ANTI-MONEY LAUNDERING, COMBATING THE FINANCING OF TERRORISM AND WEAPONS OF MASS DESTRUCTION PROLIFERATION POLICY MANUAL

Anti-Money Laundering Unit

This document does not modify nor replace any specific rules on products, services or procedures, which shall be applied according to all their terms and conditions.

BROU | CONFIDENTIAL
Law 18,381 – ART.9 Paragraph E
Confidentiality period: 15 years
2022 Version

1. INTRODUCTION

The Banco de la República Oriental del Uruguay (hereinafter BROU), as a financial intermediary institution in Uruguay, has a duty to adopt a preventive policy intended to avoid its infrastructure being used for operations related to Money Laundering, Financing of Terrorism or Proliferation of Weapons of Mass Destruction (hereinafter ML/TF/PF).

This Manual contains the internal policies adopted by BROU, for the proper management of the Money Laundering (hereinafter ML), Terrorist Financing (hereinafter TF) and Weapons of Mass Destruction Proliferation (PF) risks run by the Bank.

1.1. APPLICABLE REGULATORY FRAMEWORK

The ML/TF/PF risk Prevention System adopted by BROU is suited to its operational procedures as a financial intermediary institution, in compliance with current laws and regulations, and the general rules and specific guidelines issued by the Central Bank of Uruguay (hereinafter CBU).

The System has incorporated also the recommendations of the main organizations specialized in this subject (FATF Recommendations, Basel Committee, Wolfsberg Principles), as well as the provisions concerning international banking relations (Patriot Act, OFAC-issued Regulations) applicable to financial intermediary institutions with the same operating features as BROU's.

1.2. BASIC CONCEPTS

Money Laundering - Definition

Money laundering is a process through which criminal proceeds are incorporated into the legal economic system, making them appear to have come from a legitimate source.

In theory, the ML process has three stages: the placement of assets or funds; the layering of funds to disguise their origin, ownership and location; and finally, the integration of funds.

1.2.1. MONEY LAUNDERING PROCESS

First Stage. Placement of assets or cash.

This stage consists in introducing cash or other instruments into the financial system or any sectors of the formal economy.

Throughout the process of legitimization of criminally-derived proceeds, the criminal organizations use a vast range of individuals, not only the players of the financial system, but other agents of the economy as well.

Second Stage. Layering or Transformation

A series of operations are carried out in order to disguise or conceal the origin of funds, with the intention of removing traces and evidences.

Third Stage. Investment, integration or drawing of illicit funds.

This is the end of the process. At this stage, the money laundered comes back to the legal economic system, now disguised as "legitimate money."

Terrorist Financing - Definition

The TF crime is committed when a person organizes or, by whatever means, provides or collects funds directly or indirectly for the financing of a terrorist organization or a member of such organization or an individual terrorist, with the intention of using said funds, or knowing that they will be used, in whole or in part, for the financing of terrorist activities.

Terrorist acts are crimes that are committed with the purpose of causing death or serious bodily injuries to a civilian or any other person that does not participate directly in hostilities in an armed conflict, when the purpose of such act, that is revealed by its nature or context, is to intimidate a population or to force a government or an international organization to act or to refrain from doing so (UN International Convention for the Suppression of the Financing of Terrorism).

Financing the Proliferation of Weapons of Mass Destruction - Definition

Financing the Proliferation of Weapons of Mass Destruction is any act that provides funds or uses financial services, in whole or in part, for the manufacture, acquisition, possession, development, export, transfer of material, fractionation, transportation, transfer, storage or use of nuclear, chemical or biological weapons, their means of delivery and other related materials (including dual-use technologies and goods for illegitimate purposes) in contravention of national laws or international obligations, when the latter is applicable.

1.3. MONEY LAUNDERING CRIMES

Articles 30 through 33 in Chapter V of Law 19,574 of December 20, 2017 define the Money Laundering crimes as follows:

> ***Article 30***. *(Conversion and transfer) - The conversion or transfer of goods, products or instruments originated from any of the criminal activities established in Article 34 of this Law shall be punishable by imprisonment for a term of two to fifteen years.*
>
> ***Article 31.*** *(Ownership and possession) - Any person who acquires, possesses, uses, has in their possession or carries out any type of transaction over goods, products or instruments originated from any of the criminal activities established in Article 34 of this Law, or that are a result of said activities, shall be punishable by imprisonment for a term of two to fifteen years.*
>
> ***Article 32.*** *(Concealment) - Any person who conceals, suppresses, alters the evidence or impairs the real determination of the nature, origin, location, destination, movement or beneficial ownership of said goods, products or other rights related to them originated from any of the criminal activities established in Article 34 of this Law shall be punishable by imprisonment for a term of twelve months to six years.*
>
> ***Article 33***. *(Assistance) - Any person who assists the agent(s) in the criminal activities established in Article 34 of this Law, whether it is to ensure the benefit or the result of said activity, to hamper the justice's actions or to avoid the legal consequences of their actions, or provides any help, assistance or advice, with the same goals, shall be punishable by imprisonment for a term of twelve months to six years.*

This provision does not include the assistance or the advice given by professionals to their customers to verify their legal status or within the framework of the right of defense in legal, administrative, arbitration or mediation matters.

Also, Article 34 in Chapter V of Law 19,574 defines the criminal activities whose funds are the subject of Money Laundering:

***Article 34**. (Predicate offenses) - The following are predicate offenses arising from money laundering crimes in their different modalities provided for in Articles 30 to 33 of this Law:*

