Anti-Money Laundering and Terrorist Financing Policy

of Haitong Bank S.A.

Approved by the Board of Directors

on 15th September 2020

Version 2.2

1. Table of contents[i]

2. Purpose

The purpose of this Policy of Haitong Bank, S.A. (the "Bank") is to determine, at the level of internal regulations, the essential elements to be observed in the context of detection and prevention of money laundering, terrorist financing and financing of the proliferation of weapons of mass destruction.

This document was drafted in line with the provisions of the applicable legislation, notably Law No. 83/2017 of 18 August, Notice No. 2/2018 of the Bank of Portugal, as well as the recommendations issued by, *inter alia*, the Joint Money Laundering Steering Group, the entity responsible for providing guidance on this matter in the United Kingdom, and the Financial Action Task Force[1], an independent intergovernmental organisation whose purpose is to determine and disseminate international standards to be applied in this respect.

The standards laid down in this document must be complied with by all the Bank's employees, and are further developed and detailed in the rules set forth in the Bank's Procedure Manual on money laundering, whose reading is mandatory. The Bank's Client Onboarding Policy also supplements this Policy.

3. Scope

Pursuant to the definition adopted by the Bank of Portugal[2], "money laundering means the process through which some criminals conceal the origin of assets and income (benefits) obtained illegally, transforming the proceeds from these activities into funds which can be used legally, by dissimulating the origin or the beneficial owner of the funds".

Law No. 83/2017 expands this concept, stating that money laundering also includes the acquisition, ownership or use of property, knowing, at the time of its receipt, that such property is derived from criminal activity or from an act of participation in such activity, as well as the participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of these actions.

In addition to anti-money laundering purposes, this policy also seeks to ensure other preventative purposes in respect of activities such as: (*i)* terrorist financing; *(ii)* proliferation of weapons of mass destruction; and *(iii)* others deemed material for Haitong Bank, S.A..

[1] The most recent recommendations are contained in the document "*International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations*", published in February 2012 and which may be consulted on the site www.fatf-gafi.org.
[2] https://www.bportugal.pt/page/branqueamento-de-capitais-e-financiamento-do-terrorismo

Given the Bank's business, anti-money laundering corresponds, generally speaking, to best practice in terms of Know Your Client ("KYC"), monitoring and follow-up of transactions and performance of the other legal and regulatory duties in this respect.

3.1. Illegal acts generating funds liable to laundering

The Bank and its employees are responsible for adopting a set of practices with a view to preventing the laundering of money from the following criminal offences[3]: procuring, sexual abuse of children or dependent minors, extortion, trafficking in narcotic drugs or psychotropic substances, trafficking in arms, trafficking in human organs or tissue, trafficking in protected species, tax fraud, unlawful influence, corruption, terrorist activities and any illegal activity punishable by minimum imprisonment in excess of 6 months or maximum imprisonment in excess of 5 years (as laid down in article 368-A of the Criminal Code).

3.2. General duties of the Bank and its employees[4]

In the context of preventing and combating the laundering of money from criminal offences, the Bank and its employees are legally bound to a number of duties, namely:

a) duty to control, by determining and ensuring the application of internal policies and procedures which prove to be appropriate for the effective management of any risks of money laundering and compliance with the legal and regulatory provisions;

b) duty to identify and apply due diligence measures to clients, counterparties and their representatives and beneficial owners;

c) duty to report suspicious transactions to the Public Prosecution Service's Central Investigation and Penal Action Department (*Departamento Central de Investigação e Ação Penal do Ministério Público*, DCIAP) and to the Financial Information Unit of the Criminal Police (FIU).

d) duty to refrain from executing suspicious transactions, followed by a report to the DCIAP and the FIU and subject to confirmation by these authorities;

e) duty to refuse to establish business relationships, carry out occasional transactions or carry out other transactions when the client does not supply his/her/its identification details or those of the person on whose behalf he/she/it is acting or information on the

[3] Article 368-A of the Criminal Code.
[4] Any failure to observe these duties is a regulatory offence, pursuant to article 169 of Law no. 83/2017 of 18 August.

nature, subject matter and purpose of the business relationship;

f) duty to retain the relevant documentation for seven years;

g) duty to examine certain behaviours, activities or transactions which might correspond to a money laundering offence;

h) duty to cooperate with the competent authorities, supplying any information requested;

i) duty of non-disclosure, which prohibits the Bank's employees from disclosing to the client or any third-party that he/she/it is being investigated in this context or that a suspicious transaction report has been made[5];

j) duty to train employees so as to permit the identification of any transaction which might be related to money laundering, as well as the performance of the other duties, as a means to prevent this sort of transactions.

3.3. Role of the management body

Pursuant to article 13 of Law no. 83/2017, the management body is responsible for:

- appointing a member of the management body to be responsible for complying with the provisions of Law no. 83/2017, Notice no. 2/2018 and other applicable regulations;
- approving AML/CFT policies, procedures and controls;
- possessing adequate knowledge of the main risks of money laundering and terrorist financing to which the Bank is exposed, as well as of the processes used to identify, assess, monitor and control these risks[6];
- ensuring an appropriate AML/CFT organisational structure, preventing conflicts of interest;
- fostering a AML/CFT institutional culture supported by high standards of ethics and integrity;
- appointing a money laundering reporting officer (MLRO);
- periodically assessing the effectiveness of the policies and controls, ensuring that any shortfalls detected are corrected.

In accordance with no. 3 of the aforementioned article, the management body must refrain from interfering with any exercise of the duty to report, which shall exclusively be exercised by the MLRO. Notwithstanding, the management body is responsible for reviewing any decision

[5] Breach of this rule is a criminal offence, punishable under article 157 of Law no. 83/2017 by imprisonment for up to three years or fine.
[6] In accordance with the Bank's AML/CFT risk assessment methodology.

to refrain from exercising the aforementioned duty to report made by the MLRO, whenever he/she concludes there are no potential suspicions.

