FINANCIAL SERVICES
AGENTE DE VALORES SA

Anti-Money Laundering, Counter-Terrorist Financing and Anti-Mass Destruction Weapons Proliferation Policies and Procedures Manual.

1 INTRODUCTION

The Anti-Money Laundering and Counter-Terrorist Financing System (hereinafter the AML/CTF System) implemented by **TPCG FINANCIAL SERVICES AGENTE DE VALORES S.A. ("TPCG FINANCIAL")** and contained in this Manual, as approved by the Board of Directors in 2019, is in line with the Company's business as a securities broker in Uruguay and accordingly complies with the general and special regulations in force in Uruguay.

1.1 Company Statement

The Board of Directors of TPCG FINANCIAL believes that Corporate Integrity, understood as systematic compliance with high ethical standards within the Company, is a source of stable value and is essential in order to preserve the community's confidence in the Company.

In this regard, policies designed to ensure compliance with anti-money laundering and counter-terrorist financing laws are a fundamental tool. That belief is embodied in this Manual, which establishes the policies to be followed in order to ensure adequate prevention and control, including procedures designed to detect and report any potential money laundering and/or terrorist financing activities and/or mass destruction weapon proliferation financing activities.

In order to be able to apply this Manual properly, all employees and officers need to be familiar with the contents hereof, the related procedures and applicable laws and regulations.

All TPCG Financial employees must comply with the provisions of this Manual. The provisions hereof shall strictly apply to any and all products and services offered by the Company. Failure to comply with the standards and guidelines contained herein will result in the applicable liability and penalties, in accordance with applicable law.

If you have any inquiries or concerns regarding application of the procedures and controls established herein, please contact the Company's Compliance Officer.

1.2 Applicable Regulatory Framework

The AML/CTF System includes prevention and control policies and procedures, as well as the Company's organizational structure designed to prevent the Company from being used in money laundering or terrorist financing maneuvers. For that purpose, this Manual is based on the provisions of Act No. 19.574, dated December 20, 2017 and the related Circular Letters and Communications issued by the Central Bank of Uruguay (hereinafter BCU). A list of all applicable regulations is included in Schedule 8 hereto.

This Manual also takes into account the main international AML/CTF standards (GAFI/FATF Recommendations, Patriot Act, OFAC provisions, CIBO Principles issued by IOSCO), to the extent applicable to securities brokers similar to **TPCG FINANCIAL**.

1.3 The Company's Business

TPCG FINANCIAL is a stock brokerage firm organized in Uruguay, with vast experience in the stock and fixed income market.

While TPCG Financial's services are mainly oriented to institutional clients, the Company's clients include both individuals and entities.

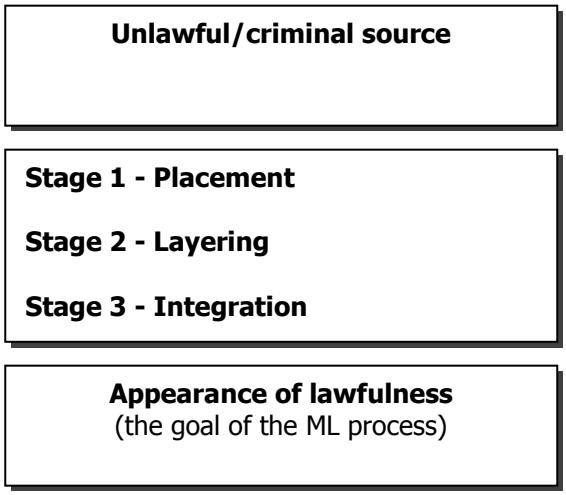
1.4 Conceptual Framework

1.4.1 Money Laundering: Definition

According to the Latin American Bank Federation, money laundering (hereinafter "ML") is "a process through which unlawful funds are integrated into the lawful economy, with the appearance of lawful funds."

- ✓ **The Money Laundering Process**

From a theoretical standpoint, ML involves three stages: placement of assets or funds, layering in order to disguise their source, ownership and location, and finally, integration of the funds.



- **Stage 1. Placement of assets or funds:** It consists of introducing cash or other valuables in the financial system or other sectors of the formal economy. In order to do that, criminal organizations use a broad range of subjects, not only in the financial system, but in other economic sectors as well.

- **Stage 2. Layering or transformation:** A series of transactions designed to disguise or hide the source of funds, by eliminating all traces and evidence of their source. Several "layers" of transactions are used in order to obscure the source of funds.

- **Stage 3. Investment, integration or enjoyment of unlawful funds:** This is the last stage of the process, where laundered money is injected back into the lawful economy, disguised as "lawful money".

✓ **<u>Unlawful or criminal source</u>**

Under the laws of Uruguay, the funds involved in ML are funds derived from the following unlawful activities:

1. The crimes contemplated in Executive Order N° 14.294, dated October 31, 1974, as amended by Act N° 17.016, dated October 22, 1998, and Act N° 19.172, dated December 20, 2013 – drug trafficking and related crimes).
2. Genocide, war crimes and crimes against humanity as defined in Act N° 18.026, dated September 25, 2006.
3. Terrorism.
4. Terrorist financing.
5. Contraband in an actual or estimated amount in excess of 200,000 UI (two hundred thousand Indexed Units).

6. Unlawful trade of weapons, explosives, ammunition or material designed for the production thereof.
7. Unlawful trade of organs, tissue or medicines.
8. Unlawful trade of men, women or children.
9. Extortion.
10. Kidnapping.
11. Pandering.
12. Unlawful trade of nuclear substances.
13. Unlawful trade of works of art, animals or toxic materials.
14. Fraud in an actual or estimated amount in excess of 200,000 UI (two hundred thousand Indexed Units).
15. Misappropriation in an actual or estimated amount in excess of 200,000 UI (two hundred thousand Indexed Units).
16. Crimes against the Public Administration as contemplated in Title IV, Book II of the Criminal Code and Act N° 17.060, dated December 23, 1998 (government corruption crimes).
17. Fraudulent bankruptcy.
18. Fraudulent insolvency.
19. The crime contemplated in Section 5 of Act N° 14.095, dated November 17, 1972 (fraudulent corporate insolvency).
20. The crimes contemplated in Act N° 17.011, dated September 25, 1998, as amended (trademark crimes).
21. The crimes contemplated in Act N° 17.616, dated January 10, 2003 as amended (intellectual property crimes).
22. The criminal behavior contemplated in Act N° 17.815, dated September 6, 2004, in Sections 77 - 81 of Act N° 18.250, dated January 6, 2008, and any criminal behavior contemplated in the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography or in connection with trade, trafficking or sexual exploitation of persons.
23. Currency counterfeiting or alteration as contemplated in Sections 227 and 228 of the Criminal Code.
24. Fraudulent insolvency proceedings, as contemplated in Section 248 of Act N° 18.387, dated October 23, 2008.
25. Tax fraud, as contemplated in Section 110 of the Tax Code, where the amount of tax fraud committed in any one fiscal year exceeds:
    A. 2,500,000 UI (two million five hundred thousand Indexed Units) in any fiscal year started on or after January 1, 2018.
    B. 1,000,000 UI (one million Indexed Units) in any fiscal year started on or after January 1, 2019.

The abovementioned amount will not apply in the case of partial or total use of ideologically or actually forged invoices or other documents in order to reduce the taxable amount or obtain a tax rebate.

In the cases contemplated in this subsection, proceedings in respect of tax fraud may be filed by administrative initiative.

26. Customs fraud, as contemplated in Section 262 of the Customs Code, where the amount involved exceeds 200,000 UI (two hundred thousand Indexed Units).

    In this case, proceedings in respect of Customs fraud may be filed by administrative initiative.
27. Homicide in the terms of Section 312(2) of the Criminal Code.
28. The crimes of serious and extraordinarily serious injuries, as contemplated in Sections 317 and 318 of the Criminal Code, if committed in the manner contemplated in Section 312(2) of the Criminal Code.
29. Theft, as contemplated in Section 340 of the Criminal Code, if committed by an organized criminal gang, in an actual or estimated amount in excess of 100,000 UI (one hundred thousand Indexed Units).
30. Burglary, as contemplated in Section 344 of the Criminal Code, if committed by an organized criminal gang, in an actual or estimated amount in excess of 100,000 UI (one hundred thousand Indexed Units).
31. Larceny, as contemplated in Section 344 bis of the Criminal Code, if committed by an organized criminal gang, in an actual or estimated amount in excess of 100,000 UI (one hundred thousand Indexed Units).
32. Theft of livestock, as contemplated in Section 258 of the Rural Code, if committed by an organized criminal gang, in an actual or estimated amount in excess of 100,000 UI (one hundred thousand Indexed Units).