1) Crimes provided for in Decree-Law 14,294 dated October 31, 1974 in wordings given by Law 17,016 of October 22, 1988 and Law 19,172 of December 20, 2013 (drug trafficking and related crimes).
2) Genocide, war crimes and crimes against humanity, categorized by Law 18,026 of September 25, 2006.
3) Terrorism.
4) Financing of Terrorism.
5) Smuggling for a real or estimate amount of over 200,000 UI (two hundred thousand indexed units).
6) Illicit trafficking in weapons, explosives, ammunition or weapon-usable materials.
7) Illicit trafficking in organs, tissues and medicines.
8) People smuggling and human trafficking.
9) Extortion.
10) Kidnapping.
11) Procuring.
12) Illicit trafficking in nuclear materials.
13) Illicit trafficking in works of art, animals or toxic materials.
14) Scam for a real or estimate amount of over 200,000 UI (two hundred thousand indexed units).
15) Misappropriation for a real or estimate amount of over 200,000 UI (two hundred thousand indexed units).
16) Offences against Public Administration, as provided for in the Uruguayan Criminal Code (hereinafter, "Criminal Code"), Book II, Title IV, and in Law 17,060 of December 23, 1998 (public corruption crimes).
17) Fraudulent bankruptcy.
18) Fraudulent insolvency.
19) The offence provided for in article 5 of Law 14,095 of November 17, 1972 (fraudulent corporate insolvency proceedings).
20) Crimes under Law 17,011 of September 25, 1998 as amended (trademark offences).
21) Crimes under Law 17,616 of January 10, 2003, as amended (intellectual property offences).
22) Criminal conducts under Law 17,815 of September 06, 2004, and articles 77-81 of Law 18,250 of January 06, 2008, and all those unlawful conducts covered by the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, or related to human trafficking, smuggling or sexual exploitation.
23) Forgery and counterfeiting of currency, as provided for in articles 227 and 228 of the Criminal Code.
24) Receivership fraud, as provided for in Article 248 of Law 18,387 of October 23, 2008.
25) Tax fraud, as provided for in Article 110 of the Uruguayan Tax Code, when the amount of the evaded tax or taxes in any fiscal year is over:
A) 2,500,000 UI (two million five hundred thousand indexed units) for fiscal years starting as from January 1, 2018.
B) 1,000,000 UI (one million indexed units) for fiscal years starting as from January 1, 2019.

Said amount shall not apply when using invoices or any other document in whole or in part ideologically or materially false for the purpose of reducing the taxable amount or obtaining a wrongful tax return.
In the cases stated in this item, the tax fraud crime may be prosecuted ex officio.
26) Customs fraud, as provided for in Article 262 of the Uruguayan Customs Code, when the defrauded amount is over 200,000 UI (two hundred thousand indexed units).
In this case the customs fraud crime may be prosecuted ex officio.
27) Homicide committed as provided for in Article 312 Item 2 of the Criminal Code.
28) The bodily harm and grievous bodily harm crimes provided for in Articles 317 and 318 of the Criminal Code, committed as provided for in Article 312 Item 2 of the Criminal Code.
29) Theft, as provided for in Article 340 of the Criminal Code, when committed by an organized criminal group and whose real or estimated amount is over 100,000 UI (one hundred thousand indexed units).
30) Robbery, as provided for in Article 344 of the Criminal Code, when committed by an organized criminal group and whose real or estimate amount is over 100,000 UI (one hundred thousand indexed units).
31) Home invasion, as provided for in Article 344 bis of the Criminal Code, when committed by an organized criminal group and whose real or estimate amount is over 100,000 UI (one hundred thousand indexed units).
32) Cattle theft, as provided for in Article 258 of the Uruguayan Rural Code, when committed by an organized criminal group and whose real or estimate amount is over 100,000 UI (one hundred thousand indexed units).
An organized crime group is a structured group of three or more people existing during a period of time and acting systematically with the purpose of committing said crimes, in order to directly or indirectly obtain an economic benefit, or any other material benefit.
33) Criminal association, as provided for in Article 150 of the Criminal Code. For the purpose of exchanging information between States, both by criminal law judicial cooperation and administrative cooperation between Financial Intelligence Units, the thresholds set forth by the previous items shall not apply.

2. PREVENTION SYSTEM

2.1. PURPOSE OF THE PREVENTION SYSTEM

The purposes of the prevention system of Banco de la República Oriental del Uruguay are to:

- Establish control and prevention systems, policies and procedures that ensure full compliance with rules and regulations in force;
- Reassure customers that BROU applies the best prevention practices, in accordance with the highest international standards in this matter;
- Define and apply Customer Due Diligence policies and procedures, in order to know the beneficial owner of the accounts and transactions, as well as the source of funds and securities;
- Implement policies and procedures regarding the Institution's staff that can guarantee their high level of trustworthiness, as well as their ongoing training in ML/TF/PF Prevention;
- Maintain an appropriate documentary backup that enables the reconstruction of the operations;

- Report unusual or suspicious transactions to the Unit of Financial Information and Analysis (hereinafter "UIAF", for its acronym in Spanish) in due time, according to the legal provisions in force and the regulations issued by the CBU.
- Comply with the obligation of reporting to the CBU's UIAF whenever the existence of assets related to terrorists or terrorist organizations is confirmed, according to the legal provisions in force and the regulations issued by the CBU.

2.2. SCOPE OF APPLICATION

This Manual applies to all BROU branches in Uruguay, as well as to branches located abroad and to members of the Brou Conglomerate, and to financial correspondents in any matters concerning the Institution's customers. This Manual should be known by all employees and applied to every product and service provided by the Institution.

2.3. CONTENTS OF THE COMPREHENSIVE PREVENTION SYSTEM

The System is composed of the following elements:

- Prevention Structure
- ML/TF/PF Risk Management System
- Customer Acceptance Policies
- Customer Due Diligence Policies and Procedures
- Transactions Monitoring Process
- Unusual and/or Suspicious Activities Report
- Financial Transactions Report furnished to the CBU
- Policies and Procedures regarding Correspondent Banks
- Policies and Procedures regarding Suppliers
- Policies and Procedures regarding Staff
- Independent Review of the Prevention System
- Prevention Manuals

3. PREVENTION STRUCTURE

BROU's Prevention Structure is composed of:

- Board of Directors of BROU
- AML Commission
- Compliance Officer
- AML Operational Committee
- Anti-Money Laundering Unit (hereinafter UPLA, for its acronym in Spanish)

3.1. BOARD OF DIRECTORS

The Board of Directors is the highest authority of the Institution in ML/TF/PF Prevention. The tasks of the Board of Directors are:

- Approving and adopting the Institution's Code of Ethics, ordering its compliance and dissemination, and approving its updates.
- Approving UPLA's organizational structure.
- Appointing the Bank's Compliance Officer.
- Dealing with issues submitted by the AML Commission.
- Receiving the report presented by the Compliance Officer on an annual basis.
- Approving UPLA's Strategic Plan.
- Approving the ML/TF/PF Prevention Manuals.
- Ordering any measure deemed necessary within the Board tasks established by the Bank's Charter.

3.2. AML COMMISSION

BROU has an AML Commission (hereinafter the Commission) which reports directly to the Board. This Commission is composed of two members of the Board, the General Manager and the Compliance Officer. One of the members of the Board acts as the Commission President.

