NOVO BANCO

General Risk Management Policies for Money Laundering and Terrorist Financing

February 2021

NOVO BANCO GROUP

CONTENTS:

ANNEXES

1. GOALS

The purpose of this document is to:

- Present an integrated vision of the General Risk Management Policies for Money Laundering and Terrorist Financing;
- Establish the defining principles, action and diligence parameters to be used by Novo Banco Group (NBG) entities to prevent, detect, manage and mitigate the risks of money laundering and terrorist financing, and to effectively comply with restrictive measures and international penalties;
- Ensure compliance with the legal and regulatory requirements for the Prevention of Money Laundering and Terrorist Financing;
- Safeguard the exposure of Novo Banco (NB) and the Novo Banco Group (NBG) to situations that incorporate a potential risk of constituting the crime of Money Laundering and/or Terrorist Financing;
- Determine the performance vectors of the risk management model adopted in this regard, per specific risk assessment exercises on the topics of the Prevention of Money Laundering and Terrorist Financing.

2. ACRONYMS

Acronym	**Definition**
AML	*Anti Money Laundering*
MLTF	Money Laundering and Terrorist Financing
BdP	Banco de Portugal
CDD	Customer Due Diligence
DCIAP	Central Investigation and Penal Action Department of the Attorney General's Office
DSF	Declaration of Source of Funds
EDD	*Enhanced Due Diligence*
FATF	*Financial Action Task Force*
NBG	Novo Banco Group
HRC	High Risk Customers
KYC	Know Your Customer

KYP	Know Your Process
KYT	Know Your Transaction
NB	Novo Banco
OHPPP	Other holders of political or public positions
PMLTF	Prevention of Money Laundering and Terrorist Financing
PEP	Politically Exposed Person
CR-UBO	Central Registry-Ultimate Beneficiary Owner
RBA	Risk Based Approach
SLA	Service Level Agreement
UBO	Ultimate Beneficial Owner
UIF	Financial Information Unit of the Judicial Police
RMA	Relationship Management Application of SWIFT

3. LEGAL AND REGULATORY FRAMEWORK

3.1. COMPANY INFORMATION

- **Name:** Novo Banco, S.A.
- **Address**: Avenida da Liberdade, n.º 195, 1250-142 Lisbon, Portugal
- **SWIFT Code**: BESCPTPL
- **Legal status**: Limited liability corporation
- **Legal entity/Lisbon Commercial Registry Office no.:** 513 204 016
- **E-mail**: www.novobanco.pt
- **Corporate Boards**: www.novobanco.pt (Company homepage> NOVO BANCO> Governance> Corporate Boards)
- **International Presence**: www.novobanco.pt (*Home> For you> Useful information> Contacts> Bank network> Branches> International)*
- **Share capital**: € 5,900,000,000.00
- **Shareholders**: Nani Holdings, SGPS, S.A. (75%) and Fundo de Resolução (Public Legal Entity) (25%)

  - http://www.fundoderesolucao.pt/pt- PT/ofundo/Paginas/OFundo.aspx)

- **Supervisory Authorities**: European Central Bank (www.ecbc.europa.eu), Banco de Portugal (www.bportugal.pt), Portuguese Securities Market Commission (www.cmvm.pt), and Insurance and Pension Fund Supervisory Authority (www.asf.com.pt).
- **External Auditors**: EY – Ernst & Young Audit & Associados – SROC, S.A.
- **Contact**: *Chief Compliance Officer* – Compliance Department
- **Address**: Avenida da Liberdade, n.º 195, 1250-142 Lisbon, Portugal
- **Telephone**: (+351) 213 804 536 / **Fax**: (+351) 213 804 581
- ***E-mail***: compliance@novobanco.pt

3.2. INTERNATIONAL STANDARDS AND RECOMMENDATIONS

NBG respects and complies with all European regulatory and legislative frameworks and domestic norms with regard to PMLTF, by executing an implementing the corresponding legal and regulatory requirements.