    As used herein, "organized criminal gang" means a structured group of three or more people that exists over a certain period of time and acts in a coordinated manner in order to commit the relevant crimes, with a view to obtaining, directly or indirectly, a financial or other economic benefit.
33. Conspiracy to commit a crime, as contemplated in Section 150 of the Criminal Code.

Any ML-related crimes contemplated by law after the enactment of Act No. 19.574 shall be taken into account by the Company in order to refrain from doing business with customers that deal in unlawful funds.

1.4.2 Terrorist Financing: Definition

Terrorist financing has been defined by the United Nations as the activity where "*a person by any means, unlawfully and willfully, provides or raises funds with the intention that they should be used or in the knowledge that they are to be used in order to (a) carry out an act*

which constitutes an offence within the scope of and as defined in one of the existing treaties; or (b) carry out any other act intended to cause death or serious bodily injury to civilians, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of any such act, by its nature or context, is to intimidate a population, or to force a good government or an international organization to do or to refrain from doing something".

Specialists generally consider that terrorist financing comes from two main sources:

The first of these is the financial aid supplied by States or Organizations, while the second is the profit derived from revenue-generating activities. As is the case with criminal organizations, terrorist groups' funding may be derived from criminal or other unlawful activities, but it may also include revenues from legitimate sources or a combination of lawful and unlawful sources. This is a key difference between terrorist groups and other criminal organizations.

Requests for funding addressed to the community and fundraisers are a very effective way of collecting funds to finance terrorism. These fundraising activities are often conducted in the name of charitable organizations.

While it may seem logical to think that lawfully obtained funds need not be laundered, terrorist groups often need to obscure or conceal the connections between them and their legitimate funding sources. Accordingly, they need to find a way to launder those funds without attracting the authorities' attention. As a rule, terrorists and their supporting organizations use the same methods as criminal organizations when laundering money.

Another important aspect of terrorist financing, that makes it even harder to detect, is the size and nature of the transactions involved. Funding a terrorist attack not always calls for large sums of money, and terrorist-related transactions are not usually complex.

1.4.3 Relationship between Money Laundering and Terrorist Financing

While the techniques used in money laundering and terrorist financing may be similar, there are certain differences that should be taken into account at the time of applying prevention policies and procedures:

- In the case of terrorist financing, the source of funds may be lawful, while in the case of money laundering it is always unlawful.

- In the case of money laundering, the funds make an essential part of the crime itself (as a rule, at a subsequent stage, after the crime is committed). In the case of terrorist financing, the funds are channeled before a crime is committed, in preparation of the actual crime.

2 AML/CTF SYSTEM

2.1 AML/CTF System Goals

- Establish prevention and control policies and procedures that ensure full compliance with all applicable laws and regulations;
- Assure our clients that **TPCG FINANCIAL** applies the best AML/CTF practices in accordance with the main applicable international standards;
- Implement personnel policies and procedures to ensure high levels of employee integrity, as well as continuous AML/CTF training;
- Apply Due diligence policies and procedures in respect of our Customers that enable the Company to know who is the ultimate beneficiary[1] of the transactions and the source of funds;
- Keep adequate supporting documentation, so as to be able to reconstruct the relevant transactions;
- Duly report any unusual or suspicious transactions to the Financial Information and Analysis Unit (hereinafter UIAF), in the terms of Section 12 of Act 19.574 and the rules issued by the BCU (Section 202 of the Securities Market Rules (RNMV, as per the Spanish acronym) and Communication No. 2014/108);
- Duly inform the BCU's UIAF if any assets are detected in connection with individual terrorists or terrorist organizations, in the terms of Section 12 of Act 19.574 and Section 203 of the RNMV.

2.2 AML/CTF System Contents

The AML/CTF System is comprised of the following:

- AML/CTF Structure.
- Customer Due Diligence Policies and Procedures.
- Transaction Monitoring Process.
- Suspicious Transaction Reports.
- Reports to BCU.

[1] *Section 190.2 of RNMV provides that: "Ultimate beneficiary is a natural person that, directly or indirectly, owns at least 15% (fifteen percent) of the capital or other equity interests or voting rights of, or otherwise exerts ultimate control over, an entity, defined as a legal person, a trust, a mutual fund or any other estate or legal structure. Additionally, "ultimate beneficiary" is a natural person that contributes funds to close a transaction or on whose behalf a transaction is closed.*
"Ultimate control" is control exercised directly or indirectly, through several intermediaries or otherwise. In the case of a trust, this definition shall apply to the trustor, trustee and beneficiary."

- Personnel Policies and Procedures.
- AML/CTF System Independent Reviews.

3 AML/CTF STRUCTURE

3.1 Board of Directors

The Board must be fully committed to the AML/CTF System's operation, by establishing adequate policies and procedures and ensuring that they are effective. As a result, in the context of the AML/CTF process, the Board of **TPCG FINANCIAL** shall have the following responsibilities, among others:

a. Adopt a Code of Ethics and Professional Conduct, ensure that it is known and complied with, and approve any updates thereto;
b. Approve an AML Policies and Procedures Manual evidencing the AML/CTF System adopted by **TPCG FINANCIAL**, and any updates thereto;
c. On an annual basis, approve performance by the AML/CTF/WPF Committee and the Compliance Officer;
d. Appoint the Company's Compliance Officer;
e. Determine whether disciplinary action should be taken in connection with any breach of the provisions of this Manual.

3.2 AML/CTF/WPF Committee

The Committee will be the highest authority in connection with application and operation of the AML/CTF System. It will be comprised of the Compliance Officer and a representative of the Board.

The Committee will meet at the request of any member thereof or any senior officer (manager) of the Company, whenever any matter is to be considered by the Committee. Committee meetings will be held at least once every three months.

Committee meetings will be validly held with the presence of the Compliance Officer and one member of the Board. The Compliance Officer will act as Secretary at any such meetings. The Compliance Officer will introduce any matters to be considered at the meeting and will produce the related documentation.

Every member of the Committee will have the right to cast one vote. Decisions will be adopted by simple majority; in the event of a tie, the Committee member that is also a Director will have two votes.

Other Company officers or external advisors may be called to participate in Committee meetings, where they will be entitled to speak but not to vote, whenever their presence is deemed to be relevant.

Minutes of Committee meetings will be prepared, stating therein the matters considered at the meeting and any resolutions adopted thereat, as well as any matters to be followed up on.

The minutes of Committee meetings will be signed by all the attendees and will be incorporated into a special, stamp-dated book.

The Committee will have the following roles and powers:

a. Check compliance with applicable laws and regulations, as well as any general and special instructions given by the Central Bank of Uruguay;
b. Consider any and all transactions submitted to it. In this regard, the Committee will inform the Board about any such transactions that are not in line with the provisions of this Manual, as well as any unusual or suspicious behavior by Customers or Company officers;
c. Appoint officers to the Compliance department, except for the Compliance Officer;
d. Analyze and approve the Compliance Officer's Annual Work Plan;
e. Analyze and approve the Annual Training Plan;
f. Keep the Company permanently updated in AML/CTF matters, and approve the AML/CTF annual personnel training plan;
g. Analyze the monthly reports associated with monthly transaction monitoring;
h. Approve every account's Transactional Profile;
i. Diligently cooperate with the applicable governmental authorities in the investigation of ML/TF crimes, in the terms of applicable law;
j. Take note of the annual assessment report issued by independent auditors in connection with AML/CTF policies and procedures, as required by Central Bank rules, analyze any observations and/or recommendations made by independent auditors, and take any relevant corrective action.

3.3 Compliance Officer

TPCG FINANCIAL's Compliance Officer will be responsible for implementing, following up on and monitoring performance of the AML/CTF System.

The Compliance Officer's hierarchy will be in accordance with his responsibilities; he will have access to all areas of the Company and will be entitled to require cooperation from any Company officer. Also, the Compliance Officer may retain the services of external providers in order to better discharge his duties, with the Board's prior approval.

The Compliance Officer shall be properly trained as necessary to discharge his duties.