The Commission is in charge of planning, coordinating and monitoring the compliance with the Bank's ML/TF/PF Prevention policies.

The tasks of the Commission are:

- Analyzing and approving the regular plans developed by the AML Unit (UPLA), as well as their level of compliance, notwithstanding the control carried out by the Audit Committee.
- Assessing, on a regular basis, the proper functioning of the ML/TF/PF Prevention Comprehensive System.
- Being aware of the reports regularly issued by the Compliance Officer on the Bank's policies regarding compliance with laws and regulations, ethical standards, conflicts of interest and investigations.

The Commission will meet on a quarterly basis or whenever its President calls for a meeting.

In addition to its members, other employees appointed by the Commission may attend the meetings if their attendance is deemed relevant to discuss the agenda.

In each meeting, minutes shall be written up to specify the issues discussed, as well as the resolutions adopted and the matters that will require further treatment. Said minutes shall be included in the Commission's Record of Minutes.

In order to open sessions, at least three members of the Commission are to be present.

In all cases, resolutions shall be adopted in writing and by unanimous decision of the members of the Commission attending the meeting. The matters that are not unanimously agreed shall be submitted to the Board of Directors for their consideration.

3.3. COMPLIANCE OFFICER

The Compliance Officer shall be in charge of proposing and developing the Institution's ML/TF/PF Prevention policies, and assessing their compliance by the Business Divisions, through the analysis of the procedures adopted for this purpose.

The tasks of the Compliance Officer are:

- Implementing the strategies and policies approved by the Board and developing well-documented procedures that allow to identify, measure and control the ML/TF risk, which shall be applied throughout the Institution, its subsidiaries and branches, as well as to outsourced services.
- Verifying that the risks fall within the levels established by the Board. If they do not, they should be informed to the corresponding management level for their resolution.
- Assessing the efficiency of the ML/TF/PF Prevention System, according to the rules in force and the best practices in this regard.
- Proposing ML/TF/PF Prevention policies and procedures for the Institution.
- Giving advice to the Commission and other areas regarding ML/TF/PF Prevention.
- Fostering the adoption of the best ML/TF/PF prevention practices within BROU.
- Verifying and coordinating the supervision and control of the ML/TF/PF Prevention System in all BROU branches.
- Collaborating with the external agents in charge of the independent ML/TF/PF Prevention System review.
- Acting as a link to competent authorities, and national and international related organizations.
- Supervising the correspondent banking relationships and ML/TF/PF Prevention due diligence in the Bank's branches abroad.
- Approving UPLA Policies and Procedures Manual.
- Reporting any suspicious activities (SAR) to the Unit of Financial Information and Analysis, notifying the General Manager.

3.4. AML OPERATIONAL COMMITTEE

The AML Operational Committee (hereinafter the AML Committee) is composed of the Compliance Officer, the Assistant General Commercial Manager and the Executive Managers of the areas involved. In addition, depending on the issues under review, there may be other non-permanent members.

The tasks of the AML Committee are:

- Making decisions regarding high ML/TF/PF risk customers or customer groups, as well as those that do not comply with the rules.
- Making decisions regarding persons' inclusion in or exclusion from the Disqualified Persons List of UPLA.

- Coordinating the necessary actions with the different areas involved in order to implement the decisions adopted by the Committee.

The AML Committee shall hold meetings on a quarterly basis or any time the Compliance Officer so requires. Every time a meeting is called to make decisions regarding the maintenance of commercial relationships with certain customers, said meeting shall be held within forty-five days from the relevant SAR.

In addition to its members, other employees appointed by the AML Committee may attend the meetings if their attendance is deemed relevant to discuss the agenda.

In each meeting, minutes shall be written up to specify the date and the issues discussed, as well as the resolutions adopted and the matters that will require further treatment. These minutes shall be included in the Operational Committee's Record of Minutes.

In all cases, resolutions shall be agreed in writing and by unanimous decision of the members of the AML Committee attending the meeting. The matters that are not unanimously agreed shall be submitted to the Commission for its consideration.

3.5. ANTI-MONEY LAUNDERING UNIT

The tasks of the Anti-Money Laundering Unit (UPLA) are:

- Advising the different services of the Institution in matters related to ML/TF/PF Prevention.
- Developing the Institution's ML/TF/PF Prevention policies and procedures, following the objectives set by the Board of Directors.
- Monitoring the effective implementation by each Business Division and other services concerned, of the rules and procedures adopted to prevent and control ML/TF/PF operations.
- Controlling that the policies and procedures adopted are reasonably suitable to prevent and detect ML/TF/PF operations, and are also in compliance with legal regulations in force and in line with the best practices.
- Keeping the Bank's ML/TF/PF Prevention Policies Manual updated, submitting the proposed amendments to consideration of the Commission on a yearly basis.
- Developing ML/TF/PF prevention training and awareness programs, in coordination with the Training Department, taking active part in their implementation.
- Centralizing the information and analysis of the Suspicious Activities Reports.
- Monitoring the efficiency and proper functioning of the automated alert system for detecting unusual transactions (SOS).
- Reporting unusual or suspicious operations to the CBU, under the established procedure, and doing the follow up of said operations.
- Keeping the Risk Lists updated and carrying out the relevant controls.
- Reporting cash operations to the CBU, pursuant to the relevant regulations.
- Acting as a link to correspondent banks in order to request and/or send information about the application of ML/TF/PF Prevention policies and procedures.
- Taking part in seminars, courses or other internal or external training activities.

- Providing advice for the preparation of the Bank's Code of Conduct, in matters related to ML/TF/PF Prevention.
- Managing the definition and parameterization of the necessary alerts for the IT system.
- Developing and maintaining the ML/TF/PF risk matrix.
- Coordinating and performing the monitoring of high-risk accounts or those established by the competent authority.
- Receiving, preparing and diligently processing the response to information requests from competent authorities, collecting and processing information through the Bank's operational services, within their respective confidentiality framework and in accordance with current regulations.

The structure of the Anti-Money Laundering Unit was approved by Resolution of the Board of Directors dated on July 21, 2022.

3.6. MANAGEMENT STANDARDS RELATED TO MONEY LAUNDERING AND TERRORIST FINANCING RISK (ML/TF)

The Bank takes on a strong commitment in complying with the minimum Management standards published by the Central Bank of Uruguay (CBU), in force since July 01, 2017, which establish the following standards concerning ML/TF risk to be applied in connection with Weapons of Mass Destruction Proliferation risk:

ML/TF RISK

The risk of ML/TF refers to the possibility of loss or damage that an entity may suffer if it is used directly or through its operations as an instrument for money laundering and/or channeling assets to fund terrorist activities, or when it is intended to conceal the assets resulting from said activities.