- **Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015**, on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
- **Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May**, amending Directive (EU) 2015/849 of 20 May, on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.
- **Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October**, on combating money laundering by criminal law. Member States must implement the legislative, regulatory and administrative provisions needed to comply with this directive before 3 December 2020.
- **Council Directive (EU) 2016/2258 of 6 December 2016**, amending Directive 2011/16/EU, as regards access to anti-money-laundering information by tax authorities.
- **Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015**, establishing rules on information on the payer and the payee which must accompany transfers of funds, in any currency, for the purposes of preventing, detecting and investigating money laundering and terrorist financing.
- **Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018,** on controls of cash entering or leaving the European Union.
- **Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016**, supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies.
- **Commission Delegated Regulation (EU)** 2019/758 of 31 January 2019 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical standards for the minimum action and the type of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third countries.

- The **40 FATF recommendations** on money laundering and terrorist financing, dating from 1990 and revised in 1996, 2003, 2004 and 2012, including the latest revision of the 9 recommendations on terrorist financing, considered international standards with regard to these matters in mutually assessing the degree of compliance with these standards by members, together with identifying new risks and methodologies for combating criminal activities[1].
- **AML (Anti-Money Laundering) Principles of the Wolfsberg Group**[2]

3.3. DOMESTIC REGULATIONS AND LEGISLATION

- **Law No. 58/2020, of 31 August**, transposes Directive (EU) No.2018 / 843, on the prevention of the Financial System for the purpose of money laundering and terrorist financing and Directive (EU) No. 2018 / 1673, on combating money laundering and terrorist financing through criminal law. It introduces several and relevant changes to the legal diplomas that conform this matter, namely in Law no. 83/2017 and in Law no. 89/2017, also revising Law no. 97/2017 and the penal framework provided by Art. 368-A of the Penal Code - Decree-Law 400/82, all of which are set out below.
- **Law no. 83/2017 of 18 August**, establishing measures of a preventive and repressive nature for combating money laundering and terrorist financing. It partially transposes Directives 2015/849/EU of the European Parliament and of the Council of 20 May 2015, and 2016/2258/EU of the Council of 6 December 2016, amending the Criminal Code and Industrial Property Code and revoking Law no. 25/2018 of 5 June and Decree Law no. 125/2008 of 21 July.
- **Law no. 89/2017 of 21 August**, approving the Legal Scheme for the Central Registry-Ultimate Beneficiary Owner (CR-UBO). It transposes Chapter III of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015, and changes codes and other legal instruments.
- **Law no. 97/2017 of 23 August**, governing the application and enforcement of restrictive measures approved by the United Nations or by the European Union, and establishing the penalty scheme applicable to the breach of these measures.
- **Law no. 92/2017 of 22 August**, requiring the use of a specific payment method for transactions of €3,000 or more, amending the General Tax Law and the General Tax Infraction Scheme.
- **Law no. 52/2003 of 22 August**, passing the Anti-Terrorism Law amended by Law no. 59/2007 of 4 September, Law no. 25/2008 of 5 June, Law no. 17/2011 of 3 May, Law no. 60/2015 of 24 June and Law no. 16/2019 of 14 February;

[1] Portugal has been a FATF member since 1990.

[2] The *Wolfsberg* Group is comprised of several leading international financial institutions: Banco Santander, Bank of America, Bank of Tokyo – Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JPMorgan Chase, Société Générale, Standard Chartered Bank and UBS.