The management body must ensure that the MLRO:

- exercises his/her duties in an independent, ongoing and effective manner and with the required autonomy to make decisions;
- has the appropriate repute, professional qualifications and availability for this function;
- has appropriate technical, material and human means and resources, including any employees necessary for the proper performance of his/her function;
- has unrestricted access in a timely manner to any internal information material for exercising his/her function, in particular information on compliance with the duty to identify and apply due diligence measures and records of transactions made;
- is not subject to any potential conflict of functions, in particular when his/her duties are not segregated.

3.4. Role of the Compliance Department and, in particular, of the MLRO

With regard to the purposes of the internal control system, pursuant to and for the purposes of article 2(c) of Notice No. 5/2008 of by the Bank of Portugal (“Notice No. 5/2008”), the goal of the Compliance function is, *inter alia*, "observance of the applicable legal and regulatory provisions (compliance objectives), including those on anti-money laundering and terrorist financing".

From the aforementioned provisions result, in particular, pursuant to and for the purposes of article 17(1)(c) of Notice No. 5/2008, the monitoring and assessment of anti-money laundering and terrorist financing internal control procedures, as well as centralisation of the corresponding notifications to the competent authorities.

Law no. 83/2017 – in its article 16 – and Notice no. 2/2018 of the Bank of Portugal – in its article 7 – require the Bank to appoint a money laundering reporting officer (MLRO), who must be a member of its senior management or an equivalent officer and who shall have exclusive responsibility for the actual application of policies, procedures and controls appropriate to an effective management of ML/TF risks and controlling compliance with the applicable legal and regulatory provisions.

Pursuant to the aforementioned articles, the MLRO shall be responsible for:

- taking part in the drawing up of and issuing a prior opinion on any AML/CFT policies, procedures and controls;

- monitoring, on an ongoing basis, the adequacy, sufficiency and currentness of AML/CFT policies, procedures and controls, proposing any necessary amendment thereto;
- participating in the establishment, monitoring and assessment of the internal training policy;
- ensuring that all material information from the various business areas is centralised;
- acting as a point of contact for judiciary, police and supervisory and inspection authorities, notably by complying with the duty to report and ensuring compliance with other reporting and cooperation obligations;
- ensuring the currentness, sufficiency, accessibility and comprehensiveness of information on the internal control system and of the policies and instrumental procedures and controls for its application made available to the relevant employees of the financial institution;
- supporting the preparation and execution of periodic assessments of the adequacy of AML/CFT policies, procedures and controls;
- proposing the adoption of any corrective action which might prove necessary to the management body;
- coordinating the drawing up of notices, reports and other information to be sent to the management body and relevant external entities.

In spite of the role played by the Compliance Department, we remind you that this Anti-Money Laundering Policy applies to all the Bank's employees, without exception.

4. Description of duties

4.1. Duty to control

The Bank, through the Compliance Department, must determine and apply internal policies, procedures and controls appropriate to effectively manage the risks of money laundering and to comply with the legal and regulatory provisions in this respect. The policies, procedures and controls determined by the Bank must include, at least:

- the establishment of an effective risk management model, with practices appropriate for the identification, assessment and mitigation of any risks of money laundering to which the Bank is, or might become exposed;
- the development of client onboarding policies, procedures and controls;
- establishment of appropriate staff ongoing training programmes, applicable from

admission;

- appointment, if required, of a MLRO;
- establishment of formal systems and processes to capture, process and store information that support, in a timely manner:
    i) the analysis and decision-making process, in particular with regard to the monitoring of clients and transactions and examination of potential suspicions;
    ii) compliance with the duties to report and to cooperate;
    iii) establishment of safe channels making it possible to ensure full confidentiality of any requests for information;
- communication to staff of duly updated and accessible information on the respective AML/CFT internal standards;
- establishment of screening procedures that ensure the application of high standards to the recruitment process of employees, irrespective of the nature of their contract;
- establishment of mechanisms to control the conduct of the Bank's employees;
- establishment of appropriate tools or IT systems, as required for the effective management of the risks of money laundering;
- establishment of mechanisms making it possible to periodically test their quality, adequacy and effectiveness, including, if applicable, an independent audit function;
- establishment of appropriate internal resources enabling the Bank's employees to report any breach of this policy through a specific, independent and anonymous channel;[7]
- development of personal data protection policies and procedures.

All AML/CFT policies, procedures and controls must be documented and the Bank, through the Compliance Department, must review them[8] to ensure that they remain up-to-date.

3.1.1 Risk management

The Bank has an AML assessment methodology, the Compliance Department being responsible for:

(a) identifying the actual risks of money laundering, including risks related to:

[7] The confidentiality of the reports received and protection of the personal data of both the reporter and of the person suspected of having committed the breach must be ensured, in accordance with Law No. 67/98 of 26 October, as amended by Law No. 103/2015 of 24 August, as well as with article 20 of Law No. 83/2017.
[8] With a frequency in line with the existing risks.

i) the nature, size and complexity of the Bank's business;
ii) its respective customers;
iii) the business areas pursued, as well as the products, services and transactions offered;
iv) the distribution channels of the products and services offered, as well as the means of communication used to contact clients;
v) the countries or territories of origin of the Bank's clients or where such clients have their domicile or otherwise carry out their business;
vi) the countries or territories where the Bank operates either directly or through third parties, belonging to the same group or otherwise;

(b) assessing the risk of money laundering, including by determining:
i) the degree of probability and the impact of each risk specifically identified, taking into account to this end all material variables in the context of its operating circumstances, including the purpose of the business relationship, the level of assets deposited by client or the volume of transactions carried out and the regularity or duration of the business relationship;
ii) the overall risk of the Bank and of its respective business areas;

(c) establishing and adopting any means of control and control procedures that prove to be appropriate to mitigate the specific risks identified and assessed, adopting particularly enhanced procedures in the event of any increased risk of money laundering;

(d) reviewing risk management practices as to their currentness.

Risk management practices, as well as their respective updating must be proportionate[9] and documented by means of written documents that reflect the risks underlying the Bank's business.

In this context, particular attention must be paid to any risks of money laundering that might result from offering products or transactions which favour anonymity, the development of new products and business practices and the use of new technologies.