The Compliance Officer will have the following roles and powers:

a. Check compliance with all prevention and control procedures adopted by the Company;
b. Assess the effectiveness of the AML/CTF System and its conformity with applicable laws and regulations, and inform the Board about the need or advisability to amend them;
c. Take note of any transactions, regardless of their amount, that should be regarded as unusual because of their features (complexity, lack of apparent legal or financial justification, etc.) or because of the relevant Customer's behavior;
d. Analyze any such unusual transactions and, if the Compliance Officer deems it necessary, forward the matter to the Committee. For purposes of this analysis, the Compliance Officer shall obtain any and all documentation related to the transaction and shall review the information contained in the relevant Customer File, as well as the customer's previous behavior, and shall generate a background file;
e. Discharge the obligation set forth in Section 12 of Act 19.574 and the regulations issued by the BCU (Section 202 of the Securities Market Rules (RNMV, as per the Spanish acronym) and Communication No. 2014/108), and report any unusual or suspicious transactions to the BCU's Financial Information and Analysis Unit;
f. Inform UIAF if he detects any assets associated with individual terrorists or terrorist organizations, in the terms of Section 12 of Act 19.574 and Section 203 of the RNMV (Terrorist-Related Assets Report);
g. Participate in the establishment of any new business relationships;
h. Along with a Customer's Account Manager, update the relevant Customer's information and/or documentation;
i. Analyze any transaction monitoring reports;
j. Develop management reports based on the results of monthly transaction monitoring, and submit those to the Committee for information purposes;
k. Prepare the Company's risk matrix and keep it updated,
l. Prepare the Compliance Officer's Annual Work Plan, to be submitted to the Committee;
m. Plan and lead AML/CTF training sessions. In this regard, the Compliance Officer shall prepare an Annual Training Plan and shall submit it to the Committee;
n. On an annual basis, assess performance of the activities contemplated in the Annual Work Plan and the Annual Training Plan, after the end of the relevant year; prepare the related reports and submit them to the Committee for information purposes;
o. On an annual basis, assess all employees in order to detect any relevant changes in their behavior, lifestyle or purchasing habits. Express evidence of this assessment shall be included in each employee's file;
p. Report any Financial Transactions to the BCU, for them to be included in the BCU's database (Section 204 of RNMV);
q. Duly inform the BCU about any cross-border transportation of moneys, precious metals or other monetary instruments in excess of USD 10.000, pursuant to the provisions of Section 206 of the RNMV (Cross-Border Transportation of Valuables);

r. Provide guidance as to retention of AML-related documents, so that they can be properly filed and safeguarded, and are readily accessible;
s. Fully cooperate with independent auditors;
t. Follow up on any recommendations and instructions given by the Securities Market Department of the Central Bank of Uruguay, UIAF, or independent auditors;
u. Act as a liaison with the Financial Information and Analysis Unit of the Central Bank of Uruguay and other authorities of competent jurisdiction;
v. Diligently cooperate with the authorities of competent jurisdiction in the investigation of any ML/TF crimes, in accordance with the laws of Uruguay;
w. Ensure that this Manual is duly updated, in line with any changes in applicable law and the Company's business, and submit it to the Board for approval.

3.4 Compliance Unit

The Compliance Unit is comprised of all human resources available to the Compliance Officer in order to discharge his AML/CTF/WPF duties.

Assistants to the Compliance Officer will be officers duly trained in AML/CTF/WPF matters, who shall do the work entrusted to them by the Compliance Officer in order to ensure effective operation of the Compliance Unit.

4 CUSTOMERS

4.1 Customer: Definition

Customer means any individual or entity with whom **TPCG Financial** establishes or maintains a legal or contractual relationship, as a result of services rendered or products sold in the context of the Company's business and in accordance with applicable legal and regulatory provisions.

Because of the nature of its business, **TPCG FINANCIAL** has two types of customers:

- institutional clients and
- customers.

4.2 Due Diligence Policies and Procedures

Customer due diligence policies and procedures established by **TPCG FINANCIAL** are designed to achieve the following goals:

- Identify, verify and record a customer, the ultimate beneficiary of the customer's funds, or their regulator, as the case may be;
- Be aware of the business from which the funds arise that are associated with any services provided by the Company;
- Classify customers in terms of the associated ML/TF risk, and apply enhanced due diligence procedures in the case of higher-risk customers;
- Monitor transactions in order to detect any unusual or suspicious behavioral patterns.

4.3 Customer Acceptance Policy

It is a policy of TPCG Financial not to establish or maintain a business relationship with individuals or entities designated by Uruguay as allegedly linked to unlawful funds movements and generally, any individuals or entities in respect of which doubts exist as to the legality of their business or professional activities.

In this regard, TPCG Financial will not establish a business relationship with any of the following individuals or entities:

a. Individuals prosecuted or convicted for ML-related crimes, in the terms of the laws of Uruguay;

b. Individuals or entities identified as terrorists or members of terrorist organizations in the lists kept by the United Nations;
c. Individuals declared to be terrorists by a final court decision, in Uruguay or abroad. Any such court decision must be publicly known or must be notified to the Company;
d. Individuals or entities included in OFAC lists;
e. Individuals or entities that fail to meet the Due Diligence requirements established in this Manual. On an exceptional basis, a business relationship may be established with a person that fails to meet the due diligence requirements, where failure to establish a relationship would operate to alert the client. Any such situation shall be immediately reported to UIAF, in accordance with the procedure described in this Manual;
f. Individuals or entities that were included by the Company in a Suspicious Transaction Report ("ROS", as per the Spanish acronym), whose accounts the Company's Management resolves to close;
g. Entities that are "Shell Banks", defined as a bank that:
    - does not do business at its registered office in the jurisdiction where it is authorized to operate.
    - does not have any one or more full-time employees at its registered office.
    - does not keep transaction records at its registered office, and
    - is not subject to supervision by the banking authority that issued the bank's license to do business.

4.4 Institutional Clients - Due Diligence Policies and Procedures

4.4.1 Definition

A legal person that, while not intending to open an account and/or give assets in custody to a broker, engages in securities transactions with the broker, which are settled on a "versus payment" basis through a securities clearing service such as Euroclear/DTC etc.

4.4.2 Due Diligence

TPCG FINANCIAL will operate only with domestic and foreign institutional clients that comply with the customer acceptance policy established by the Board in this Manual.

In order to start operations with an Institutional Client, the Company must obtain at least the following information:

- Name.
- Registered office.
- Settlement instructions.
- Evidence of powers of attorney.

- Supporting documentation in order to establish whether or not the client is AML/CTF regulated.
- Financial and economic information.

In this regard, Institutional Clients will be asked to fill in an Institutional Client File ("*Ficha*") (Schedule 1.1), which must be duly dated and signed.

If a counterparty is regulated and supervised, the information required in order to start operations with the Company may be replaced, at least in part, by information that is publicly available on the website of the counterparty and/or the applicable regulatory/supervisory authority.

Additionally, an Institutional Client's File shall contain the following internal documentation:

- "*Resumen Contrapartes Institucionales*" for (Schedule No. 1.2), containing proof of any checks and controls run by the Compliance Officer and approval of the business relationship by the applicable Company officers,
- Proof of background check (UN, OFAC and other lists; web searches, etc.),
- Detailed Report ("*Informe Circunstanciado*") (Schedule No. 1.3), completed and signed by the Account Representative, for any clients subjected to enhanced due diligence procedures (paragraph 4.3.5).

4.4.3 Institutional Clients: Background Check

The following checks shall be run by the Compliance Officer in order to accept a new Institutional Client:

- Cross-referencing against OFAC, UN and other lists

At the beginning of a business relationship, an Institutional Client and its senior management will be checked against OFAC and UN lists, among others. This service is outsourced by the Company.

If any match is detected between a potential Client or other parties involved in the relevant transaction and the names included in OFAC or UN lists, additional information must be obtained in order to establish whether or not any such entities or individuals are actually included in those lists.

If in spite of any such additional information, it remains unclear whether an entity or individual is included in an OFAC or UN list, or if their inclusion in the list is confirmed, the transaction shall not be closed, and the matter shall be immediately informed to the Compliance Officer, who shall consider whether a Suspicious Transaction Report needs to be generated.

- Identification of Politically Exposed Persons

The Company must establish whether a potential Institutional Client is related (as a family member or close associate) to a Politically Exposed Person[2] (PEP). In that case, the Client shall be classified as High Risk, and shall be subjected to the Enhanced Due diligence process (paragraph 4.3.5).

PEPs shall be identified by checking a database supplied by a third-party vendor.

4.4.4 Institutional Clients: Transactional Profile

An Institutional Client's Transactional Profile is defined by reference to the total assets managed annually, as follows:

Risk Level	Transactional Profile
Low	10% financial assets turnover
Medium	5% financial assets turnover
High	1% financial assets turnover

In order to implement a formula, we have assumed a 500% turnover for Broker Dealers (securities brokers and brokerage firms), 100% for Mutual Funds and 300% for Hedge-Funds/Family-Office/Investment Advisors.

In the case of transactions with several mutual funds managed by the same manager, a limit

[2] *In the terms of Section 196 of the RNMV, a Politically Exposed Person is anyone who "holds or has held at any time over the last 5 years a relevant public position in Uruguay or abroad, such as: heads of state or government, senior politicians, senior members of the government, the judiciary or the military, members of the Senate or the House of Representatives, senior political party members, directors and senior managers of state-owned companies and other public-sector entities. The notion of Politically Exposed Person includes also anyone who holds or has held at any time over the last 5 years a senior position in an international organization, such as: senior managers, directors, deputy directors, members of the board or equivalent positions."*

will be established for it ("Asset Manager" or Investment Advisor). For purposes of automated transaction monitoring, the limit may be distributed among the various Funds managed by the same manager, provided that they are AML/CTF regulated.