- **Law no. 52/2019 of 31 July**, passing the scheme for the performance of duties by holders of political positions and high public positions**.**
- **Law no. 5/2002 of 11 January and subsequent amendments,** establishing measures to combat organized and economic/financial crime. Establishes a special scheme for the collection of evidence, breach of professional secrecy and forfeiture of assets to the State for various types of crimes, including money laundering and the counterfeiting of money and comparable securities.
- **Law no. 15/2017 of 3 May** - Prohibits the issuance of bearer shares.
- **Criminal Code –** article 368-A - Money Laundering, on classifying the crime of money laundering.
- **Decree Law no. 61/2007 of 14 March**, approving the legal scheme applicable to the control of amounts in cash, transported by individuals, entering or exiting the EU through the national territory, together with the control of cash transactions with other EU Member States.
- **Decree Law no. 123/2017 of 25 September**, establishing the scheme for converting bearer securities into registered securities, enforcing Law no. 15/2017 of 3 May.
- **Ministerial Order no. 233/2018 of 21 August**, governing the legal scheme of the CR-UBO (Central Registry-Ultimate Beneficiary Owner), pursuant to articles 22 and 23 of Law no. 89/2017 of 21 August. The legal scheme of the CR-UBO is laid out in article 34 of Law 83/2017 of 18 August. **Respective "Amendment no. 33/2018" (Official Gazette [D.R.], Series 1 – no. 194 – 9 October 2018)**, publishing amendments to Ministerial Order no. 233/2018 of 21 August, with regard to article 14 (1) and article 17 (1).
- **Ministerial Order no. 200/2019 of 28 June,** establishing deadlines for the initial CR-UBO statement, and revoking articles 13 through 17 of Ministerial Order no. 233/2018 of 21 August. **Ministerial Order no. 310/2018 of 4 December**, defining the types of risk transactions to be reported on a systematic basis to the DCIAP (Central Investigation and Penal Action Department of the Attorney General's Office) and UIF (Financial Information Unit of the Judicial Police), and governing the form and terms of the notifications.
- **Ministerial Order no. 150/2004 of 13 February -** Approves the list of countries, territories and regions with clearly more favourable tax regimes (instrument re-enacted by article 290 of Law no. 114/2017 of 29 December**).**
- **Ministerial Order no. 345-A/2016 of 30 December**, on the amendment of Ministerial Order no. 150/2004, which establishes the list of countries, territories and regions with special tax schemes.
- **Council of Ministers Resolution no. 88/2015 of 1 October**, creating the Steering Committee for PMLTF Policies.

3.4. REGULATORY STANDARDS OF SECTORAL AUTHORITIES

- **Banco de Portugal Notice no. 2/2018 of 26 September**, governing the application of the following instruments: i) Law no. 83/2017 of 18 August; ii) Law no. 97/2017 of 23 August. It revokes Banco de Portugal Notice no. 5/2013 of 18 December, which included amendments introduced by Banco de Portugal Notice no. 1/2014 of 28 February.

This notice governs the following:

i) conditions for exercising, procedures, instruments, mechanisms, formalities of application, information provision obligations and other aspects needed to ensure compliance with preventive measures against money laundering and terrorist financing, within the business scope of financial entities subject to supervision by Banco de Portugal;

ii) the resources and mechanisms needed for these entities to comply with the obligations laid out in Law no. 97/2017;

iii) The measures to be taken by payment service providers to detect transfers of funds with omitted or incomplete information on the payer or payee, and the procedures to be used to manage transfers of funds not accompanied by the information required by Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015, with regard to information accompanying transfers ("Regulation (EU) 2015/847);

- **Banco de Portugal Notice no. 8/2016 of 30 September**, aimed at governing the obligations of registry and disclosure to Banco de Portugal pursuant to article 118-A (3) and (5) of the General Credit Institution and Financial Firm Scheme ("RGICSF") and article 9-A of the Legal Scheme for Payment Services and Electronic Currency ("RJSPME"), along with the conditions, mechanisms and procedures needed for actual compliance;
- **Banco de Portugal Notice no. 7/2009 of 16 September**, prohibiting the granting of credit to entities headquartered in offshore jurisdictions considered uncooperative, or whose final beneficiary is unknown, defining offshore jurisdiction and uncooperative offshore jurisdiction, and requiring a statement from the prudential supervisory authorities of offshore jurisdictions where credit transactions are to be performed, to ensure that there are no obstacles to the provision of information.
- **Banco de Portugal Notice no. 5/2008 of 18 December**, which states that credit institutions, financial firms and affiliates headquartered in third countries must have an internal control system to ensure efficient, cost-effective business performance, the existence of financial and management information which is complete, reliable, pertinent and timely, and respect for applicable legal and regulatory provisions. It revokes Notice no. 3/2006 of 9/5.
- **Banco de Portugal Instruction no. 5/2019 of 30 January 2019** - establishing a single annual reporting model and the required information to be reported periodically to Banco de Portugal by entities subject to supervision with regard to PMLTF.
- **Banco de Portugal Instruction no. 6/2020 of 6 March 2020 –** amending instruction no. 5/2019 to include information on specific procedures to comply with Regulation (EU) 2015/8 in the Money Laundering and Terrorist Financing Prevention Report;
- **CMVM Regulation no. 2/2020 of 5 March 2020**, establishing measures of a preventive nature to combat money laundering and terrorist financing to be implemented by obliged financial entities subject to CMVM supervision and by auditors within the scope of the powers granted by Law no. 83/2017 of 18 August ("LBCFT") and by Law no. 97/2017 of 23 August (Law no.