3.1.2 Information systems

The Bank has appropriate and up-to-date information systems, which enable the Bank:

- to record all identification data and other particulars concerning its clients, representatives and beneficial owners;

[9] Proportionate to the nature, size and complexity of the Bank.

- to identify, by filtering its Client Database against the lists of World-Check, the United Nations, the OFAC, the Bank of England, the Bank of Portugal, politically exposed persons and people or entities identified in restrictive measures;
- to assign a money laundering risk profile to each client;
- to monitor and detect transactions which may constitute a money laundering or terrorist financing offence.

3.1.3 Whistleblowing system

The Bank has a whistleblowing system that enables its employees to report any fault related to possible breach of legal or regulatory provisions or internal policies or procedures to the Head of Compliance.

This system corresponds to a specific, independent and anonymous channel that ensures the reception, handling and filing of reports.

3.1.4 Monitoring of branches and affiliates

The Bank has procedures for the monitoring of its branches and affiliates abroad by the Compliance Department, laid down in the internal regulations *Compliance Report by Geography*. In accordance with the aforementioned rules, the Compliance Department receives bimonthly reports from the local heads of the Compliance function containing all information required, in particular in respect of AML/CFT. Thereafter, monthly meetings or videoconferences are held with representatives of the Group's units to discuss the issues stated in the reports, the information being compiled and submitted to the Executive Committee each month.

4.2. Duty to identify and apply due diligence measures[10]

The duty to require identification falls under the KYC – Know Your Client – and KYB - Know Your Business – practices and applies to all clients and counterparties before beginning to execute any transaction.[11]

[10] Related procedures: Identification of Counterparties, Opening of Bank Deposit Accounts, Opening of Advisory Accounts and Opening of Management Accounts.
[11] Article 65 of Law No. 83/2017.

By means of internal regulations, the Bank lays down the rules regulating the collection of all identification details of its clients and counterparties, as well as the respective evidence required, in accordance with Law no. 83/2017 and Notice no. 2/2018 of the Bank of Portugal.

This duty must be performed whenever:

1. a business relationship is established or an occasional transaction is carried out and:
   - any bank or securities deposit, advisory or management account is opened;
   - the Bank, without opening an account, executes any transaction, even if only occasional, whose amount in isolation or in aggregate (several transactions apparently related to one another) is equal to or greater than €15,000 or corresponds to any transfer of funds in excess of €1,000;
2. there is a suspicion that the transactions might be related to money laundering or terrorist financing, regardless of the amount or any exemption or threshold;
3. there are doubts about the veracity or adequacy of previously obtained client identification data.

4.2.1. Beneficial owners[12] [13]

When the client is a legal entity or a legal arrangement, the Bank must obtain satisfactory knowledge of the client's beneficial owners and keep written records of all actions taken to this end.

Beneficial owner means:

(a) the natural person(s) who ultimately own or control a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity;[14]
(b) the natural person(s) who otherwise control the legal entity;
(c) the natural person(s) who hold the position of senior managing officials if, after having exhausted all possible means and provided there are no grounds for suspicion.[ii]

[12] Beneficial owner means, within the meaning of article 2(1)(h) of Law no. 83/2017: "the natural person(s) who ultimately own or control the client and/or the natural person(s) on whose behalf a transaction or activity is performed".
[13] See Law no. 89/2017 of 21 August, which approves the regulations on the Central Register of Beneficial Owners, as well as Ordinance no. 233/2018, which regulates this system.
[14] For the purposes of assessing the beneficial owner status, the following should be taken into account: (i) direct ownership: shareholdings representing more than 25% of the client's share capital are owned by a natural person; (ii) indirect ownership: shareholdings representing more than 25% of the client's share capital are owned by a legal entity controlled by two or more natural persons or several legal entities controlled by the same natural person(s); (iii) other circumstances which might otherwise indicate control.

Legal entities that establish or maintain business relationships or perform occasional transactions with the Bank must supply in due course: (i) information on their legal or formal owner; (ii) sufficient, accurate and current information on their beneficial owners; (iii) particulars on the nature of the control exercised by the beneficial owner and the underlying economic interests; and (iv*)* any other documents, data and information required for the Bank to comply with the applicable regulations.

The Bank must ensure any procedures necessary to consult the Central Register of Beneficial Owners.

4.2.2. Simplified measures[15]

The Bank may, after having identified a demonstrably low risk of ML/TF[16], take simplified measures under the duty to identify and apply due diligence measures.[17] Simplified measures means, for instance:

(a) verification of the client's and the beneficial owner's identification after establishment of the business relationship;
(b) reduction in the frequency for updating details collected in compliance with the duty to identify and apply due diligence measures;
(c) reduction in intensity of the ongoing monitoring and in the depth in which transactions are analysed in the event of the sums involved being low;
(d) non-collection of specific information and non-application of specific measures making it possible to understand the purpose and the nature of the business relationship, where such purpose and nature can be reasonably inferred from the type of transaction made or from the business relationship established.

The measures adopted must be consistent with the low risk factors identified.

4.2.3. Enhanced measures[18]

Enhanced measures must be adopted when a higher risk[19] of money laundering is identified in the business relationships, the occasional transactions or the transactions carried out. Enhanced measures means, for instance:

[15] Pursuant to and for the purposes of article 35 of Law No. 83/2017 and article 28 of Notice no. 2/2018 of the Bank of Portugal.
[16] Law no. 83/2017 contains, in its Schedule II, an illustrative list of factors and types that may indicate a potentially lower risk. This schedule is reproduced in Schedule I to this Policy.
[17] Cases listed in Schedule II to Law no. /2017 of 18 August.
[18] Pursuant to and for the purposes of article 36 of Law No. 83/2017.
[19] Law no. 83/2017 contains, in its Schedule III, a illustrative list of factors and types that may indicate a potentially higher risk. This schedule is reproduced in Schedule II to this Policy.