Money laundering operations are carried out for the purpose of legalizing (or at least giving legal appearance to) goods of an illicit origin; covering the illicit origin of the resources eliminating their connection with the activity that originated them, or mixing illegal money with legitimate financial transactions for the purpose of justifying the origin of the total amount of money as resulting from a legal activity that serves as facade. By contrast, funds used to support terrorism may come from legitimate sources, criminal activities, or both. In this case, what matters is to hide the source of financing, without regard to its legitimacy or illicitness, because if it is possible to cover up the source, it will be available for future financing activities. Financial institutions play an important role, since individuals or criminal organizations will attempt to use them in many ways, from the placement of cash into legal financial channels, carrying out multiple transactions or bank drafts to erase traces, transferring the securities custody and hindering the tracking of illicit funds, to formally integrate them back into the legal financial channels using the facade of a licit economic activity and entering into transactions which would be considered normal for any company, such as imports, exports, payment of services or interests on loans, but with the special characteristic of having an illegitimate and often fictional origin.

Institutions must implement a system including policies, practices and procedures which would allow for the identification, assessment, monitoring and mitigation of the risk of being used as an instrument for money laundering or channeling to fund terrorist financing. To do so, institutions must have policies and procedures duly documented and informed to all relevant staff, which shall be a part of the comprehensive risk management of the

institution and applied continuously to the entire financial group. Strict rules to getting to know their customers shall be implemented, in order to identify who is the "real beneficiary" of the account. It is also necessary to establish ethical standards to ensure the integrity of the staff and to define continuous training programs for the employees in order to enable them to recognize the innovations related to these illicit actions and to proceed according to the situation. Likewise, the bank's commercial interests should be in no way opposed to the efficient performance of the compliance function. The entity should assume an operational and accountability structure consistent with its size, operational complexity and level of risk.

67. The Board of Directors must approve the strategy and policies that promote a proper management of ML/TF risk, on an individual and consolidated basis, subject to periodic review. The Board of Directors must regularly review the ML/TF risk exposure and ensure that risk levels are within the established framework.

(…)

68. Senior Management must ensure the implementation of the risk policies approved by the Board of Directors in relation to money laundering and terrorist financing risk and the development of procedures for its identification, measurement, monitoring and control.

(…)

69. The Compliance Officer is responsible for the implementation, follow-up and control of the proper operation of the ML/TF risk prevention system.

(…)

4. ML/TF/PF RISK MANAGEMENT SYSTEM

The Money Laundering, Financing of Terrorism and Proliferation of Weapons of Mass Destruction Risk Management System ("SARLAFTP", by its Spanish acronym) analyzes, at least once a year, the inherent and residual ML/TF/PF risk levels of the Bank's operations, assessing such levels according to the methodological framework adopted by the Bank for Risk Management purposes.

The Five Risk Factors (RF) -indicated by the best practices- are identified and weighted as per their contribution to the consolidated ML/TF/PF risk of the Bank: Customer, Product, Channels, Geographical Areas and Processes. Risk events are identified under said RFs; the risk before controls (inherent risk), the existing controls, and the post-control risk (residual risk) are analyzed for each event.

The Bank shall only conduct transactions or offer products or services when the associated ML/TF/PF residual risk is "Low" or "Moderate".

The SARLAFTP shall be implemented in branches located in Uruguay as well as abroad.

5. CUSTOMER DUE DILIGENCE POLICIES

In compliance with Law 19,574 issued on December 20, 2017, BROU will not establish a business relationship or conduct operations when it is unable to conduct due diligence as provided for in this manual.

When this situation arises in connection with a customer in the course of a business relationship, it will be brought to an end and the employee shall consider the appropriateness of filing a Suspicious Activity Report.

To this effect, the Bank shall assess if the customer's intention is to avoid the due diligence, based on criteria of reasonableness. If the Bank considers that such intention exists, the Bank shall comply with its legal obligation of reporting the transaction as suspicious to the CBU. Obtaining the necessary information for the due diligence regarding the ML/TF/PF risk is part of an integrated process within the commercial relationship, which should enable the correct identification of the customer and the beneficial owner, as well as to determine the purpose, nature and volume of the transactions that the customer is expected to conduct.

Notwithstanding the specific regulations issued for the different products and operations, the business units shall be especially cautious when accepting a new commercial relationship and in case of changes in a customer's risk profile. It is of the utmost importance that the employees in charge of admitting a new customer or approving a transaction, as well as those assisting in said task, pay careful attention to the information and documents provided by the potential customer. They shall also be responsible for the accuracy and completeness of the information loaded into the IT systems and tools, as provided for by the Bank.

BROU's prevention policy aims not only at the merely formal identification but also at getting to "know your customer". To this effect, the employees who are in charge of conducting the due diligence must obtain the necessary information and documents to identify the customer and the beneficial owner, verify their identity, make a reasonable assessment of the volume and nature of the customer's economic activity, understand their transactions and relate them with the nature and size of the customer's business.

Articles 6 and 7 of Law 19,484 establish the following, in relation to the identification of the tax residency and the beneficial owner:

> ***Article 6 (Due diligence) -*** *Financial entities subject to reporting in virtue of this law, shall identify the tax residency of natural persons, legal persons or other entities maintaining accounts with them. The same requirement shall apply to the beneficial owner when applicable. (…)*
>
> ***Article 7 (New accounts. Tax Residency Statement) -*** *Since the entry into force of this law, no new accounts may be opened, and no debt instrument or interest may be issued without complying, among others, with the requirement of declaring to the financial entity the tax residency of natural persons, legal persons or other entities and beneficial owners when applicable.*
>
> *(…)*

5.1. PURPOSE OF THE CUSTOMER DUE DILIGENCE PROCESS

BROU has adopted policies, procedures and controls for Customer Due Diligence purposes -based on its ML/TF/PF risk assessment-, which aim at achieving the following objectives:

- Identifying Customers and verifying their identity, through documentary evidence;
- Identifying the beneficial owners and taking reasonable measures to verify their identity;
- Obtaining information about the purpose of the commercial relationship and the volume and nature of Customers' transactions;

- Knowing the Customers' economic activity, business or profession, as well as the source of funds;
- Monitoring Customers' transactions in order to analyze whether they are consistent with the information that the Bank holds about said customers.