4.4.5 Institutional Clients: Risk-based Categories

Institutional Clients will be categorized as low, medium or high risk, based on the following risk factors:

a. AML/CTF Regulated

A high risk will be deemed to exist where an institutional client is not subject to AML/CTF regulation.

In the case of Asset Managers/Investment Advisors, the determining factor will be whether or not they or the designated manager and/or any entity performing that role in connection with the Mutual Funds managed by them and/or with which they operate, are AML/CTF regulated.

b. AML/CTF Risk Jurisdiction

A high risk will be deemed to exist where an institutional client operates in a high-risk jurisdiction in terms of ML/TF that is included in the following FATF lists:

- Non-cooperative countries.
- High-risk countries.

c. Negative Track Record

A medium risk will be deemed to exist where an institutional client has a relevant publicly known negative track record in terms of ML/FT.

Finally, a low risk will be deemed to exist where none of the abovementioned risk factors exist.

Clients will be categorized as follows:

Risk Level	Risk Factors
Low	None

Medium	Negative AML track record
High	**Non-regulated and/or NON-FATF jurisdiction**

4.4.6 Institutional Clients: Due Diligence Levels

Due diligence requirements are related to the risk involved by an institutional client, as follows:

Risk Level	Knowledge
Low	Transactional Profile
Medium	+ Satisfactory Explanation by the Client
High	**+ Detailed Report**

4.4.7 Enhanced Due Diligence Procedures

Relationships with high-risk Institutional Clients will be subject to Enhanced Due Diligence procedures. In these cases, in addition to the generally applicable process (paragraphs 4.3.1 - 4.3.4), the following additional procedures shall apply:

a. The relationship will require the approval of a Board member and the "green light" of the Compliance Officer[3];
b. A detailed report must be prepared, describing all the factors considered when establishing the Client Transactional Profile (Schedule 1.3). The report must be backed by supporting documentation that enables the Company to establish the Client's economic and financial condition (Financial Statements and the related CPA report, tax returns, or other relevant documentation).

[3] In the case of existing clients as of the effective date of this Manual, the approval of a Board member and the green light of the Compliance Officer will be required in order to continue to operate with any such clients.

In the case of a Detailed Report concerning an Institutional Client located in a NON-FATF Jurisdiction, special attention shall be paid to the quality of the regulator and regulations applicable to the Client, as well as the existence of an AML/CTF program.

In the case of a Detailed Report concerning an unregulated Institutional Client organized in a FATF jurisdiction, the information to be included will depend on the type of institutional client involved (Mutual Fund, Broker, Hedge Fund, Family Office, etc.) and may include, among other things, documentation concerning the client's shareholders/ managers, history, business type and volume, profile of the client's clients.

c. A more stringent update policy shall apply, as provided in paragraph 4.5 below;
d. The relationship must be more closely monitored in terms of the quality and frequency of controls.

4.4.8 Institutional Clients: Client Acceptance

In order for a client to be accepted, the full Institutional Client file shall be supplied by the Compliance Officer to the relevant authorizers. For that purpose, the Compliance Officer shall first check that all the requisite information is included in the file, as well as proof of the verifications done.

In the case of a High Risk Institutional Client, in accordance with the Enhanced Due Diligence procedures, acceptance of the new client must be greenlighted by the Compliance Officer.

Express evidence of approval (date and signature of the relevant officer) shall be included in the "*Resumen Contrapartes Institucionales*" form (Schedule No. 1.2).

4.5 Customers - Due Diligence Policies and Procedures

Definition:

Customer means any individual or entity that holds an account with TPCG Financial and accordingly has met all the due diligence requirements described in this Manual. TPCG Financial will provide securities brokerage, investment advice and custody services to these customers.

Due Diligence

In order to establish a new account, the following information and documentation must be obtained from a potential Customer and included in the Customer File.

a. Individuals

- Natural Person Account Opening Form (Schedule No. 2.1), duly filled in, dated and signed by the Customer (accountholder). At least the following data must be supplied by the customer:
  - name in full;
  - date and place of birth;
  - ID type, number and country of issuance;
  - tax registration number in the customer's jurisdiction, where applicable;
  - marital status (if the customer is married or in a common law marriage, the name and ID number of their spouse/common law spouse must be supplied);
  - address and telephone number;
  - profession, occupancy or main line of business;
  - amount of income.
- Proof of address.
- Copy of the Customer's ID or passport and those of the Customer's attorneys in fact and individuals authorized to operate the account, or proof of inquiry from some source of official information;
- Copy of the ID or passport of the account's ultimate beneficiary[4], or proof of inquiry from some source of official information, where applicable;
- Powers of attorney or other documentation evidencing the existence of attorneys in fact and individuals authorized to operate the account, where applicable.
- Supporting documentation in respect of the Customer's business and source of funds, in the case of customers subject to Enhanced Due Diligence.
- Copies of tax returns or other documentation filed with the tax authorities, in the case of customers subject to Enhanced Due Diligence.

The Customer Record ("*Ficha de Cliente*") must include a statement as to whether a customer acts on his own behalf or on behalf of a third party and, in the latter case, all the abovementioned information must be obtained in respect of the ultimate beneficiary.

b. Entities

- Legal Person Account Opening Form (Schedule No. 2.2), duly filled in, dated and signed by a customer representative. At least the following data must be supplied by the customer:
  - Company name;

4 Ultimate beneficiary is a natural person that, directly or indirectly, owns at least 15% (fifteen percent) of the capital or other equity interests or voting rights of, or otherwise exerts ultimate control over, an entity, defined as a legal person, a trust, a mutual fund or any other estate or legal structure. Additionally, "ultimate beneficiary" is a natural person that contributes funds to close a transaction or on whose behalf a transaction is closed (Section 15 of Act No. 19.574).

- Date of organization;
- Registered office and telephone number;
- Tax registration number;
- Main line of business;
- Amount of revenues;
- Ownership and control structure, including the identity of the company's shareholders or owners and the name of the company's ultimate beneficiary or controlling person (if different from the shareholders/owners). The identity of any shareholder or owner must be disclosed who holds in excess of 15% of the company's equity interests.

Any individuals associated with the account, whether as ultimate beneficiaries, representatives, attorneys in fact or individuals authorized to operate the account held at **TPCG FINANCIAL**, shall provide their personal data as part of the company's Customer Record.

- Proof of address.
- By-laws, operating agreement or other documentation evidencing the company's existence and registration with the relevant Registry.
- Copies of any documents evidencing the powers of the company's representatives and any individuals authorized to operate the account (minutes of Board meetings, powers of attorney, etc.).
- Copy of the ID (or proof of inquiry from some official source of information) of the ultimate beneficiaries, representatives, attorneys in fact and individuals authorized to operate the company's account, where applicable.
- Proof of registration of the ultimate beneficiaries with the relevant Registrar.
- Supporting documentation in respect of the Customer's business and source of funds, in the case of customers subject to Enhanced Due Diligence.
- Copies of tax returns or other documentation filed with the tax authorities, in the case of customers subject to Enhanced Due Diligence.

The information referred to in 1) above must be obtained from the ultimate beneficiary. Additionally, the same information must be obtained from any individuals acting as representatives, attorneys in fact or individuals authorized to operate the account held at **TPCG FINANCIAL.** Information concerning the amount of revenues will be requested only where those revenues are the source of the funds held in the account.

Additionally, a Customer File (for both Individuals and Entities) shall contain the following internal documentation:

- Proof of background check (UN, OFAC and other lists; web searches, etc).
- Detailed Report form (Schedule No. 2.5). This requirement shall be mandatory for clients subject to Enhanced Due Diligence (high-risk clients, or clients that operate substantial amounts).

- "Customer Summary" ("*Resumen Clientes*") form (Schedule No. 2.3 and 2.4), dated and signed by the Compliance Officer (as proof of the verifications made) and the Account Representative (as evidence of approval of the new Customer).

On the other hand, when an account is first opened and whenever funds or securities are deposited into the account, a Customer shall fill in a Statement of Source of Funds (Schedule No. 3), stating therein that the relevant funds or securities are not derived from unlawful activities. This statement shall be included in the Customer File.

4.5.1 Customer Identity Check

The identity of a Customer (accountholder/s) and the account's ultimate beneficiary[5] (where applicable) must be determined, recorded and checked by means of supporting documentation.

For that purpose, copies of the relevant identity documents shall be obtained and kept as part of the Customer File.

Any such identity documents must be issued by a governmental authority, must be valid and must contain a recent photograph that enables the Company to identify the relevant individual.

For purposes hereof, a valid ID is an identity document (for Uruguay and MERCOSUR member countries) and/or passport, as the case may be.