(a) obtainment of additional information on clients or their representatives or beneficial owners, as well as on transactions planned or carried out;
(b) the taking of additional steps to verify the information obtained;
(c) involvement of higher hierarchical levels to authorise the establishment of business relationships, the carrying out of occasional transactions or transactions in general;
(d) increase in the depth or frequency of the monitoring procedures applied to the business relationship or certain transactions or set of transactions, with a view to detecting possible indicators of suspicion and subsequently complying with the duty to report;
(e) reduction in the time intervals for updating information and other details collected in the course of compliance with the duty to identify and apply due diligence measures;
(f) authorise the monitoring of the business relationship by the money laundering reporting officer or another employee that is not directly involved in the business relationship with the client;
(g) requirement that the first payment concerning a certain transaction be made by traceable means with origin in a payment account opened by the client with a financial entity or any other duly authorised entity that, not being situated in a higher-risk third country, has demonstrably applied equivalent identification and due diligence measures.

4.2.4. Politically exposed persons

In the context of their business relationships or occasional transactions with clients or their representatives or beneficial owners who are politically exposed persons (PEPs), by way of supplement to the standard identification and due diligence procedures, the Bank shall:

(a) detect the PEP status acquired before or after establishment of the business relationship or the carrying out of the occasional transaction;
(b) ensure approval by a member of its senior management for (i) establishing business relationships or carrying out occasional transactions; (ii) continuing business relationships with such persons when they become politically exposed persons after establishment of the business relationship;
(c) take adequate measures to establish and verify the source of wealth and of funds that are involved in the business relationships, occasional transactions or transactions in general;
(d) conduct enhanced, ongoing monitoring of business relationships, in particular with a view to identifying any transactions that should be reported.

To this end, PEP means any individual who is or has been entrusted in the immediately preceding year with any prominent political or public function, as well as his/her immediate family members and close business associates, as follows:

Prominent political or public functions

- heads of State, heads and members of the Government, such as ministers, secretaries and under-secretaries of State;
- members of parliament or other representative houses;
- judges of the Constitutional Court, of the Supreme Court of Justice, of the Supreme Administrative Court, of the Court of Auditors and members of supreme courts, of constitutional courts or of other high-level judicial bodies of other states and international organisations;
- representatives of the Republic and members of the autonomous regions' own government;
- the Ombudsman (*Provedor de Justiça*), State Counsellors and members of the National Data Protection Committee (*Comissão Nacional da Proteção de Dados*), the Judges' Council (*Conselho Superior da Magistratura*), the High Council of Administrative and Tax Courts (*Conselho Superior dos Tribunais Administrativos e Fiscais*), the Attorney General's Office (*Procuradoria-Geral da República*), the High Council of the Public Prosecution Services (*Conselho Superior do Ministério Público*), the High Council for National Defence (*Conselho Superior de Defesa Nacional*), the Economic and Social Council (*Conselho Económico e Social*) and the Media Authority (*Entidade Reguladora para a Comunicação Social*);
- heads of diplomatic missions and consular offices;
- high-ranking officers in the armed forces in office;
- chairmen and councillors performing executive functions on city councils;
- members of the management and supervisory bodies of central banks, including the European Central Bank;
- members of the management and supervisory bodies of public institutes, public foundations, public undertakings and independent administrative entities, irrespective of their designation;
- members of the management and supervisory bodies of state-owned enterprises, including regional and local state-owned enterprises;

- members of the governing bodies of national or regional political parties;
- directors, deputy directors and members of the board or persons who perform equivalent functions in an international organisation.

Immediate family members

- spouse or partner;
- parents, children and their respective spouses or partners.

Close business associates

- natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements with a PEP;
- natural persons who own share capital or voting rights in a legal entity or assets of legal arrangements which are known to have been set up for the *de facto* benefit of a PEP;
- natural persons who are known to have corporate, business or professional relations with a PEP.

In a conservative approach, the Bank may identify and classify as PEPs in a database any other categories of persons who present characteristics that might suggest political exposure.

4.2.5. Additional due diligence

In addition to the identification of clients, counterparties, representatives and beneficial owners, the Bank's employees must:

a) take appropriate action to understand the client's ownership and control structure, where the client is a legal entity or a legal arrangement;

b) obtain information on the purpose and purported nature of the business relationship;

c) obtain information, when the risk profile of the client or the characteristics of the transaction so advise ("high risk" or, potentially, "unacceptable")[20], on the origin and destination of any funds transferred within a business relationship or execution of an occasional transaction;

d) continuously monitor the business relationship, so as to ensure that these transactions are consistent with the institution's knowledge of the client's activities and risk profile;

[20] The client risk profiles are defined in the Bank's Client Onboarding Policy.

and

e) update any information details obtained in the course of the business relationship.

4.2.6. Performance by third parties of the duty to identify and apply due diligence measures

If the Bank decides to hire a third party to perform the identification and due diligence procedures, the Bank must ensure:

- that the third party is an entity covered by Law no. 83/2017, is authorised to perform identification and due diligence procedures and is reliable, there being no publicly known information which might affect its reputation;
- that it collects complete information on the clients from the third party or performs a new identification, in the event of insufficiency of the information or if the associated risk so advises;
- compliance with all record-keeping requirements laid down article 51 of Law No. 83/2017, as if the identification and due diligence procedures performed by the third-party were performed by the Bank itself;
- that the third party:
    - gathers all the information and performs all identification, due diligence and record-keeping procedures that the Bank must observe itself;
    - immediately provides a copy of the identification and identity verification data and other relevant documentation on the client and his/her/its representatives and beneficial owners that were the subject of identification and due diligence procedures;
    - has an appropriate AML/CFT internal control system;
    - has the necessary human, material and technical resources to perform the identification and due diligence procedures face-to-face or at a distance, as the case may be;
    - has employees with appropriate AML/CFT training;
    - identifies the employee who performed the duty to identify and to apply due diligence measures and the date of such performance;
    - collects the identification details of clients and their representatives or beneficial owners before the business relationship is established.

4.3. Duty to notify

The Bank, through the MLRO, shall immediately inform the DCIAP and the FIU when it knows, suspects or has reasonable grounds to suspect that any cash or other property, regardless of the amount or value involved, is proceeds of criminal activity or is related to terrorist financing.

Accordingly, the Bank's employees must advise the Compliance Department[21] whenever they have reason to suspect that they are facing a situation with these characteristics.