5.2. .COMMERCIAL RELATIONSHIPS AND CUSTOMER ACCEPTANCE POLICY

5.2.1. COMMERCIAL RELATIONSHIPS DEFINITION

Commercial relationships are all the business counter-parties of the Bank, including suppliers, who are subject, in this regard, to the same regulations and due diligence as the customers.

5.2.2 COMMERCIAL RELATIONSHIPS ACCEPTANCE POLICY

It is BROU's policy not to establish or maintain commercial relationships with the following Natural and Legal Persons:

1. Natural Persons that have been indicted or convicted of ML crimes by a national or foreign Court, whenever BROU confirms conclusively such condition. The AML Committee shall analyze their inclusion in UPLA's Disqualified Persons List. (*)
2. Natural Persons that have been indicted or convicted of terrorism offences by a national or foreign Court, whenever BROU confirms conclusively such condition. The AML Committee shall analyze their inclusion in UPLA's Disqualified Persons List. (*)
3. Natural or Legal Persons included in the lists of the Office of Foreign Assets Control (hereinafter OFAC) of the United Nations Organization (hereinafter UN) or national list defined in decree 136 of May 16, 2019, as provided for in the Resolution of the Security Council S/RES/1373 (hereinafter National List).
4. Natural or Legal Persons, whether existing or prospective customers, not satisfying the Due Diligence requirements established by the Bank, as applicable.
5. Persons disqualified to operate with the Bank, by Resolution of the Board of Directors.
6. Persons included in UPLA's Disqualified Persons List, by resolution of the AML Committee.

(*) If a court has granted an acquittal to the defendant, or the case has been closed, thus being acquitted, the AML Committee may establish an exemption to the general principle established in 1 and 2 above, based on the relevant transaction risk assessment.

As for convicts, once they prove having served their sentence or that it has been suspended, the above procedure shall be followed.

5.3. BROU CUSTOMERS

BROU regular customers are all those Natural and Legal Persons that have entered into a contract to make use of different financial products or services. Therefore, the Bank only operates

with duly registered Customers that have satisfied all the requirements of the customer acceptance process, and all the conditions required for the use of the relevant product or service.

The Bank does not consider customers those who do not hold a customer account with an operating credit or deposit product with the Bank and whose sole relationship with the Bank consists in conducting the following transactions:

Transaction
• Payment of social benefits delivered by national public entities. (For example: Beneficiaries of the Ministry of Social Development (Mides), Family Allowances, etc.) • Receiving payments or items managed by government offices, which the Bank has the obligation to pay. (For example: Funds from the Ministry of Livestock, Agriculture and Fisheries (MGAP)). • Receiving transfers from abroad, whose ordering parties are foreign Social Security Organizations that have signed an agreement with BROU to execute their payments, provided that the payment details state that they are "PENSION, RETIREMENT OR INCOME PAYMENTS" for amounts not exceeding: US$3,000 (three thousand US dollars) or its equivalent in other currencies. • Checks or Bills of Exchange issued by BROU, cashed at our counters. • Deposits to third party accounts. • Other transactions made for account and by order of a customer.

The Bank also does not consider customers those whose sole relationship with BROU is as officer, proxy, spouse or beneficial owner of a client, provided that they are not registered as holder of any product.

5.4. WALK-IN CUSTOMERS DEFINITION

'Walk-in' Customers are those who make a series of occasional transactions, for an amount not exceeding USD 15,000 or its equivalent in other currencies.

Their activity shall be restricted to currency exchange transactions and domestic money orders.

If these customers begin to operate on a regular basis or their transactions, individually or in the aggregate, reach the referred threshold, they shall be categorized as 'Regular,' and registered normally as customers, upon conducting the Due Diligence procedures provided for in 5.5.

5.5. REGULAR CUSTOMER DUE DILIGENCE

Customer Due Diligence (hereinafter CDD) is applied to all Regular Customers of BROU.

BROU's customer identification procedures shall set the minimum information requirements for regular customer identification, considering customer risk and their operational risk, and according to the provisions of Article 297 of the Communications Compilation of Financial System Regulation and Control Rules (RNRCSF, by its Spanish acronym) issued by CBU.

Likewise, additional requirements or any other applicable rules shall be imposed to the products or services contracted according to the customer's ML/TF/PF risk.

Link to the RNRCSF issued by CBU:

https://www.bcu.gub.uy/Acerca-de-BCU/Normativa/Documents/Reordenamiento%20de%20la%20Recopilación/Sistema%20Financiero/RNRCSF.pdf

5.6. CUSTOMER IDENTIFICATION

5.6.1. VERIFICATION OF CUSTOMER'S IDENTITY

During the Know Your Customer process, the employees in charge shall determine and verify, based on documentary evidence, the identity of the customer (holder/s), the beneficial owner and their representatives and attorneys in fact (authorized to operate), and adopt reasonable measures to identify the actual beneficial owner of the funds, if applicable.

The identity document of the spouse, domestic partner (in case of a legally recognized union) or any other person/s related to the holder(s), who is/are registered in the computer systems but do not operate in their own name with BROU, shall also be required.

The identification of natural or legal persons stated in the previous paragraph shall be made at least upon presentation of a valid document as defined by CBU. Generally, the identity documents should be issued by an official authority, be in force and have a photo of the individual requesting the Bank's services.

In the case of a Legal Person, the regulations shall establish the documents required to prove its existence, and the documents that prove the legal capacity of its representatives and authorized signatories to enter into contracts. The requirement of retention and safekeeping of said documents shall be established in the corresponding procedures.

5.7. IDENTIFICATION OF POLITICALLY EXPOSED PERSONS

The Know Your Customer Process shall include due diligence steps to determine whether the potential Customer is a Politically Exposed Person (PEP), a relative or a close associate of a PEP, in which case, the commercial relationship shall be subject to special acceptance procedures and transaction monitoring.

The Bank has established two methods for the identification of PEPs: a Customer's self-disclosure (PEP, or a relative or close associate of a PEP), and scanning against data bases of PEPs accepted by BROU.

5.8. BUSINESS ACTIVITY OF THE CUSTOMER

BROU will try to gain a proper knowledge of the Customer, obtaining accurate information regarding the Customer's business activity or profession and the origin of funds, in order to connect this information with the expected transactions. To this effect, the customer accounts ownership must be consistent with the transactions and activity type carried out through said accounts.