A business relationship shall not be finally established unless and until all the customer identification procedures have been completed. Any of the following mechanisms may be selected for that purpose:

TYPE OF CLIENT	AMOUNT[6]	FACE-TO-FACE VERIFICATION
a) **Customers engaged in business** (individuals and entities engaged in commercial, industrial, agricultural, financial, professional or other	Annual transactional profile or Accumulated transactions in a calendar year	**Personal contact** with the **accountholder, representative or attorney in fact** **Contacted by:** Company personnel or third

[5] The ultimate beneficiary need not be identified in the case of customers whose shares are listed on a domestic stock exchange or a reputable foreign stock exchange, or are directly or indirectly owned by companies whose shares are so listed, provided that any such shares are available for immediate purchase or sale in the relevant stock markets. This exception shall apply to listed securities only.

[6] In order to calculate the applicable thresholds, the full amount deposited or to be deposited in the account will be considered.

activities)	**in excess of USD 1,500,000**	parties (Section 198 – DDC Outsourcing).
	Annual transactional profile or Accumulated transactions in a calendar year **in excess of USD 120,000.**	**Personal contact** with the **accountholder, representative or attorney in fact** Contacted by: **Another domestic or foreign FI** registered as such with the relevant regulatory authority in the FI's jurisdiction or **A Notary Public** or the equivalent in the relevant jurisdiction.
b) **Customers not engaged in business (investment vehicles, holding companies, etc)**	Annual transactional profile or Accumulated transactions in a calendar year **in excess of USD 500,000 (NON-RESIDENTS)**	**Personal contact** with **any one of the ultimate beneficiaries** Company personnel or third parties (Section 198 – DDC Outsourcing).
	Annual transactional profile or Accumulated transactions in a calendar year **in excess of USD 120.000**	**Personal contact** with **any one of the ultimate beneficiaries** Contacted by: **Another domestic or foreign FI** registered as such with the relevant regulatory authority in the FI's jurisdiction or

		A Notary Public or the equivalent in the relevant jurisdiction.

Where a client's identity is checked by the Company's personnel, a statement to that effect must be included in the copy of the client's ID.

4.5.2 Customer Background Check

In order to onboard a new Customer, the following checks shall be run by the Compliance Officer:

- Cross-referencing against OFAC, UN and other lists

Before a customer is admitted, all the parties involved (accountholders, representatives and individuals authorized to operate the account, controlling members or shareholders, and ultimate beneficiaries) shall be checked against OFAC and UN lists, among others, by a third-party service provider.

In the event that any matches are detected between the name of a potential client (individual or entity) or other parties involved in the relevant transaction (representatives, attorneys in fact/individuals authorized to operate with **TPCG Financial**, ultimate beneficiaries, wire transfer beneficiaries), additional information shall be obtained in order to establish whether or not any such individuals or entities are actually included in OFAC, UN or other lists (name in full, ID number, date o birth, among others).

If in spite of any such additional information, it remains unclear whether an entity or individual is included in an OFAC or UN list, or if their inclusion in the list is confirmed, the transaction shall not be closed, and the matter shall be immediately informed to the Compliance Officer, who shall consider whether a Suspicious Transaction Report needs to be generated.

- Identification of Politically Exposed Persons

TPCG Financial needs to establish whether or not a potential Customer or ultimate beneficiary is a Politically Exposed Person[7] (PEP), or a family member or close associate of

[7] *In the terms of Section 196 of the RNMV, a Politically Exposed Person is anyone who "holds or has held at any time over the last 5 years a relevant public position in Uruguay or abroad, such as: heads of state or government, senior politicians, senior members of the government, the judiciary or the military, members of the Senate or the House of Representatives, senior political party members, directors and senior managers of state-owned companies and other public-sector entities. The notion of Politically Exposed Person includes also anyone who holds or has held at any time over the last 5 years a senior*

any such PEP. If that is the case, the Customer shall be regarded as High Risk, and the Enhanced Due Diligence procedure shall apply (paragraph 4.4.5).

Two mechanisms have been established by **TPCG Financial** in order to identify PEPs:

i) the statement made by the Customer in the Customer Record at the time of opening an account, where the Customer must disclose any governmental positions held at any time over the last five years,
ii) a third-party provider's database.

- Other checks

No new Customers will be admitted without at least one personal and/or banking reference.

4.5.3 Customer Business and Profile

Information shall be obtained about the Customer's business or profession and the source of any funds to be held in the account, in order to define the Customer's Profile.

Both quantitative (potential transaction volume) and qualitative (nature of the transactions to be closed) parameters shall be considered in order to determine a Customer's profile.

The chart below summarizes the parameters to be considered when establishing a Customer's Transactional Profile:

Customer	Transactional Profile (TP)	Transactional Profile adjusted by Risk
Individual	Economic condition (liquid funds) (2) Low Risk=TP	Low Risk = TP Medium Risk = TP x 0.9 High Risk = TP x 0.8
Entity	15% net profits (3) + liquid funds (4)	

The following information shall be considered when establishing a Customer's Transactional Profile:

position in an international organization, such as: senior managers, directors, deputy directors, members of the board or equivalent positions."

(1) Economic condition: The customer's liquid funds (savings). This information shall be obtained from the Statement of Assets submitted by the customer, with the signature thereon certified by the CPA Association, or by any other means whereby a Customer's economic condition may be established, such as certification of revenues, invoices issued over the last two months, pay stub, proof of retirement payments, or other supporting documentation in respect of a customer's income.

(2) Net Profits as per the customer's audited annual financial statements.

(3) Liquid funds: the most liquid funds that make part of a Customer's Assets (such as Cash & Banks, Financial Investments, etc.).

Where a Customer transacts substantial amounts or is regarded as High Risk, in accordance with Enhanced Due Diligence procedures, the Customer's Transactional Profile shall be stated in the "Detailed Report" (Schedule No. 2.5), including a description of the factors considered in order to determine the Transactional Profile, such as:

- ✓ Manner how the Customer first became a customer, or number of years of the business relationship with him, as the case may be;
- ✓ Description of the Customer's business or profession and source of funds (especially where the funds in question are not derived from the business or profession informed by the Customer);
- ✓ Description of the factors considered when establishing the Customer's transactional profile (products or services that a Customer uses or expects to use, reason for the transactions, expected amounts);
- ✓ Description of any available supporting documentation.

For these purposes, the following amounts shall be regarded as **Substantial Amounts,** depending on the type of customer involved:

Type of Customer	Assets Under Management
Individuals	USD 800,000
Entities	USD 3,000,000

Also, the report must be backed by supporting documentation that enables **TPCG Financial** to establish a Customer's economic and financial condition or explain the source of funds handled by the Customer (audited financial statements, tax returns, proof of distribution of profits, contracts of purchase/sale or other documentation). Additionally, copies must be

obtained of any tax returns or equivalent documentation filed with the relevant tax authority.

TPCG Financial may resort to publicly available information or private-sector providers in order to obtain information for the purpose of checking a Customer's activities generally or any specific transactions.

Special Circumstances

In the event that the source of any particular funds is a specific transaction (e.g. sale of real property), a customer may produce specific related documentation to explain the source of funds:

Source of funds as reported by the Customer	Requisite document
Sale of real estate	Copy of the notarized deed of sale or bill of sale, where a reference is included to payment made
Sale of vehicles	Certified copy of the bill of sale
Severance payment/insurance claim	Copy of the payment certificate issued by the insurer or employer
Retirement benefits	Copy of the relevant receipt
Gambling	Copy of a certificate issued by the gambling establishment, stating that the customer has won and the amount of his winnings
Special bonuses	Copy of the relevant receipt

All such information and documentation obtained or prepared as part of the Due Diligence process shall be included in the Customer File, as well as any checks made. This information shall be regularly updated.

4.5.4 Direct Customers: Risk Categories

Three risk categories have been defined by **TPCG Financial** as far as ML is concerned: High Risk Customers, Medium Risk Customers and Low Risk Customers.

In order to establish a Direct Customer's category, several risk factors are considered and weighed in accordance with their relative importance. The chart below summarizes the risk factors considered and their relative weight:

Risk Factor	Weight
Line of business	30%
PEP	30%
Country of residence	10%
Country of organization or birth	5%
The Customer transacts Substantial Amounts	25%
	100%

Customer Risk Rating

A Customer's risk category will depend on the final rating obtained.

Risk Category	Final rating
High Risk	30
Medium Risk	20
Low Risk	0

To the extent that a single factor involves various degrees of risk for a Customer, certain charts have been developed where different risk categories are assigned within each such factor. The relevant charts and the internal rating associated with each risk factor are included in Schedule No. 4 hereto.

4.5.5 Enhanced Due Diligence Procedures

High-risk customers, counterparties and transactions will be subject to Enhanced Due Diligence procedures.