97/2017), and establishing periodic obligations for information to be provided by obliged entities.

- **Regulation no. 276/2019 of 26 March 2019,** of Instituto dos Mercados Públicos, do Imobiliário e da Construção, I. P. (IMPIC, IP) - Regulation for preventing and combating money laundering and terrorist financing in the real estate sector;
- **Regulation no. 686/2019 of 2 September 2019 of the Food Safety and Economic Surveillance Authority,** governing the specific obligations of preventing and combating money laundering and terrorist financing for managing entities of crowd funding platforms by donation or for consideration.
- **BdP Circular Letter no. CC/2020/00000062 of 27 November 2020**, on the application of reinforced measures – use of complex equity or domain structures for the practice of money laundering.
- **BdP Circular Letter no. CC/2020/00000063 of 27 November 2020**, on the application of reinforced measures – Use of companies established via expedited means for the practice of money laundering.
- **BdP Circular Letter no. CC/2020/00000074 of 31 December 2020,** on jurisdictions of risk and reinforcement on the FATF list.

4. RISK MODEL (MLTF)

Establishing an effective model for managing the risks of money laundering and terrorist financing ("Risk Model"), with suitable practices for identifying, assessing, managing, controlling and communicating the existing and future risks to which NBG is exposed in this regard, has become a priority in meeting the strategic goals which are aligned with the Group's business model, stakeholder commitments and regulatory requirements in force.

The managing board is responsible for establishing and annually updating the institution's degree of risk tolerance, by monitoring the effective risk profile and guaranteeing consistency between both.

The Compliance Department's organic structure, powers and duties have been approved by the managing board.

By ensuring the independence of the control function, as stated in the *"Compliance Function Regulations"*, the degree of tolerance to risk for NBG and its primary business units entails a respect for the defining principles of the "*Compliance Policies and Guidelines for NB Group Financial Entities",* in accordance with a methodology adapted to the circumstances and legal reality of each unit/market, based on the principle/axiom of a ***Risk-Based Approach*** **(RBA)**, the perceived level of risk and the Group's degree of exposure.

In accordance with the "Compliance Policies and Guidelines for NB Group Financial Entities", the Board of Directors has approved the "Money Laundering and Terrorist Financing Risk Management Model" document. This model undergoes updating periodically, or whenever justified by a relevant occurrence,

duly contextualized and published.

In this regard, the Risk Model used is rooted in a control environment which keeps the risk profile within established levels per the defined degree of risk tolerance, limits set for the types of risk considered acceptable for each relevant business, recommendations from supervisory and regulatory boards and best domestic and international practices.

As such, the Risk Model's primary means of mitigation are adequate programs in the areas of Know Your Customer (KYC), Know Your Transactions (KYT) and Know Your Process (KYP), implemented and defined in specific company procedure manuals and rules, as well as in a separate document, thereby ensuring legal and regulatory compliance as well as the rationale and underlying mechanisms of the institution's specific policies for managing these risks.

In terms of **risk jurisdictions**, NBG has three different changeable and dynamic AML risk scenarios, supported by international lists and domestic legislation, which point to different approaches for action, consideration and analysis, with three different risk grades – High Risk, Medium Risk and Low Risk.