5.9. ENHANCED DUE DILIGENCE

An Enhanced Due Diligence process shall be conducted for higher risk customer categories, as determined by the regulations. To this effect, in addition to applying the general Due Diligence procedure, special requirements shall be imposed, according to the type of transaction, customer's activity and operations.

5.9.1. CORRESPONDENT BANKING RELATIONSHIPS

5.9.1.1. CORRESPONDENT BANKS

BROU allows the establishment of correspondent banking relationships with domestic and foreign financial institutions.

As for domestic financial institutions, said relationship shall be established under conditions that enable said institutions to maintain accounts or carry out payments or fund transfers for their own customers through our institution or vice versa.

As for foreign financial institutions, the relationship is formalized through BROU's accounts with said institutions, intended for the processing of transfers or for carrying out investments on our own or on behalf of our customers.

The correspondent banking relationships shall be established only with entities that are effectively regulated and supervised in their country of residence. Therefore, to open and maintain a correspondent banking relationship, information should be obtained about the management, reputation and business nature (main activities, purpose of the account, geographical area of operation, inter alia) of the correspondent financial institution. Furthermore, before starting the relationship, the ML/TF/PF Prevention policies and procedures applied by the correspondent should be obtained and assessed, in particular those concerning the acceptance and knowledge of the Customer.

No business relationship shall be established with correspondent financial institutions incorporated in jurisdictions that do not require a physical presence or with institutions that allow their accounts to be used by such type of entities.

Irrespective of the documents employed to define the responsibilities of each institution, especially those concerning customer knowledge, BROU has adopted the Wolfsberg Questionnaire and the PATRIOT Act Form to exchange information with the correspondent financial institutions, for the purpose of collecting relevant information from a preventive point of view.

5.9.1.2. CORRESPONDENT FINANCIAL INSTITUTIONS

BROU establishes relationships with correspondent financial institutions that render authorized services in the country at their own expense and under their own responsibility, according to the CBU rules and regulations.

All necessary actions shall be taken for the Correspondent Financial Institutions to apply the policies and procedures required by the Bank, and ensure a proper training in ML/TF/PF Prevention in relation to the contracted services.

The design and performance of the services provided by the Correspondent Financial Institutions shall ensure an appropriate monitoring and control of the transactions executed, in compliance with current ML/FT prevention regulations.

5.9.2. POLITICALLY EXPOSED PERSONS (PEPs)

PEPs are those individuals who "are entrusted or have been entrusted over the last 5 years with prominent public functions, in the country or abroad, such as: Heads of State or of Government, senior politicians, senior government, judicial or military officers, senators and members of the Legislative Branch, important political party leaders, directors and senior executives of state owned corporations and other public entities.

Those individuals who are entrusted or have been entrusted over the last 5 years with a senior position in an international organization are also deemed politically exposed persons, such as: members of senior management, directors, deputy directors, members of the board or equivalent senior officials.

The relationships with PEPs, their relatives and close associates shall be subject to enhanced Due Diligence procedures, which should be applied, at a minimum, within the following five years after the politically exposed person has left office.

5.9.3. ACCOUNTS OPENED OR TRANSACTIONS RELATED TO NATURAL OR LEGAL PERSONS THAT MANAGE THIRD-PARTY FUNDS.

The regulations shall state the special due diligence requirements to be applied when a Customer manages third-party funds, whether the Customer is subject to financial regulation and supervision or not, in accordance with Section 302 of the RNRCSF.

When dealing with Customers subject to financial regulation and supervision, due care should be taken to ensure that the Customer applies adequate procedures for the acceptance and due diligence of its customers.

The regulations shall state when third-party funds are to be managed through special purpose products, and the Customer shall provide information that allows to identify the customer on whose behalf it is operating (the Customer of the Customer) and to determine the origin of funds.

5.9.4. REQUIREMENTS FOR OUTGOING FUND TRANSFERS

Our outgoing fund transfer service is rendered only to Regular Customers. When a fund transfer is sent, the provision of the Beneficiary's full information (full name, address and account number or ID number) must be verified.

Before sending a fund transfer abroad, the Customer must give transfer instructions, in the manner and on such terms as provided for by BROU.

The ordering party, the beneficiary and the paying bank shall be checked against the lists of the UN, OFAC and National Lists. No transaction shall be carried out if there is a true match with said lists. The regulations shall provide for the implementation of other control lists for due diligence purposes.

5.9.5. REQUIREMENTS FOR INCOMING FUND TRANSFERS

Our incoming fund transfer Service is rendered only to Regular Customers. When a fund transfer is received, the provision of the Ordering Party's full information (full name, address and account number or ID number) must be verified.

Special care should be taken with those incoming transfers that do not fully identify the ordering party as stated above. If said information cannot be completed, the transfer should be evaluated to determine if it constitutes an unusual or suspicious activity which would warrant issuing a report.

When acting as intermediary, the Bank should keep the Ordering Party's information during the whole payment chain.

The ordering party, the beneficiary and the issuing bank shall be checked against the lists of the UN, OFAC and National Lists. No transaction shall be carried out if there is a true match with said lists.

5.9.6. FUND TRANSFERS IN GENERAL

International fund transfers in which the ordering party or beneficiary is a currency exchange (casa de cambio), one of the companies included in Title III, Chapter I, Section I, Art. 87 of the RNRCSF, or a fund transfer institution, shall not be processed.

BROU shall not participate in circuits of services related to international fund transfers from non-supervised financial institutions. Subject to the transaction's risk, the ordering or paying institution might be required to have a banking license.

For these purposes, those institutions which are not financial institutions but offer regular and professional domestic or foreign transfer and money order services are also deemed fund transfer institutions, regardless of their operational method (electronic transfers, instructions by telephone, internet, apps, etc.).

The regulations shall provide for enhanced due diligence procedures when the transaction is executed by order and for account of a third party. In these cases, enhanced due diligence processes shall be applied to allow the correct identification of beneficial owners as well as the origin of the funds involved.

5.9.6.1. NESTED ACCOUNTS

Nested accounts occur when a financial institution gains access to the financial system of another country by covertly operating through a correspondent account belonging to another foreign financial institution.

If BROU or its correspondent financial institutions are unaware of said situation, they would be effectively granting anonymous access to the financial systems involved.

Nested account activities are unacceptable for BROU in accordance with the requirements of their correspondent banks.

5.10. SIMPLIFIED DUE DILIGENCE

The Bank may establish simplified due diligence procedures for customers, products and operations of low ML/TF/PF risk.