Without prejudice to the risk categories allocated by **TPCG Financial**, the following shall be regarded as high risk:

- Business relationships and transactions with non-residents located in countries that fail to comply with international AML/CTF standards,
- Transactions by persons that are not regularly in personal contact with TPCG Financial,
- Politically Exposed Persons, their family members and close associates,
- Any unusual transactions in terms of **TPCG Financial**'s standard practice.

The following procedures shall apply to High Risk Customers, in addition to the applicable general Due Diligence procedure (paragraphs 4.4.1 - 4.4.4):

a) The relationship with the Customer shall be approved by a member of the Board and greenlighted by the Compliance Officer[8].

b) A Detailed Report including the transactional profile allocated to the Customer, and describing the factors considered when determining the transactional profile. The report must be backed by supporting documentation that enables **TPCG Financial** to establish the Customer's economic and financial condition and the source of any funds handled by the Customer (audited financial statements, tax returns, proof of distribution of profits, contracts of purchase/sale or other documentation).

c) Copies of any tax returns or equivalent documentation filed with the applicable tax authority. This requirement shall not apply to Politically Exposed Persons whose annual transactions, in accordance with their respective transactional profile, are under USD120,000 (one hundred twenty thousand U.S. dollars) or the equivalent amount in other currencies, or who transact up to that amount in any given calendar year. In that case, the requisite documentation shall be the documentation that enables **TPCG Financial** to determine the Customer's economic and financial condition or explain the source of any funds handled by the Customer. The Customer's accumulated transaction volume shall be considered in order to determine the applicable threshold.

d) The customer's information must be updated more frequently, as provided in paragraph 4.6 below;

e) The relationship with the customer must be monitored more closely, with more frequent controls.

f) Additional information must be obtained for certain types of customers, products or services (paragraph 4.6).

The requirements set forth in (b) and (c) above shall also apply to customers that transact Substantial Amounts.

4.5.6 Customer Acceptance

In order for a customer to be accepted, the relevant Customer File shall be supplied by the Compliance Officer to the relevant authorizers. For that purpose, the Compliance Officer shall first check that all the requisite information is included in the file, as well as proof of the verifications done.

[8] In the case of existing clients as of the effective date of this Manual, the approval of a Board member and the green light of the Compliance Officer will be required in order to continue to operate with any such clients.

In the case of a High Risk Customer, in accordance with the Enhanced Due Diligence procedures, acceptance of the new customer must be greenlighted by the Compliance Officer.

Express evidence of approval (date and signature of the relevant officer) shall be included in the "*Resumen Clientes*" form (Schedule No. 2.3 and 2.4).

4.6 Customer Information Update and Retention Policies

Information update and retention policies shall apply to both Direct Customers and Institutional Clients.

4.6.1 Customer Information Updates

Any and all information and documents obtained or prepared in the context of the Customer Due Diligence process shall make part of the relevant Customer File and shall be regularly updated as follows:

Type of Customer	Frequency of updates
High Risk	Annual
Transacts Substantial Amounts	Every two years
Medium Risk	Every three years
Low Risk	Every five years

Notwithstanding the above, any such information shall be updated whenever any outdated or inadequate information is detected, in the light of **TPCG Financial**'s direct relationship with a customer or as a result of transaction monitoring efforts.

The Compliance Unit shall be responsible for updating any such information, in coordination with the Compliance Officer. The update process involves a comprehensive review of the relevant Customer File in order to detect any need to update the Customer's information and/or documentation. In particular, each such review shall involve the following activities:

- Checking that a customer's information is updated and no relevant changes have occurred, such as: change of address, change or expansion of a customer's business, changes in a legal person's ownership structure or representatives.
- Reviewing the Customer's Transactional Profile, and suggesting any applicable changes;
- Where applicable[9], checking that a customer's economic and financial information is updated, and that the customer has provided **TPCG Financial** with the latest tax return or equivalent documentation filed with the tax authority,

[9] This requirement is mandatory in the case of clients who are subject to Enhanced Due Diligence procedures (High-Risk Customers and customers that transact Substantial Amounts).

- Checking money laundering risk parameters.

4.6.2 Customer Documentation Retention

The following documentation shall be adequately retained:

- Any information and documentation obtained or prepared in the context of a Customer's Due Diligence process, including copies of documents and forms requested at the time of opening the Customer's account, shall be retained for a term of at least 5 years after the relationship with a Customer is terminated;
- Supporting documentation in connection with any transactions shall be retained for a term of at least 5 years after the relationship with a Customer is terminated;
- Documentation regarding Suspicious Transaction Reports filed by **TPCG Financial** shall be retained for a term of at least 10 years after the date of the relevant Report.

4.7 Special Due Diligence Procedures

4.7.1 Outgoing transfers

Where a Customer requests an outgoing transfer of funds or securities outside of Uruguay, the following steps shall be taken:

- The Customer shall submit a written instruction, duly signed by the accountholder or by a representative or an individual authorized to operate the account, identifying therein the Transferor (customer name, account number), the Beneficiary Bank (name, ABA/SWIFT), Intermediary Bank (where applicable) and the ultimate beneficiary of the relevant funds (name, account number, address).
- **TPCG Financial** shall check that the account where the funds or securities are to be credited (beneficiary) is held by the Customer or a company controlled by the Customer. Where the ultimate beneficiary of the transfer is a third party, the Customer shall explain the reasons for the transaction and shall provide supporting documentation in that regard. Even if supported by adequate documentation, payments to third parties may be made solely in exceptional cases and must be duly justified, and greenlighted by the Compliance Officer.

Where a transfer is instructed by a Correspondent Bank, the actual transferor (ultimate beneficiary) must be properly identified by the Correspondent Bank.

Before any such transaction is authorized, the Compliance Officer shall cross-reference all the individuals and entities involved in the transaction (the Customer, the actual transferor (ultimate beneficiary), and any Correspondent Banks) against UN, OFAC and other applicable lists, by using the services of a third-party provider.

4.7.2 Customers that Handle Third-party Funds and are not Subject to Financial Regulation or Supervision

Special attention shall be paid to the customer's business, in order to determine whether it might involve transactions on behalf of third parties.

Pursuant to Central Bank rules (Section 197 of the RNMV), this category includes any individuals or entities "*that regularly handle third-party funds derived from or related to the following professional, financial, commercial or savings activities*:

- *Real estate purchase, sale, construction, promotion, investment or management,*
- *Purchase and sale of business establishments;*
- *Management or custody of moneys, bank accounts, securities or other assets;*
- *Investments and financial transactions generally;*
- *Establishment, operation or management of legal persons or other entities;*
- *Foreign trade transactions where any amounts are paid or collected on behalf of third parties".*

This provision does not include any transactions or accounts that involve third parties' funds by reason of fees or commissions only.

Any customers that regularly handle third-party funds shall be specially monitored, in the light of the higher risk involved. Accordingly, enhanced due diligence procedures shall apply whenever:

a. Transactions are closed in an excess of USD 600,000 in any calendar year. In order to determine the accumulated amount, **TPCG Financial** shall consider the aggregate amount deposited into the account; in the case of transactions not associated with an account, **TPCG Financial** shall consider their accumulated amount minus the amount of any transactions related to another transaction.

   As part of the enhanced due diligence process, **TPCG Financial** shall establish the identity of the ultimate beneficiary of any transaction in excess of USD 10,000. Alternative procedures may be established for that purpose; for example, by means of regular reports where a customer states the amounts transacted in a given period and identifies each and every ultimate beneficiary.

Follow-up efforts in connection with these customers should enable **TPCG Financial** to monitor the transactions accumulated by each ultimate beneficiary.

Enhanced due diligence procedures shall apply immediately after the threshold is exceeded. In the following calendar year, enhanced due diligence procedures shall apply from the beginning of the year, except where **TPCG Financial** determines that the threshold was exceeded as a result of a specific transaction, and not as part of the customer's expected profile.

b. The customer carries out any individual transaction in excess of USD 50,000.

At least the following information shall be obtained in order to identify a transaction's ultimate beneficiary:

- Name in full,
- Copy of the identity document[10],
- Address.

Where warranted by the risk involved in the transactions or the accumulated amount thereof, additional information shall be requested about the transactions' ultimate beneficiary and the source of funds.

Additionally, the name of the beneficiary shall be cross-referenced against UN and OFAC lists, among others.

Where a Customer refuses to provide information about a transaction's beneficiary, the transaction shall be analyzed in depth in order to establish whether a Suspicious Transaction Report (ROS) is warranted (paragraph 6.1 of this Manual). If it happens again, the Compliance Officer shall additionally consider the advisability of restricting and even terminating the Company's relationship with that Customer.

[10] This requirement may be disregarded when the particulars of the parties involved arise clearly from a transaction's supporting documentation.