4.4. Duty to refrain

Under the duty to refrain, it is prohibited to execute any transaction which the Bank suspects of being related to any money laundering offence. In the event of such a suspicion, the MLRO must report to the DCIAP and the FIU that the Bank has refrained from executing a transaction or set of transactions. Following this notice, the DCIAP may, within six business days, order the temporary suspension of the respective execution[22], which will subsequently be subject to confirmation by the court in the context of a criminal enquiry.

The Bank may execute transactions with regard to which it has complied with its duty to refrain, under the following circumstances:

a) when it is not notified, within six business days of the aforementioned report, of the decision to order a temporary suspension;
b) when it is notified, by the deadline referred to in the preceding paragraph, of the DCIAP's decision not to order a temporary suspension, in which case transactions may be immediately executed.

4.5. Duty to refuse

The heads of the Bank's business areas must refuse to execute transactions when the client does not supply: *(i)* his/her/its identification or the identification of the person on whose behalf he/she/it is effectively acting, in the terms set forth in the law[23]; *(ii)* information on the beneficial owner and the ownership and control structure; *(iii)* information on the nature and purpose of the business relationship and the origin of the funds[24].

[21] Through the appropriate channels created to this end, stated in the intranet.
[22] See articles 48 and 49 of Law No. 83/2017.
[23] Article 50(1)(a) of Law No. 83/2017.
[24] Article 50(2)(b) of Law no. 83/2017 of 8 May.

In this event, the Compliance Department will analyse the underlying circumstances and, if it suspects that the situation might be related to any money laundering offence, it will make the notifications foreseen in the duty to report, and consider terminating the business relationship.

4.6. Duty to retain documents

All the documentation collected and generated in the context of the money laundering and terrorist financing system must be retained for a seven-year period.

This set of information includes: the policies, procedures and controls, as well as the periodic assessments of their effectiveness; the risk assessments performed in accordance with the approved methodology; documents evidencing compliance with the duty to identify and to apply due diligence measures (in this case, the Bank must retain the documentation for seven years after the end of the business relationship with the client); reports of shortcomings made internally by the Bank's employees (whistleblowing); suspicious transaction reports submitted to the FIU and the DCIAP, as well as systematic transaction reports; the analyses and findings made in the context of exercise of the duties to refrain, to refuse and to examine; records of training actions.

Originals, copies, references or any other durable media, with an identical value as evidence, of supporting documents and transaction records must always be retained, so as to make it possible to recreate the transaction, for at least seven years[25] after its execution, even if, should it fall within a business relationship, such business relationship has already ended.

4.7. Duty to examine

All the Bank's employees must analyse with particular care any behaviour, activity or transaction whose characteristics make it particularly liable to be related to money laundering, in particular:

a) the nature, purpose, frequency, complexity, unusualness and exceptionalness of the behaviour, activity or transaction;

b) the apparent absence of an economic purpose or a lawful end associated with the behaviour, activity or transaction;

[25] Without prejudice to the 12-year period to retain records laid down in authorisation no. 3924/2016 issued by the National Data Protection Commission (CNPD).

c) the amounts, origin and destination of the funds moved;

d) the place of origin and destination of the transaction;

e) the means of payment used;

f) the nature, activity, patterns of operation and the parties' economic condition and profile;

g) any other risk features identified in the transaction;

h) the type of transaction, product, shareholding or legal arrangement structure that might favour anonymity.

The outcome of this analysis must be written down and retained for at least seven years, being open to inspection by auditors and supervisory and inspection entities[26].

4.8. Duty to cooperate

The Bank, through the Compliance Department or the MLRO, must provide any assistance requested by court and police (DCIAP and FIU), supervisory and tax and customs authorities in the context of the duty to cooperate, notably by supplying all information and submitting all documents requested by the aforementioned authorities[27].

4.9. Duty of non-disclosure

The Bank, through the members of its bodies, its employees and any other person who provides services to the Bank, is barred from disclosing to the client or any third party that a criminal investigation is in progress or that it has transmitted any information to the authorities or, further, any internal or external information material for the prevention, investigation and detection of money laundering[28].

This duty does not prevent the disclosure of information to entities belonging to the same business group, the competent authorities or other relevant financial entities, provided this is made for anti-money laundering purposes[29].

[26] See article 52(5) of Law No. 83/2017.
[27] See article 53 of Law No. 83/2017.
[28] As already mentioned, breach of this duty is a criminal offence, punishable under article 157 of Law no. 83/2017 by imprisonment for up to three years or fine.
[29] See article 54 of Law No. 83/2017.

4.10. Duty to provide training[30]

The Bank, through the Compliance Department, should adopt the actions necessary so that its bodies, the relevant employees[31] and the employees whose functions are directly related to anti-money laundering purposes have appropriate knowledge of the obligations resulting from the legislation and regulations in force.

The anti-money laundering and terrorist financing training policy should be designed on a pluri-annual basis and provide for: (*i)* training of new employees; and (*ii)* training of relevant employees at least once a year.

5. Group relations and applicability[32]

The Bank must ensure that the anti-money laundering and terrorist financing principles and procedures that apply internally are extended to all its branches and affiliates abroad[33], in a way that makes it possible:

i. to assess the risks inherent in the business carried out;
ii. to exchange information within the Group with a view to achieving the goals sought by the Anti-Money Laundering and Terrorist Financing Policy.

If the legislation of the country of incorporation of any branch or affiliate prevents application of the principles, policies or measures set forth in this document, the Bank must inform the Bank of Portugal thereof and of the policies adopted to address the increased risk resulting therefrom.

6. Data protection and processing

The Bank is authorised to process any personal data required to perform its anti-money laundering duties, provided that this data cannot subsequently be used for any other purpose[34].