4.1 COMPLIANCE RISK ASSESSMENT

The evaluation of risk, commonly known as *risk assessment*, is done by NBG within the scope and context of each operating process, by means of established mechanisms and procedures which: i) include the operating processes themselves; ii) are applied in the wake of the operating processes and underlying business relationships; iii) or, in some situations, à posteriori from the occurrence of these operating procedures or upon completion/execution of the transactions in relation to the established business relationships.

NBG considers and incorporates, in its functions for the prevention and detection of money laundering and terrorist financing, the latest market practices and most recent standards in force, supported in the Prevention of Money Laundering and Terrorist Financing Risk Model, which recently underwent review and updating.

This matter is specifically addressed in a related document.

5 CUSTOMER ACCEPTANCE POLICY[3]

Establishing any business relationship must be contextualized with respect for legal and regulatory requirements in force and, as such, subject to rejection in the following cases:

- Counterparties whose reputation, per credible sources, is tied to activities of a criminal nature or whose business precludes a justified knowledge of the assets' origin, or makes it difficult to prove;

[3] The concept of "customer" must be understood in a broad manner, including customers from business relationships, customers from sporadic transactions, customer representatives and people authorized to act on customers' behalf;

- Counterparties who, in the account opening process, refuse to provide information or documentation deemed necessary to properly comply with legal and regulatory obligations to which the bank is bound.
- Shell banks, entities performing activities akin or equivalent to those of a financial entity, entities established in a country or jurisdiction without a physical presence involving actual direction and management (with the mere existence of a local agent or subordinate employees not constituting a physical presence), and not belonging to a regulated financial group;
- Payable through accounts[4] - "Accounts made available by correspondents which, directly or through a sub-account, allow the performance of transactions, on their own behalf, by customers of the respondent or other third parties";
- Anonymous accounts, numbered accounts or accounts with fictitious names[5]: NBG does not provide its customers with anonymous or numbered accounts;
- Sanctioned entities, namely those on international lists to be referenced on a mandatory basis in the banking circuit;
- Entities with a specific risk profile, through indicators considered relevant to preventing money laundering and terrorist financing in relation to given business segments (e.g. management or marketing of digital currency; online and casino gaming/gambling) or given risk jurisdictions (e.g. offshore, non-cooperating centres);

Customers whose money laundering risk analysis justifies additional measures[6], namely situations legally classified as potentially higher-risk[7], new or existing business relationships within these situations or others defined internally according to their degree of risk, will be subject to **conditional approval** (subject to the scrutiny of the Compliance Department).

6 RISK FACTOR MITIGATING PROCESSES AND CONTROLS (MLTF)

6.1 KNOW YOUR CUSTOMER (KYC) - COUNTERPARTY ANALYSIS (ACCOUNT OPENING, EQUITY STAKE MANAGEMENT, COUNTERPARTY ASSESSMENT AND RMAs)

When establishing and monitoring business relationships with customers (account opening, inclusion of new holders in existing contracts, counterparty assessment in transactions (*due diligence*), and establishment of RMAs with financial institutions (*Relationship Management Application* of Swift), and

[4] Pursuant to article 2 (m) of Law no. 83/2017 of 18 August.

[5] Pursuant to article 64 of Law no. 83/2017 of 18 August.

[6] Pursuant to article 36 of Law no. 83/2017 of 18 August, which establishes measures for combating money laundering and terrorist financing, partially transposing Directives 2015/849/EU of the European Parliament and of the Council of 20 May 2015, and 2016/2258/EU of the Council of 6 December 2016, amending the Criminal Code and Industrial Property Code and revoking Law no. 25/2008 of 5 June and Decree Law no. 125/2008 of 21 July.

[7] Laid out in Annex III of Law no. 83/2017 of 18 August and BdP Notice 2/2018.

in compliance with general applicable regulatory duties such as identity verification and due diligence[8], processes and procedures are in place which employ computer tools used comprehensively for all risks identified, allowing customers to be classified in terms of their risk profile (*scoring*).

In this regard, the function of preventing money laundering and terrorist financing assigned to the Compliance Department can be activated via a request for additional support information and documentation, technical and/or targeted clarifications, cooperation in understanding ownership and control structures, and assistance in identifying UBOs (*Ultimate Beneficial Owners*), potentially even denying the start of the business relationship if items considered satisfactory are not obtained.