Simplified procedures shall be adjusted to the regulations of the CBU.

When said measures are adopted, relevant controls must be established in order to determine if an account or a customer has no longer the profile on which the application of the simplified

measures was based. In such case, the additional due diligence procedures must be applied according to the new risk scenario.

Simplified CDD measures are not applicable when there is a suspicion of ML/TF/PF.

6. TRANSACTIONS MONITORING PROCESS

BROU has implemented an automatic monitoring system of its Customers' transactions, in accordance with the best international ML/FT/PF prevention practices.

7. UNUSUAL AND/OR SUSPICIOUS ACTIVITIES REPORT

7.1. REPORTING DUTY

For the purpose of complying with the provisions of Article 12 of Law 19,574 and Article 313 of the RNRCSF issued by BCU, any unusual or suspicious transaction must be reported to the UIAF, as provided for by the Regulator.

In this regard, the transactions considered suspicious or unusual are those -whether executed or not-, that according to the customs and practice of the related activity, are unusual, have no evident economic or legal justification, or have an unusual or unjustified complexity; as well as those financial transactions which raise suspicion of an illegal origin.

The reporting duty applies also to those transactions that, despite involving assets with a legitimate origin, are under suspicion of being related to natural or legal persons involved in terrorist financing offences or of being destined to finance any terrorist activity.

7.2. UNUSUAL OR SUSPICIOUS TRANSACTIONS GUIDE

7.2.1. DESCRIPTION

For the purpose of collaborating in the process of detection of suspicious transactions by the reporting persons, CBU's UIAF publishes suspicious or unusual transaction Guides that compile types or patterns of financial transactions which might be linked to the legitimation of assets originated from criminal activities. BROU employees as well as those of financial correspondents providing services for BROU customers are obliged to be acquainted with them.

7.3. REPORTING ON TERRORISM-RELATED ASSETS

7.3.1. REPORTING DUTY

In accordance with the provisions of Article 314 of CBU'S RNRCSF, the Financial Intermediaries should report to the UIAF the existence of assets related to persons that are in any of the following situations:

- They have been identified as terrorists or as belonging to terrorist organizations, they are included in individuals or associated entities lists catalogued as per the UN

Security Council Resolutions, to prevent terrorism and its financing, as well as the proliferation of mass destruction weapons;

- They have been declared terrorists by final judgment of a national or foreign court.

7.3.2. LIST CHECKING AND ASSET FREEZING

As stated in Art. 3 of Law 19,749 dated on May 16, 2019, Financial Institutions should continuously check and verify:

A) The lists of individuals or entities associated with terrorist organizations, issued by the UN pursuant to the UN Security Council Resolutions S/RES/1267, S/RES/1988, S/RES/1989 and subsequent.

B) The lists of individuals or entities associated with financing the proliferation of mass destruction weapons, catalogued pursuant to the UN Security Council Resolutions S/RES/1718, S/RES/1737, S/RES/2231 and subsequent.

C) The appointment of natural or legal persons or entities pursuant to the UN Security Council Resolution S/RES/1373.

D) The list of persons declared terrorists by final decision of a national or foreign court, as stipulated by Law 17,835 (Art. 17, item B) issued on September 23, 2004.

In compliance with said article of Law 19,749 and with Art. 3 of Decree 136/2019 issued on May 16, 2019, in case of a match, BROU shall freeze, immediately and on a preventive basis, funds and other assets of any nature of natural or legal persons or entities whose names or identification data match with the lists, and shall therefore block all incoming funds.

The natural or legal person or entity affected shall not be notified.

List checking and freezing procedures described in this article, shall comply with the provisions of Law 19,749 (Art. 4 through 6), as stated below:

> ***Article 4*** *(Immediate notification and confirmation of the measure). - Reporting persons shall notify BCU's UIAF, immediately, that a preventive freezing has been placed, and unless the circumstances established in the following item have occurred, said Unit shall inform the competent criminal court which shall have a term of up to seventy-two hours to determine if said freezing was placed on a natural or legal person or entity appearing in the UN Lists mentioned by Art.3 of this Law, and without any previous notification, shall decide to maintain the freezing or not. Once the measure is confirmed, the interested party shall be notified within three working days.*
>
> *The UIAF may order to lift the preventive freezing stipulated in the previous item if it is proven by any reliable means that the freezing of funds and other financial assets or economic resources was due to a homonymy or false positive. Once ordered, said lift must be informed to the National Secretariat for Combating the Money Laundering and the Financing of Terrorism ("SENACLAFT", by its Spanish acronym).*
>
> *The resolution adopted by the competent court, whether providing for or dismissing the freezing of funds and other financial assets or economic resources, shall be informed to the UIAF which, in turn, shall communicate the resolution to the reporting persons.*
>
> *Notwithstanding the foregoing, the UIAF shall inform the SENACLAFT of any preventive freezing that may have been placed.*

Article 5 *(Maintaining the measure) - Preventive freezing shall be maintained until the individual or entity is eliminated from the lists mentioned in Art 3 of this Law.*

If the reporting persons fail to comply with the duties established in the previous articles, the administrative sanctions and penalties provided for in Articles 12 and 13 of Law 19,574 issued on December 20, 2017 shall be applied, according to the specific circumstances.

Article 6 *(Homonymy or false positive). If after the freezing provided for by the competent criminal court, it is proven by any reliable means that the freezing of funds and other financial assets or economic resources was due to homonymy or false positives, at the request of the interested party, the court shall order to lift the freezing within two working days at the latest.*

7.4. LEGAL REGULATIONS REGARDING REPORTING PERSONS

Chapter II of Law 19,574 identifies financial and non-financial reporting persons, among which the Bank is included, which cooperate with the prevention system as follows:

Article 12. (Financial entities subject to reporting) *- All natural or legal persons subject to CBU's control are legally bound to report the transactions, whether executed or not, which according to the customs and practice of said activity are unusual, have no evident economic or legal justification or have an unusual or unjustified complexity. Those financial transactions involving assets suspicious of illicit origin should also be reported, in order to prevent the money laundering crimes under Articles 30 through 33 of this Law, and to prevent terrorist financing. In this last case, the reporting requirement includes those transactions that - even if they involve assets of licit origin - are suspected to be related to natural or legal persons involved in ML or destined to the financing of any terrorist activity.*

The reports shall be submitted to the CBU's UIAF, according to the provisions stipulated by the CBU.

Armored transportation companies shall also be subject to the reporting obligation.