[30] Related procedures: Anti-Money Laundering / Employee Training.
[31] Within the meaning of article 2(1)(f) of Notice no. 2/2018 of the Bank of Portugal, relevant employees means: members of the management body; employees who perform duties implying direct, face-to-face or at a distance contact with clients; employees allocated to compliance, risk management or internal audit functions.
[32] For the purposes of this document, Group means, within the meaning of article 2(1)(t) of Notice no. 2/2018: "a set of entities composed of: *(i)* a legal entity or any other undertaking that ultimately controls another legal entity(ies) or undertaking(s) forming part of the group (parent undertaking), its subsidiary undertakings or other undertakings in which the parent undertaking or its subsidiary undertakings hold a participation, in particular when one nor more control indicators occur; or (ii) other undertakings linked to each other by a control relationship, in particular when one nor more control indicators occur".
[33] See article 22 of Law no. 83/2017 and article 16 of Notice no. 2/2018 of the Bank of Portugal.
[34] Without prejudice to other legal provisions on the protection of personal data, notably Law no. 67/98 of 26 October, as amended by Law No. 103/2015 of 24 August.

Schedule I - Illustrative list of factors and types indicating a potentially lower risk (attached to Law no. 83/2018)

1 — Client risk factors:

a) companies whose shares are admitted to trading on a regulated market and subject, by virtue of the rules of such market, the law and other mandatory instruments, to duties to inform that ensure appropriate transparency in respect of beneficial owners;
b) public administration or state-owned companies;
c) clients residing in lower-risk geographies, identified in line with no. 3 of this schedule.

2 — Product, service, transaction or distribution channel risk factors:

a) life insurance, pension fund or similar savings product agreements with a low premium or annual contribution;
b) insurance agreements associated with pension funds, provided they neither have a redemption clause nor can be used as security for loans;
c) pension, complementary pension or similar schemes to pay retirement pensions to employees, whose contributions are deducted from salaries and with rules prohibiting the assignment of rights;
d) limited and clearly defined financial products or services with a view to increasing the level of financial inclusion of certain types of clients;
e) products in which the money laundering and terrorist financing risks are controlled by other factors, such as limits in terms of sums that may be credited or the transparency of their ownership, including certain types of electronic currency.

3 — Geography risk factors

a) European Union Member States;
b) third countries with effective money laundering and terrorist financing systems;
c) countries or jurisdictions identified by reliable sources as having a low level of corruption or other criminal activities;
d) third countries subject, on the basis of reliable sources, such as published mutual assessment, detailed assessment or monitoring reports, to obligations to prevent money laundering and terrorist financing consistent with the FATF's revised recommendations and which effectively implement such obligations.

7. Schedule II - Illustrative list of factors and types indicating a potentially higher risk (attached to Law no. 83/2018)

1 — Client risk factors:

a) business relationships taking place in unusual circumstances;
b) clients residing or doing business in higher-risk geographies, identified in line with no. 3 of this schedule;
c) legal entities or legal arrangements used as a means to hold personal assets;
d) companies with nominee shareholders or whose capital is represented by bearer shares;
e) clients who/which carry out activities involving involved cash-intensive transactions;
f) corporate ownership or control structures that appear unusual or excessively complex taking into account the business carried out by the client.

2 — Product, service, transaction or distribution channel risk factors:

a) private banking;
b) products or transactions which might favour anonymity;
c) payments received from third parties unknown or not related to the client or the business carried out by the client;
d) new products and new trade practices, including new distribution mechanisms and payment methods, as well as the use of new technologies or technologies under development for both new and existing products.

3 — Geography risk factors

a) third countries identified by reliable sources, such as published mutual assessment, detailed assessment or monitoring reports, as not having effective money laundering and terrorist financing systems, without prejudice to the legal provisions on high-risk third countries;
b) countries or jurisdictions identified by reliable sources as having a significant level of corruption or criminal activities;
c) countries or jurisdictions subject to sanctions, embargo, other restrictive measures or additional countermeasures applied, among others, by the United Nations and the European Union;
d) countries or jurisdictions that provide funding or support terrorist activities or actions or in whose territory operate terrorist organisations.

8. Schedule III - Illustrative list of potential suspicion indicators (available in the portal of the Money Laundering and Terrorist Financing Policy Coordination Committee[35])

A. GENERAL INDICATORS

- Clients who/which have business relationships, execute occasional transactions or execute transactions in general that – due to their nature, frequency, amounts involved or any other factor – are inconsistent with their profile.
- Clients who/which, without any reasonable explanation, handle cash: (a) in unusual amounts; (b) in amounts inconsistent with their profile; (c) wrapped or packaged in an unusual way; (d) in poor condition; or (e) represented by small denomination banknotes, with a view to exchanging them for higher denomination banknotes.
- Clients who/which, in any way whatsoever, seek to persuade the financial institution's employees to ignore any AML/CFT legal obligation or internal procedure.
- Clients who/which are reluctant or refuse to provide identification details/evidence/other information particulars or to take any verification action deemed necessary by the financial institution to:
    - identify the client, his/her/its representative or the beneficial owner;
    - understand the client's ownership and control structure;
    - know the nature and purpose of the business relationship;
    - know the origin and destination of the funds; or
    - characterise the client's business.
- Clients who/which are reluctant or refuse to provide original or equivalent documents.
- Clients who/which are reluctant or refuse to update their information details.
- Clients who/which are reluctant or refuse to deal face-to-face with the financial institution.
- Clients who/which provide identification details, evidence or other information details which:
    - are unreliable as to their authenticity;
    - are unclear as to their content;
    - are difficult to verify by the financial institution; or
    - present unusual characteristics.
- Clients who/which present different identification documents each time the same are requested by the financial institution.
- Clients who/which, in the course of their business, use pseudonyms, nicknames or any alternative expressions other than their true name or designation.