6.1.1. POTENTIALLY HIGHER RISK FACTORS AND TYPES

In addition to these general processes and procedures, based on legal and regulatory requirements and bearing in mind a more effective management of risks associated with MLTF, specific processes and procedures are used for potentially higher risk factors and types, namely with regard to: i) **Correspondent Relationships** (outside the European Union); ii) **Politically Exposed Persons** (resident and non-resident); iii) **Holders of Other Political or Public Positions**; iv) **and Actual Beneficiaries**.

6.2 TERRORIST FINANCING

Terrorist financing is a worldwide phenomenon, with serious repercussions on the reputation of financial institutions, of which we must be particularly wary.

A Terrorist Financing crime occurs when someone, by any direct or indirect means, provides, collects or holds funds, assets, products or rights which may be transformed into funds, for the purpose of being used in planning or carrying out terrorist acts, whose conduct and punishments are legally defined[9].

In compliance with the duties to prevent terrorist financing, and through internal communications and alerts, the main indicators of suspicion have been disseminated by the commercial departments so that, based on knowledge of customers (KYC) and their transaction profile (KYT), they may identify potentially suspicious behaviour and/or transactions.

6.3 CORRESPONDENT BANK RELATIONS

Initiating correspondent banking relationships (including accounts and RMAs) is subject to a scoring calculation, in which domiciliation – in high-risk third countries, in countries or jurisdictions not belonging to the European Union identified by the European Commission as having domestic schemes for combating money laundering and terrorist financing with strategic shortcomings constituting a significant threat to the European Union's financial system – is ranked, resulting in a relevant risk classification.

[8] Pursuant to article 23 of Law no. 83/2017 of 18 August – Duty of identification and diligence.

[9] In accordance with Law no. 83/2017 of 18 August, article 2 - "Definitions" sub-paragraph s) "*Terrorist financing", the conduct provided for and punished by article 5-A of Law no. 52/2003 of 22 August ("Anti-Terrorism Act"), as amended by Law no. 59/2007 of 4 September, Law no. 25/2008 of 5 June, Law no. 17/2011 of 3 May and Law no. 60/2015 of 24 June.*

The risk assessment is aimed at understanding the nature of the counterparty's business, proper licensing, whether its policies and procedures are aligned with the best international practices, the composition of its shareholder structure, members of its Executive Board, Actual Beneficiaries and open-source consultation, together with supplementary identification procedures as provided for by law[10].

Responses to bank correspondent due diligence requests (KYC/KYT) are also produced within the scope of PMLTF.

There are certain own transactions, within the scope of securities custody agreements in which the custodian banks are chosen by NB (service providers) to provide settlement services for securities custodianship and transactions in international markets, with a correspondent relationship with each of these entities, which are subject to identification and due diligence.
The securities transactions in question can be performed on behalf of customers or the bank, with a legal obligation to keep them in separate custodian accounts.

For these types of transactions, NB ensures the opening, upholding of conditions or closing of accounts which support this service at other banks. Custodian accounts opened at banks depend on, and are directly related to, technical accounts classified as Nostro accounts.

With regard to payment transactions, i.e. transfers issued or received by/from correspondent banks, clearing houses or other counterparties on behalf of customers, or on behalf of the bank itself, NB can also intervene in the opening, upholding of conditions or closing of the associated Nostro accounts.

6.4 OWN OPERATIONS

The bank includes the following under “Own Operations”:

i) Pure own portfolio transactions (securities, available funds and equity holdings) in which NB has the role of buyer/seller counterparty vis-à-vis clearing houses, brokers, selected custodians or other entities;
ii) Trading room transactions entered into and performed from the standpoint of cash management with banks and brokers;
iii) Transactions performed on behalf of third parties who are not customers (custodians, correspondents, financial intermediaries, agents, management and maintenance of RMAs, off-balance-sheet transactions, etc.).
iv) Own transactions (or otherwise) between NB and any other entities in the same group, outside the scope of a clientele relationship, i.e. intra-group transactions (NB with other NBG entities, and NB with foreign branches).

