model for the Prevention and Fight Against Fraud

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 specific measures to prevent fraud involving its employees, through guidelines and control procedures intended to prevent and detect irregular activities.

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 the 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 to determine responsibilities and required measures.

The procedures and decisions made during treatment of incidents shall be formalized 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 frauds 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

All information related to the pillars described above, as well as the records of transactions and services provided shall be kept in their original form or in electronic files, according to the 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

Management, employees, partners, and outsourced service providers of Itaú Unibanco shall, within the limits of their duties, immediately report proposals or occurrences of situations or operations with indication or evidence of illicit acts identified in the prospection, negotiation, or during the relationship using the following established channels, by physical or electronic means:

Situations Related to Money Laundering or Terrorism Financing

In Brazil, communications shall be sent to DRCMPLD:

- Telephone: +55 11 2757-6753;

Situations Related to Fraud and Other Illegal Acts

In Brazil, communications shall be sent to the Supervising Department of Fraud Investigation and Prevention:

- External Telephone: 0800-723-0010

- Website: www.itau.com.br/atendimento/pravoce/Denuncia;

- External email: inspetoria@itau-unibanco.com.br and fornecedor_relatos@itau-unibanco.com.br;

Audit Committee:

- External e-mail: comitê.auditoria@itau-unibanco.com.br

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 of 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 management personnel and employees to sanctions ranging from administrative to criminal penalties for money laundering, terrorist financing, fraud, corruption, and other illegal acts.

Negligence and Voluntary Failure are considered non-compliance with this policy and the Code of Ethics and Corporate Policy on Integrity, Ethics and Conduct, and may be subject to disciplinary measures under internal rule.

EXCHANGE OF INFORMATION

Where applicable and according to the information security guidelines set forth in internal policy information may be exchanged between control areas to comply with the guidelines set forth herein.

RELATED REGULATIONS

This policy should be read and interpreted together with the following documents:

Circular Letter No. 4.001/2020 of the Central Bank of Brazil;

Circular No. 3.462/2009 of the Central Bank of Brazil;

Circular No. 3.680/2013 of the Central Bank of Brazil;

Circular No. 3.978/2020 of the Central Bank of Brazil and its amendments;

Circular No. 445/2012 of the Superintendence of Private Insurance and respective amendments;

Decree-Law No. 2,848/1940 - Brazilian Penal Code;

Instruction No. 617/2020 of the Securities and Exchange Commission and respective amendments;

Instruction No. 18/2014 of the National Superintendence of Supplementary Social Security;

Anti-Corruption Law No. 12,846/2013;

Federal Laws No. 9,613/1998 and No. 12,683/2012;

Brazilian Federation of Banks' Self-regulation Regulation No. 011/2013;

Financial Action Task Force (GAFI) recommendations;

Resolutions No. 006/1999 of the Council on Financial Activities Controls;

Resolution No. 021/2012 of the Council on Financial Activities Controls;

Resolution No. 4.753/2019 of the National Monetary Council;

Resolution No. 4.567/2017 of the National Monetary Council; and

Wolfsberg Anti-Money Laundering Principles.

GLOSSARY

Illegal Acts: all conscious human actions or omissions intended to commit criminal offenses - money laundering, terrorism financing, corruption, and fraud.

Close Collaborators: Natural person known to have any kind of close relationship with a politically exposed person, including for: i) having joint participation in a private legal entity; ii) figure as mandatory, even for private instrument the person mentioned in item i); or iii) having joint participation in arrangements without legal status; and natural person who has the control of legal entities or arrangements without legal personality, known to have been created for the benefit of politically exposed person.

Shell Banks: a bank established in a jurisdiction where it has no physical presence and that is not part of a regulated financial group.

Final Beneficiary: the individual who ultimately holds control over the legal entity or on behalf of whom a transaction is conducted. Also considered final beneficiary the representative, including the attorney-in-fact and the designee, who exercise de facto control over the activities of the Legal Entity customer.

CTF: Counter Terrorism Financing.

Special Attention: situations requiring enhanced monitoring are those involving, but not limited to:

- I - proposals for relationships and transactions with politically exposed persons;

- II - evidence of overriding identification and communication procedures;

- III – customers and transactions whose final beneficiary is not identifiable;

- IV - transactions originating in countries that apply the recommendations of the Financial Action Task Force (FATF) insufficiently; and

- V - situations in which it is not possible to maintain updated customer registration information.

Voluntary failure: intentional involvement in illegal actions, such as structuring or advising others to structure transactions for the purpose of circumventing communications to regulatory bodies, or conscious involvement in transactions whose proceeds come from illegal acts.

Itaú Unibanco: Itaú Unibanco Holding S.A.

Politically Exposed Persons (PEPs): are the public agents who perform or have performed, in the last five years, in Brazil or in foreign countries, territories and facilities, relevant positions, jobs or public functions, as well as their representatives, direct or collateral relatives up to the second degree, spouse, civil partner, stepson, stepdaughter, as well as close collaborators. Also considered PEPs are legal entities whose representatives or controllers, directly or indirectly, are PEPs.

AML: Anti-Money Laundering.

Focal Points: management personnel or employees appointed by the business unit Executive Officer to ensure compliance with the corporate AML/CTF guidelines by the business unit.

Retaliation: persecution, reprisal or revenge against management personnel or employees who report their doubts, suspicions, or findings. Examples of retaliation include threats, demotion, "blacklisting", suspension, termination, etc.

Casualty: refers to atypical events that result in losses or disasters to Itaú Unibanco, such as: assaults to agencies and clients, extortion by means of kidnapping, theft, accidents, break-ins, among others.

Approved by the Board of Directors on July 30, 2020