[35] http://www.portalbcft.pt/sites/default/files/anexos/indicadores_suspeicao_genericos_1.pdf

- Clients who/which postpone or do not deliver any documentation that may be submitted to the financial institution after the business relationship is established.
- Clients who/which seek to suspend or alter the business relationship or the occasional transaction after the identification details and their respective evidence or other information details relevant to know the client are requested of them.
- Clients who/which do not wish any correspondence to be sent to their stated address.
- Clients who/which, being apparently unrelated, give identical addresses or contact details (telephone number, fax number, email address or other details).
- Clients whose address or contact details (telephone number, fax number, email address or other details) prove to be false or are permanently inactive, particularly when the financial institution tries to contact them shortly after the business relationship is established.
- Clients whose address or contact details (telephone number, fax number, email address or other details) change frequently.
- Clients who/which appear to be acting on behalf of a third party without, however, disclosing it to the financial institution or, if they do, refuse to supply the necessary information details on the third party on whose behalf they are acting.
- Clients who/which seek to establish close relationships with employees of the financial institution.
- Clients who/which seek to restrict their contacts with the financial institution to one or more specific employees of the financial institution, in particular when – if this or these employees are absent – they decide not to execute or suspend any transaction.
- Clients who/which show unusual knowledge of money laundering and terrorist financing legislation.
- Clients who/which evidence uncommon interest in knowing the financial institution's AML/CFT policies, procedures and internal controls.
- Clients who/which, within a short period of time, have started similar business relationships with different financial institutions.
- Clients who/which carry out their business in different successive locations, apparently trying to avoid their detection by third parties.
- Clients who/which recurrently execute transactions to an amount below the limits that would trigger adoption of identification procedures[36].

[36] The Bank adopts identification procedures for all clients and counterparties with whom/which it deals, irrespective of the amount of the transaction in question.

- Clients who/which purchase valuable goods and sell the same within a short period without apparent reason.
- Clients who/which, on the same day or within a short period of time, execute transactions in different branches of the institution.
- Clients who/which give unclear or inconsistent explanations about transactions or are not familiar with their purpose.
- Clients who/which give excessive and unsolicited explanations about transactions.
- Clients who/which evidence nervousness or unusual urgency in executing transactions.
- Clients related to transactions suspected of ML/TF, notified by the financial institution to the competent authorities.
- Clients related to transactions suspected of ML/TF, notified by the supervisory authorities under article 40 of the Law and of which the financial institution is aware.
- Clients who/which are being or have been investigated for criminal activities, in particular ML/TF or any offence underlying the latter (provided this information is directly known by the financial institution or obtained from a reliable public source).
- Clients explicitly mentioned by the competent authorities as potentially related to ML/TF activities.
- Clients who/which carry out any sort of financial activity without being duly authorised or skilled to this end.
- Transactions evidencing a degree of complexity apparently unnecessary for the purpose for which they are intended, due to, *inter alia*, the number of financial operations, financial institutions, accounts, parties and/or countries or jurisdictions involved.
- Transactions for no apparent purpose or economic reason.
- Transactions whose frequency, unusualness or exceptionalness have no plausible reason in light of the client's profile.
- Transactions apparently inconsistent with current practice in the client's industry or business.
- Transactions involving shell companies.
- Transactions unrelated to the client's known business and involving persons or entities related to countries or jurisdictions publicly known as:
    - places of production of / trafficking in narcotics;
    - having high levels of corruption;
    - money laundering hubs;
    - sponsoring or supporting terrorism; or
    - sponsoring or supporting the proliferation of weapons of mass destruction.

- Transactions unrelated to the client's known business and involving persons or entities related to the countries, territories or regions with highly favourable tax systems contained in the list in Ordinance No. 150/2004 of 13 February or other countries or jurisdictions with highly restrictive banking secrecy legislation.
- Business relationships or occasional transactions in which it is sought to disguise the identity of the beneficial owners, notably through complex shareholding structures.

B. INDICATORS RELATED TO BANK DEPOSIT ACCOUNTS

- Clients who/which maintain a considerable number of bank deposit accounts open, in particular when some remain dormant for long periods.
- Clients who/which have bank deposit accounts with several credit institutions located in the same country/geographic area.
- Clients who/which make deposits without accurately knowing the sums to be deposited.
- Clients who/which open accounts with significant amounts of cash.
- Clients who/which frequently use personal accounts to execute transactions related to their business activity.
- Accounts frequently presenting operations for which the relevant accountholder gives no reasonable explanation.
- Accounts opened in branches geographically distant from the client's address or work place.
- Accounts whose operations largely exceed those foreseeable at the time they were opened.
- Accounts co-owned or operated by a high number of persons personally or professionally unrelated to one another.
- Accounts owned by legal entities pursuing unrelated economic activities, where all accounts are operated by the same individuals.
- Accounts operated through a high number of small credits and a small number of high debits.
- Accounts with frequent credits and/or debits in cash, where such operations are not consistent with the client's profile or business or activity.
- Accounts in which frequent deposits are made by persons apparently personally or professionally unrelated to the relevant accountholders.
- Accounts used to concentrate funds coming from other accounts which are subsequently transferred in block, in particular in the case of outbound international transfers.
- Accounts which, for no apparent reason, evidence a sudden increase in operations, amounts processed and/or their respective average balances.

- Accounts dormant for a long period and which are suddenly operated by significant amounts or deposits in cash.
- Accounts almost exclusively used to transfer funds to and from abroad.
- Accounts owned by entities domiciled in offshore centres and which have the same beneficial owner, with frequent and complex movements of funds.
- Accounts with a high and frequent number of deposits made exclusively through ATMs or night deposit facilities, in particular when these deposits are made in cash.
- Accounts with deposits in cash immediately after their accountholders access a safe that they have in the financial institution.

C. INDICATORS RELATED TO LOANS

- Early repayment of loans, when these are made:
    - unexpectedly and for no apparent logical reason;
    - with economic losses for the borrower;
    - using third-party funds;
    - using funds of uncertain origin and inconsistent with the client's profile;
    - using funds transferred from accounts with several financial institutions; or
    - in cash (in particular in the context of consumer loans).
- Loan applications for no apparent economic reason, taking into account, for instance, the significant value of the assets owned by the client.
- Loan applications by clients who/which show no interest in discussing the terms of the transaction, in particular the costs associated therewith.
- Loan applications based on security or assets, belonging either to the client or a third party, deposited with the financial institution and whose origin is unknown and whose value is inconsistent with the client's financial condition.
- Loan applications by clients who/which have already obtained loans from institutions located in offshore centres and which are unrelated to the client's known business.
- Loan applications by clients who/which declare income whose origin is not fully clarified by its owners to the financial institution.
- Loan applications by clients who/which propose the application of significant sums in deposits or other products in consideration for the approval of such loans.
- Loan applications whose documentation concerning the borrower intended for the respective file is supplied to the financial institution by a third party apparently unrelated to the transaction.
- Absence of evidence of how the sums lent are used, the client withdrawing in cash the loan amount deposited in his/her/its bank deposit account.