[10]Pursuant to article 27 of Law no. 83/2017 of 18 August – “Determining the purpose and nature of the business relationship, the origin and destination of the funds of the business relationship or sporadic transaction, and constant monitoring of the business relationship in accordance with the customer's risk profile”.

Transactions negotiated, compensated and settled by customer instructions by means of third parties, trading, custodians, liquidators, compensators, paying agents or others are not considered in this regard.

This aspect has been duly provided for in legislation in force, namely article 63 of Law 83/2017 of 18 August, and article 44 of BdP Notice no. 02/2018 of 26 September, while the activity itself is regulated by market mechanisms.

Business counterparty relationships comply with established contracts and SLAs (Service Level Agreements), which tend to follow international standards and conditions in clauses, thereby mitigating current risks associated with financial circuits.

As a rule, NB uses central market entities with recognized standard business practices (Interbolsa, LCH Clearnet), national brokers (Haitong and others) and international brokers (Pershing LLC and others) bound to rules in force and duly regulated and overseen by respective supervisors, as well as reputable global custodians also subject to strict regulatory frameworks (Euroclear, JPMorgan, Intesa SanPaolo, KAS Bank, Pershing LLC), using simplified due diligence measures for situations of continuity resulting from established contractual relationships and potentially low risk assessment.

In the event of risk from the standpoint of PMLTF, DCOMPL will be responsible for intervening in at attempt to gauge the requisite degree of mitigation and correction.

6.5 POLITICALLY EXPOSED PERSONS (PEPs), FAMILY MEMBERS AND ASSOCIATES OF PEPs AND OTHER HOLDERS OF POLITICAL OR PUBLIC POSITIONS (OHPPP)

In establishing business relationships, at the start or over their course (addition of holdings in contracts), with customers who are resident or non-resident PEPs[11] (*Politically Exposed Persons*) or who have a similar classification[12], the bank collects declarations with regard to the holding of the political/public position, with the involvement of higher hierarchical levels needed to authorize the establishment of business relationships with these customers.

Article 39 of Law 83/2017 of 18 August introduced a broader concept of PEP, expanding the range of natural persons to be distinguished, resulting in additional due diligence measures, namely the requirement to submit proof of assets (prior to establishing the business relationship or performing any sporadic transaction over the course of the relationship in the event of

the subsequent acquisition of the above-mentioned entities, over the course of updating information).

[11] Pursuant to article 2 Definitions – sub-paragraphs cc), dd), i), ii) and iii) of Law no. 83/2017 of 18 August, cc) *"Politically exposed persons", natural persons who perform, or who have performed in the past 12 months, in any country or jurisdiction, prominent public duties of a higher level; (…) dd) "Persons recognized as closely tied"; i) "Any natural person known as a co-owner of a politically exposed person (…)"; ii) "Any natural person who is the owner of share capital or holder of voting rights of a legal person (…) known as having a politically exposed person as an actual beneficiary"; iii) "Any natural person known to have corporate, commercial or professional relationships with a politically exposed person"*.

[12] Pursuant to article 2 - Definitions of Law no. 83/2017 of 18 August, sub-paragraph gg) "*Holders of other public political positions*", *natural persons who, not classified as politically exposed persons, perform or have performed, in the past 12 months and in the national territory, any of the following duties: i) the duties referred to in (3) of Law no. 4/83 of 2 April, Public control of the wealth of holders of political positions, as amended by Law no. 38/83 of 25 October, Law no. 25/95 of 18 August, Law no. 19/2008 of 21 April, Law no. 30/2008 of 10 July and Law no. 38/2010 of 2 September, when not classifying the respective holder as a "politically exposed person"; ii) Members of the representative or executive body of a metropolitan area or other forms of municipal association.*

Given the new regulatory requirements and questions involving the new model of the Money Laundering and Terrorist Financing Prevention Report, the bank made the necessary adaptations and technology developments with a view to: i) break down information between PEPs and OHPPPs, and; ii) individually consider the positions held and the jurisdictions where these PEPs perform (or performed) these functions.