The activity of the reporting entities shall be under the supervision of the CBU.

The non-compliance with the reporting requirement shall determine the application, according to the specific circumstances, of the sanctions and administrative measures provided for in Decree-Law N° 15,322 issued on September 17, 1982, as per Law 16,327 issued on November 11, 1992 and the amendments introduced by Laws 17,523 issued on August 4, 2002 and 17,613 issued on December 27, 2002.

(…)

Article 22. (Non-disclosure obligation).- *Confidentiality is required. No reporting persons, including the persons contractually related to them, shall put on the record of the participating persons or third parties, the updates and reports carried out or produced on them, complying with the obligation imposed in articles 6, 12, 13 and 26 of this law and the financial sanctions related to the prevention and repression of terrorism and its financing, as well as the prevention, suppression and interruption of the proliferation of mass destruction weapons.*

Those who breach this obligation shall be liable to the penalties stipulated in articles 12 and 13, respectively.

Upon receipt of the report, the UIAF may instruct the reporting persons on the steps to be taken regarding the transactions in question and the commercial relationship with the customer. If within three business days the Unit does not give any instructions, the reporting persons may act in their best interests.

(…)

Article 23. (Exemption of liability) - *The compliance in good faith with the informing obligation provided for in articles 6, 12, 13 and 26 of this law and the financial sanctions related to the prevention and repression of terrorism and its financing, as well as the prevention, suppression and interruption of the proliferation of mass destruction weapons, as long as they adjust to the procedures that the CBU or the Executive Power establishes on this matter, constituting obedience to a legal regulation passed for general interest (article 7 of the Constitution of the Oriental Republic of Uruguay), shall not constitute a violation of secret or professional or commercial reserve. Therefore, it shall not result in any civil, business, labor, criminal, administrative liability or any other kind of liability.*

When analyzing transactions involving reporting persons, the provisions of Art. 225 of Law 19,899 issued on July 9, 2020, must be observed:

Article 225.- (Due diligence procedures).- *The following paragraphs are added to Article 17 of Law 19,574 issued on December 20, 2017: "The fact that the transaction or activity was carried out using electronic means of payment, such as bank transfers or other payment instruments issued by financial intermediaries, or which they were obliged to pay, or securities of which they were depositories, does not exempt non-financial reporting persons, designated by article 13 of this Law, from the application of due diligence procedures, but considering the lower risk of money laundering or terrorist financing that these cases pose, and in the case of resident and non-resident customers from countries which comply with the international standards regarding the prevention of money laundering and terrorist financing, these procedures may consist in the application of simplified due diligence measures. The foregoing shall not apply in the situations referred to in articles 20 and 22 of this Law and articles 13, 14, 42, 46 and 89 of its regulatory Decree No. 379/2018 issued on November 12, 2018, in which case, enhanced due diligence measures should be applied. When the originator of the payment is an individual other than the one performing the transaction, simplified or enhanced due diligence procedures should also be carried out on such individual, as established in the previous paragraph. The origin and destination accounts of the funds or securities may be held in foreign financial intermediaries, provided that such institutions are located in countries that comply with international standards on money laundering and terrorist financing."*

7.5. RECORD-KEEPING

In compliance with Article 21 of Law 19,574, BROU shall keep the records of all the transactions carried out with or for its customers, both domestic and international, including as well, all the information about customer knowledge obtained during the due diligence process, for a minimum period of five years after the commercial relationship is ended or after the date of the occasional transaction. Notwithstanding the foregoing, the general retention period set forth in Book III, "Administration" of BROU's Compilation of Rules is applicable.

The records of the transactions and information obtained from the due diligence process must be sufficient to allow the reconstruction of individual transactions to provide, if necessary, evidence for prosecution in the relevant jurisdiction.

These records and the information regarding customers and transactions must be available to the supervising authorities and the competent criminal court, upon their request.

8. REGULATORY REPORTS

BROU shall implement the necessary procedures to comply in due time and manner with the regulatory reports established by Article 550 of the RNRCSF, by Law N° 19,484 of Fiscal Transparency and its regulations, and by FATCA rules.

9. STAFF POLICIES

The implementation of staff policies that aim at reaching a high level of staff integrity and their ongoing learning and training in ML/TF/PF prevention is one of the cornerstones of the Bank's Prevention System.

9.1. KNOW YOUR EMPLOYEE POLICY

With regard to Prevention, knowing staff members is of key importance. Thus, BROU has adopted a series of measures intended to ensure a high level of staff integrity and adherence to institutional principles and values, relying on the dissemination of its Code of Ethics.

For this purpose, in accordance with article 291 b) of the RNRCSF, their personal, professional and financial background must be considered when assessing the rationale behind significant changes in their financial position or consumption behavior.

Financial correspondents providing services for BROU customers shall have policies in force consistent with this manual, in relation to: Code of Ethics, Staff Recruitment, Monitoring and Training.

9.1.1. CODE OF ETHICS

All staff members must fully comply with the provisions of the Code of Ethics, in line with the Code of Best Practice of the Bank. To this effect, they are obliged to prioritize legality and ethical principles over mere profit or the achievement of business goals. Likewise, they should avoid being in a position that may lead to a conflict between their personal interest and BROU's.

9.1.2. STAFF TRAINING

The Bank is committed to maintain its staff duly trained and updated in ML/TF/PF Prevention.

UPLA shall develop an Annual Training Program to be submitted to the Compliance Officer (C.O.) for approval. The C.O. will account for said Program to the Commission.

Newly recruited employees shall receive special training, while the particular needs of each sector shall be dealt with according to the assessments carried out.

A specific program shall be developed, which will be intended for the specialization of all UPLA employees in ML/TF/PF Prevention.

10. INDEPENDENT REVIEW OF THE PREVENTION SYSTEM

An external Audit Firm shall conduct an annual independent review of the Comprehensive Prevention System. On the basis of said review, the Audit Firm shall submit a report to the Board of Directors of BROU, expressing their opinion on the suitability and proper functioning of the ML/TF/PF prevention policies, procedures and controls. In their report, Auditors should state the most important deficiencies or omissions detected, as well as their recommendations to remedy said deficiencies, and the corrective actions adopted by the Bank.

11. PREVENTION SYSTEM MANUALS

UPLA is responsible for updating the following manuals, with the following regularity:

- ML/FT/PF Prevention Manual - annually
- Processes and Procedures Manual - annually
- FATCA Policies Manual - every four years

Contents