D. INDICATORS RELATED TO TRANSFERS OF FUNDS

- Transfers broken down into several transactions, so as to evade compliance with the legal and regulatory obligations applicable to transactions above a certain amount.
- Outbound international transfers inconsistent with the client's known business, notably due to their amount, frequency or beneficiaries.
- Transfers in which – at any time during the fund circuit, including when the funds are made available to their ultimate beneficiaries – any individuals or legal entities not duly authorised to carry out such business by the competent authorities of the relevant countries or jurisdictions act, formally or informally, in any capacity whatsoever.
- Transfers with no apparent connection between the client´s known business and the payors/beneficiaries of the transactions or the countries/geographic areas of origin/destination of such transfers.
- Transfers in which the client refuses or is reluctant to give an explanation for executing the transaction.
- Transfers in favour of a beneficiary or originating from a payor about whom/which the client proves to have little information or is reluctant to supply information.
- Transfers to amounts greater than those foreseeable when the business relationship was established with the client.
- Outbound international transfers to a significant number of beneficiaries apparently without any family ties to the client.
- Transfers to a significant number of beneficiaries who are nationals of countries or jurisdictions publicly known as being related to terrorist activities.
- Transfers regularly instructed by the same individual or legal entity to different beneficiaries and to equal or similar amounts.
- Transfers regularly instructed by the same individual or legal entity to the same beneficiary and to different amounts.
- Transfers instructed by different individuals or legal entities to the same beneficiary, on the same or very close dates.
- Transfers instructed by different individuals or legal entities who/which share one or more personal details (surname, address, employer, telephone number, etc.), and which are executed on the same or very close dates.
- Transfers instructed by different individuals or legal entities whose funds are made available by only one of them.
- Transfers made using third-party funds.

- Transfers to significant amounts with instructions to make the funds available to the relevant beneficiary in cash.
- Inbound international transfers in which the funds transferred are immediately withdrawn from the client's account or, if there is no account, are immediately transferred to other beneficiaries.
- Transfers with instructions to make the funds transferred available to third parties other than the beneficiaries of the transactions.
- Outbound international transfers matched with inbound international transfers to the same or similar amounts.
- Transfers in which clients show unusual interest and curiosity about the fund transfer system, such as operational procedures, limits, etc.
- Outbound international transfers made at a time apparently unrelated to the payment of wages, in particular when instructed by immigrant citizens.

E. INDICATORS RELATED TO MANUAL FOREIGN EXCHANGE TRANSACTIONS

- Transactions broken down into several sales/purchases, so as to evade compliance with the legal and regulatory obligations applicable to transactions above a certain amount.
- Transactions inconsistent with the client's known business, notably due to their amount or frequency.
- Transactions made at a foreign exchange rate more favourable to the financial institution than the advertised rate and/or payment of fees higher than those due, on the client's initiative.
- Transactions in which clients wish to exchange significant sums in a foreign currency for another foreign currency.
- Transactions with non-resident clients who appear to travel to the national territory in order to buy/sell foreign currency.
- Frequent transactions with low denomination banknotes or currencies with low international circulation.
- Transactions in which the clients give instructions to the financial company to subsequently deliver the resulting proceeds to a third party.
- Transactions in which the clients insist upon receiving the proceeds through a cheque of the financial institution, when this is not usual practice in the financial institution in question.
- Transactions in which the clients request to receive the proceeds in foreign currency in banknotes of the highest denomination possible.
- Transactions in which the clients request to receive the proceeds in several postal orders in low amounts, in favour of several beneficiaries.

F. ECONOMIC INDICATORS RELATED TO EMPLOYEES OF FINANCIAL INSTITUTIONS

- Employees who repeatedly fail to comply with AML/CFT legal obligations or internal procedures.
- Employees who establish informal and close relationships with clients that exceed the usual standards applying to their functions or are inconsistent with the financial institution's internal practice.
- Employees who evidence a pattern of social behaviour or other external signs inconsistent with their financial condition as known by the financial institution.

G. OTHER INDICATORS

- Transactions related to the sale of real estate in which:
    - the sale value is significantly above the market value;
    - payment is made by bearer cheque or a cheque endorsed in favour of a third party apparently unrelated to the transaction;
    - payment is made in cash, in particular originating from a bank deposit account owned by a third party apparently unrelated to the buyer; or
    - the property in question has been recently acquired by the seller.
- Transactions related to not-for-profit organisations in which:
- the nature, frequency or amount of transactions is inconsistent with the size of the organisation, its goals and/or its known activity;
- the frequency and amount of transactions suddenly increase;
- the organisation keeps significant amounts in its bank deposit account over extended periods;

a) the organisation only obtains contributions from individuals and entities not resident in Portugal;

b) the organisation seems to have little or no human and material means allocated to its activity;

c) the representatives of the organisation are not resident in Portugal, in particular when significant sums are transferred to the countries of residence of these representatives; or

d) the organisation is somehow related to countries or jurisdictions publicly known as places of production of/trafficking in narcotics, having high levels of corruption, money laundering hubs, sponsors or supporters of terrorism or sponsors or supporters of the proliferation of weapons of mass destruction.

Schedule IV - Version Control

Version no.	Date	Written by:	Approved by:	Nature of Change
1.0	11/08/2014	Compliance Department	Board of Directors	**Initial version**
2.0	20/03/2017	Compliance Department	Board of Directors	**Review of initial version** **Review of links and applicability** **Additions: Schedules III to V**
2.1	28/11/2017	Compliance Department	Executive Committee	Review of 2.0 Review of links and the applicable legislation, notably Law No. 83/2017 of 18 August
2.2	05/02/2019	Compliance Department	Executive Committee	Review of 2.1 Annual review of links and of the legal and regulatory framework, notably Notice no. 2/2018 of the Bank of Portugal.
2.2	15/09/2020	Compliance Department	Board of Directors	Ratified by the Board of Directors