5 TRANSACTION MONITORING PROCESS

The monitoring process described below shall apply to all TPCG clients (Institutional Clients and Customers).

The monitoring system is designed to follow up on transactions by **TPCG FINANCIAL's** clients, with an emphasis on high-risk clients.

TPCG FINANCIAL's monitoring process is divided in two categories: decentralized and centralized monitoring.

5.1 Decentralized Monitoring

In the course of their duties, all **TPCG Financial** Employees shall be on the alert to detect and report any unusual transactions.

Account Representatives must pay attention to any red flags associated with Customer transactions or behavior; they must check the transactions carried out by Customers in order to detect any transactions that may seem unusual because of the transaction amount, type, frequency or counterparty involved.

5.2 Centralized Monitoring

Customer transactions will be monitored by the Compliance Unit in order to determine whether they are in line with the relevant Customer's Transactional Profile.

On a daily basis, the Compliance Officer will receive a list of the day's transactions from Back Office, including: amount, currency, type of transaction, counterparty / customer.

If any unusual transaction is detected, the Compliance Officer may request additional information in order to explain it. A detailed analysis will be made in order to determine whether the transaction can be satisfactorily explained or whether an investigation should be started.

Additionally, on a monthly basis, the Compliance Unit will check the volume transacted by customers against their transactional profile in order to detect any unusual transactions. Any deviations shall be analyzed by the relevant Account Representative, in order to determine whether the transaction involved is unusual or suspicious.

In the light of the analysis made, which must be based on the information obtained as part of the relevant Customer's Due Diligence process, the Account Representative shall take and duly record one of the following courses of action:

- If the Account Rep understands that the transaction is unusual or suspicious, he shall immediately inform the Compliance Officer and shall provide him with all the relevant information;
- If the Account Rep concludes that the Customer's transactional activity has changed substantially and, as a result, it is necessary to change the Customer's Transactional Profile or even his Risk Category, he will provide the Compliance Officer with the relevant information;
- If the transaction is found to be a one-off, and is adequately justified, the reasons shall be stated for which the applicable limits were exceeded by the Customer;
- If the Account Rep suspects that the Customer may be handling third-party funds, additional information shall be requested from the Customer. If the Account Rep's suspicions are confirmed, the customer shall be immediately reclassified as a High Risk Customer, and the provisions of paragraph 4.6.2 above shall apply.

After the matter is analyzed by the Account Rep, the resulting reports shall be submitted to the Compliance Officer for his review and subsequent filing.

A management report shall be prepared by the Compliance Officer, which will contain the outcome of monthly monitoring activities. The report shall be submitted to the Board of Directors for information purposes.

5.3 Transactions with FATF Non-Cooperative Nations or Territories

Special attention shall be paid to transactions with individuals and entities, including financial institutions, who are residents of nations or territories that:

- are not members of the Financial Action Task Force (FATF/GAFI) or similar regional organizations (Latin America Financial Action Task Force (GAFILAT), Caribbean Financial Action Task Force (CFATF), Middle East - North Africa Financial Action Task Force (MENAFATF) and Asia Pacific Group (APG), etc.; or
- are subject to special action by any of the abovementioned task forces, because they fail to apply, or do not apply sufficiently, FATF recommendations;
- are included in the OFAC list.

Any transactions involving any such territories shall be analyzed in order to determine whether they are lawful. In this regard, **TPCG Financial** shall analyze whether the transaction is reasonable, by evaluating whether the client has any connection with the relevant territory

(bank accounts, affiliates, etc.) and requesting any additional information or documentation as **TPCG Financial** may deem necessary.

In the light of the outcome of the abovementioned analysis, **TPCG Financial** may take any of the following courses of action:

- if the transaction is regarded as unusual or suspicious, the Suspicious Transaction Report procedure shall start (paragraph 6.1);
- if the transaction is found to be reasonable in the light of the Client's circumstances, or is found to be a one-off transaction that is adequately justified, **TPCG Financial** shall keep a record of the analysis made, duly documenting therein the reasons for the decision made.

6 SUSPICIOUS TRANSACTION REPORT

Pursuant to the provisions of Section 12 of Act Nº 19.574, dated December 20, 2017, and Section 202 of the RNMV, any and all individuals and entities subject to BCU supervision are under an obligation to report any transactions (whether actually closed or not) that in the light of normal business practices are found to be unusual, without apparent economic or legal justification, or unreasonably complex, as well as any financial transactions involving suspicious assets.

Suspicious transactions are defined by the RNMV as: *"any transactions (whether actually closed or not) that in the light of normal business practices are found to be unusual, without apparent economic or legal justification, or unusually or unreasonably complex, as well as any financial transactions involving suspicious assets, in order to prevent money laundering and terrorist financing activities. The obligation to report shall extend to cover any transactions that –even where lawful assets are involved- are suspected to be associated with individuals or entities involved in money laundering or terrorist financing activities, or designed to fund any terrorist activities."*

Additionally, the RNMV provides that any such transactions must be immediately reported by Securities Brokers to the Financial Information and Analysis Unit (UIAF) of the Central Bank of Uruguay.

6.1 Suspicious Transaction Detection, Analysis and Reporting

The process of detection, analysis and reporting of suspicious transactions shall meet the following requirements:

- An officer who detects an unusual or suspicious transaction shall immediately inform the Compliance Officer by means of an internal memorandum (Schedule No. 6), providing all the information about the transaction.

  The officer **shall keep the information strictly confidential and shall not warn the client** about the matter.

- The Compliance Officer shall analyze the transaction, by comparing it with the information contained in the relevant Customer's File. If necessary, the Compliance Officer shall request additional information and shall prepare a file, ensuring that the information contained in it is reliable.

- After those steps are taken, if the Compliance Officer believes that the transaction is unusual or suspicious on the face of it, in accordance with the standards set forth in applicable laws and regulations, he shall submit the matter to the Committee. Otherwise, the Compliance Officer shall properly document the analysis made and the reasons for his decision not to report the transaction, and shall inform the Committee before the matter is set aside.

- The Committee shall analyze the transaction and, if they find it to be unusual or suspicious in accordance with applicable laws and regulations, the Committee shall instruct the Compliance Officer to file immediately a Suspicious Transaction Report (ROS) with the Financial Information and Analysis Unit, in accordance with the provisions of Communication No. 2014/108 issued by the Central Bank of Uruguay. The Company's Board shall be informed accordingly.

  After a ROS is submitted, **TPCG Financial** shall follow instructions from the Financial Information and Analysis Unit of the Central Bank of Uruguay.

  Additionally, the Board shall consider whether or not **TPCG Financial** should continue to operate with the relevant customer, transferor, beneficiary or customer's customer.

  In the event that the Board decides to continue to operate with them, this decision must be explained and the Compliance Officer shall be asked to follow up on any transactions by the relevant customer, transferor, beneficiary or customer's customer.

  If the Committee understands that the transaction is not unusual or suspicious, the transaction will not be reported. The reasons for such a decision must be stated in the minutes of the relevant Committee meeting. The Compliance Officer may disagree with this decision; his dissent must be recorded in the minutes of the relevant Committee meeting.

6.2 List of Unusual and Suspicious Transactions

BCU's Financial Information and Analysis Unit has issued a list of unusual and suspicious transactions, high-risk transactions and red flags in connection with purchase, sale, construction, investment and other transactions involving real property, as well as a list of high-risk transactions and red flags in connection with terrorist financing (Communication No. 2002/198, No. 2010/216, No. 2012/191 and No. 2018/294), in order to help financial institutions detect suspicious transactions. Those lists are enclosed as Schedule No. 5 hereto.

Please bear in mind that the abovementioned lists are not exhaustive, but are merely a compilation of financial transaction types or patterns that might be related to money laundering activities.

In the event that any of the transactions so listed are detected, the officers involved shall evaluate whether the transaction is sufficiently explained by the information and documentation in the Company's possession regarding the Customer. If the officers involved understand that the transaction is not adequately justified by the supporting documentation available to the Company, the matter shall be immediately reported to the Compliance Officer, who shall be provided with all the relevant information.

6.3 Information about Terrorist-related Assets

Pursuant to the provisions of Section 203 of the RNMV, the Financial Information and Analysis Unit must be informed about any assets associated with any of the following persons:

- Persons identified as terrorists or members of terrorist organizations in the lists prepared pursuant to the Resolutions of the United Nations Security Council, which are designed to prevent terrorism and terrorist-financing activities and the proliferation of weapons of mass destruction;
- Persons declared as terrorists by a final court order in Uruguay or abroad.

In the event that terrorist-related assets are detected by a **TPCG FINANCIAL** officer in accordance with the abovementioned definition, the matter shall be immediately reported to the Compliance Officer, who shall be provided with all the relevant information.

The Compliance Officer will consider the matter in order to determine whether or not the assets in question are associated with an individual or organization of the types identified in local legislation (individuals or entities designated in a UN list or declared as terrorists by a final court order in Uruguay or abroad). If a terrorist connection is determined to exist, the matter shall be immediately submitted to the Board of Directors. The Board shall take note and shall instruct the Compliance Officer to file immediately a Suspicious Transaction Report with the BCU's Financial Information and Analysis Unit.

Otherwise, the Compliance Officer shall properly document the analysis made and shall inform the Board.

7 REPORTS TO THE CENTRAL BANK OF URUGUAY.

7.1 Reporting of Financial Transactions to BCU

The Central Bank of Uruguay shall be informed about any individuals or entities that carry out any of the following transactions (Section 204 of the RNMV):

a. receiving cash from customers in excess of US$ 10,000 (ten thousand U.S. dollars) or the equivalent amount in other currencies.
b. cash withdrawals by customers in excess of USD10,000 (ten thousand U.S. dollars) or the equivalent amount in other currencies.
c. receiving funds (from customers or from third parties for the Company's customers) via domestic or foreign wire transfers in excess of USD 1,000 (one thousand U.S. dollars) or the equivalent amount in other currencies, irrespective of the manner of operation used.
d. remittance of funds (to customers or to third parties on behalf of the Company's customers) via domestic or foreign wire transfers in excess of USD 1,000 (one thousand U.S. dollars) or the equivalent amount in other currencies, irrespective of the manner of operation used.

In the cases contemplated in a. and b. above, any transactions below the relevant thresholds shall also be reported, where the accumulated amount of transactions in any given account exceeds USD 10,000 (ten thousand U.S. dollars) or the equivalent amount in other currencies in any calendar month.

7.2 Reporting of Cross-border Transportation of Cash and Monetary Instruments

The BCU shall be informed about any cross-border transportation of cash, precious metals or other monetary instruments in excess of USD 10,000 (ten thousand U.S. dollars) or the equivalent amount in other currencies. (Section 29 of Act 19.574, Section 206 of the RNMV, and BCU Communication No. 2006/277)

Before any such transaction is conducted, the relevant form ("*Declaración de Entrada o Salida*") shall be filed with the BCU by electronic means, at the website used for the purpose of submitting information to the BCU.

The system shall automatically generate an ID number for each form that is confirmed, which can be printed out. This will serve as evidence, before any applicable governmental authorities, of the fact that the relevant form has been filed with the Central Bank of Uruguay.

If a transaction informed to the BCU is not actually carried out, it must be cancelled within two business days after the scheduled date of the transaction.

7.3 Information regarding Transactions and Services

TPCG FINANCIAL shall annually provide information regarding the Company's transactions and services, classified by ML/TF risk factors.

This information shall be provided to UIAF within 30 days after the close of the relevant fiscal year.

7.4 Reporting of Customer Accounts

The Superintendence of Financial Services shall be informed about any custody accounts and other customer accounts opened or closed, including the particulars of the accountholders, attorneys in fact and individuals authorized to operate on behalf of the customer.

This information shall be supplied within 5 business days after any such accounts are opened, closed or modified.

8 PERSONNEL POLICIES AND PROCEDURES

8.1 Know Your Employee

Knowing our employees is crucial for AML/CTF purposes. In this regard, **TPCG FINANCIAL** has taken several steps designed to ensure the integrity of our employees, as well as their commitment to the Company's principles and values.

8.1.1 Hiring Practices

At the hiring stage, the Company will make its best efforts to check the information supplied by applicants. Additionally, any such applicants shall be checked against UN and OFAC lists. No employee shall be hired without first checking the references supplied by him/her.

Whenever a new employee is hired, he/she shall be supplied with a copy of the Manual of Ethics and Conduct, the Code of Good Practices, and the AML/CTF Manual. Any new employee shall be interviewed by the Compliance Officer, who shall impress upon him/her the importance of AML/CTF efforts in the eyes of **TPCG FINANCIAL**'s Board, as well as the need to strictly apply the controls established by the Company. Also, any new employee shall be informed about the Company's AML/CTF policies, procedures and controls involved in his/her job.

8.1.2 Employee Assessment

The Compliance Officer shall make a general assessment of the Company's employees in order to detect any relevant changes in their behavior that can be regarded as a red flag or call for follow-up.

In this regard, the Compliance Officer shall analyze factors such as: relevant changes in an employee's purchase habits (purchase of real property, vehicles or other assets that are not in line with an employee's financial condition) or lifestyle (holiday destinations, travels, among other things) and other changes in an employee's behavior, such as his/her refusal to go on vacation, indebtedness levels that exceed his/her ability to pay, etc.

This assessment shall be made once a year, or whenever the circumstances so warrant. The outcome of the assessment shall be properly documented and recorded in the relevant Employee File.

8.1.3 Employee Files

TPCG FINANCIAL keeps files in respect of each Company employee, which contain the information obtained at the time of hiring a person, any training received by him/her, and other relevant events. Any penalties imposed on an employee shall also be recorded in the Employee File, where applicable.

An Employee File shall contain the following:

- Personal data.
- Résumé.
- Photocopy of the employee's ID.
- Proof that the employee has received a copy of the Code of Ethics and Professional Conduct, the Code of Good Practices and the Claims Procedure.
- Proof that the employee has received a copy of the AML/CTF Manual.
- Proof of training received by the employee.
- Proof of background checks (OFAC, UN and other lists).
- Proof of annual assessment by the Compliance Officer (Schedule No. 7).

The abovementioned documentation shall be properly kept in a manner that ensures its confidentiality.

8.1.4 Code of Ethics and Professional Conduct

All **TPCG FINANCIAL** employees shall comply fully with the provisions of the Code of Ethics and Professional Conduct. Employees shall give priority to legality and compliance with ethical standards rather than profit or the accomplishment of business goals. Employees shall avoid any situation that may generate a conflict between their own personal interests and the Company's.

8.1.5 Training

TPCG FINANCIAL is committed to keeping all employees duly trained and constantly updated in AML/CTF matters.

The Annual Training Plan shall be prepared by the Compliance Officer and submitted to the Board for approval. Without prejudice to the terms of the Plan, the Company shall facilitate attendance by employees at other training sessions in Uruguay or abroad.

Formal records shall be kept of each such training session in the relevant employee's File.

8.1.6 Confidentiality

TPCG FINANCIAL employees shall not disclose to the parties involved or third parties, any actions taken or reports produced in the performance of the AML/CTF information duties to which **TPCG Financial** is subject, in accordance with the provisions of Sections 202 and 203 of the RNMV (duty to report unusual and suspicious transactions, and duty to report on terrorist-related assets) and/or in response to a request for information by UIAF.

8.2 Breach of AML/CTF Policies and Procedures

Any breach of the provisions of this Manual shall be subject to penalties, taking into account the involvement of the parties whose duty it is to comply with the provisions hereof.

The above shall apply to any breach of the provisions of this Manual, whether negligent or intentional.

An employee shall be deemed to have acted negligently where any provision of this Manual is breached as a result of his lack of skill, negligence or lack of attention, without the employee's intending to do so.

An employee shall be deemed to have acted intentionally where:

- He had the actual and direct intention to enter into a transaction, while knowing that the transaction would breach or violate any of the provisions of this Manual, or
- He had the actual and direct intention to enter into a transaction, without intending to breach the provisions of this Manual, but knowing that the outcome could breach or violate the standards or principles contained herein.

Any such breach, whether negligent or intentional, shall result in a penalty. The penalty shall depend on the seriousness of the infraction and the intention of the violator, as follows:

- any intentional breach shall be regarded as serious, and shall result at least in suspension of the employee involved. If a breach is regarded as very serious, it may even result in termination of employment on the grounds of evident misbehavior;

- in the event of an intentional breach, the matter will be reported to the Central Bank of Uruguay for any applicable purposes. Whenever a crime is presumed to exist,

particularly crimes of money laundering, the matter shall be immediately reported to the police and the criminal court of competent jurisdiction;

- A breach committed with negligence may result in the following penalties:
  - Reprimand accompanied by a warning about the application of a more serious penalty if a second violation is committed. This penalty shall apply in the event of any minor violation.
  - Suspension without pay, in the case of a serious breach.
  - Termination of employment without severance payment, in the case of a very serious breach or repeated serious breaches.

9 AML/CTF SYSTEM: INDEPENDENT REVIEWS

An annual review of the AML/CTF System shall be conducted by an independent auditor. As a result of this review, the auditor shall issue a report containing his opinion as to the adequacy and operation of the Company's AML/CTF policies and procedures. Additionally, the report shall contain any significant flaws or omissions detected by the auditor, as well as recommendations designed to overcome those, and any corrective action implemented by the Company.