The bank now records information on the following entities:

- **Politically Exposed Persons** - natural persons who in the last 12 months, in any country or jurisdiction, perform or have performed the following prominent senior public functions (list attached);
- **Close Family Members** – i) Parents or children of politically exposed persons; ii) Spouses or partners of politically exposed persons and spouses or partners of the politically exposed person's parents and children;
- **Persons recognized as closely tied** - i) Any individual known as a co-owner, with a politically exposed person, of a legal entity or charitable organization without legal status; ii) Any individual who is the owner of the share capital or holder of voting rights of a legal entity, or of the assets of a charitable organization without legal status, which is known to have a politically exposed person as an actual beneficiary; iii) Any natural person known to have corporate, commercial or professional relationships with a politically exposed person;
- **Holders of other political or public positions** - individuals who do not qualify as a politically exposed person, but in the past 12 months have held any of the following positions in the national territory (list attached).

The bank records information over the course of the transition period/implementation of the new model and retrieves the corresponding history.

6.6 CUSTOMER RISK ASSESSMENT AND SCORING MODELS

In establishing business relationships, and to understand the ownership and control structure of legal persons or charitable organizations without legal status, the bank identifies and collects information on the actual beneficiary(ies), thereby complying with the Duty of Identification.

The risk assigned to counterparties, their representatives and actual beneficiaries is gauged in two different ways:

1) Initially, by combining different risk indicators found in the bank's risk model and comprising the "PML/TF scoring"

   The result of the "PML/TF" scoring can be:

   i) Maintenance (low risk);
   ii) Monitoring (medium risk);
   iii) Investigation (high risk);

Only processes resulting in a scoring of "Investigation" (High Risk – Investigation) require intervention from DCOMPL.

Only processes obtaining a DMO scoring result (Medium Risk and Low Risk – Monitoring and Maintenance) are routed to and handled directly by the Operating Means Department (DMO)

2) Over the course of their relationship with the bank, through a collection of scores of a diversified nature, previously identified and re-evaluated at a regular frequency:

The result of "AML Risk" can be:

i) High;

ii) Medium;

iii) Low.

Within the scope of analysing and approving counterparties, and based on risk, measures are taken to prove the quality of actual beneficiaries, namely by collecting documentary evidence needed to fully understand the shareholder structure of these counterparties, so as to properly identify them and, at the same time, relate the actual beneficiaries identified with the customer.

Pursuant to the law, the bank performs consultations and, if applicable, notifies the competent service for the CR-UBO – Central Registry-Ultimate Beneficiary Owner, when any information on the actual beneficiary's capacity is omitted, inaccurate, non-compliant or outdated.

The bank also collects the identities of the managing boards, other relevant senior officials, and shareholders with voting rights of 5% or more.

6.7 INFORMATION UPDATING

Since understanding customers and gathering information to do so does not end at the time of establishing the business relationship, and must be reinforced and updated regularly in accordance with the assigned degree of risk or whenever events so justify, procedures have been put in place to fulfil the duty of updating information[13]. Measures for updating information have different priorities and frequencies and vary according to the degree of risk associated with the customer.

6.8. KNOW YOUR TRANSACTIONS (KYT) - MONITORING

With a view to constantly monitoring the performance of customers, customer transaction profiles are analysed, and customers undergo evaluation and comparison based on historical customer knowledge, the underlying economic rationale of the professional position and/or business sector, and their potential involvement in situations of money laundering and terrorist financing risk, while also considering the regions involved.

An understanding of the potential circuits of origin and destination of contractual funds is obtained at the time of establishing the business relationship. Subsequently, background information on the

[13] Pursuant to article 40 of Law no. 83/2017 of 18 August – Updating Procedures.

transacting of funds is assessed whenever needed which, together with the transactions recorded in each contact, must contain the identification of the ordering party and beneficiary.

With regard to controls in place for transaction monitoring (Monitoring), the bank conducts an assessment through a comparative analysis of alerts generated by an automatic contract monitoring tool, in accordance with specific parameters, with additional due diligence (EDD - Enhanced Due Diligence) measures whenever so justified, from the standpoint of preventing money laundering and terrorist financing.

Over the course of the monitoring process, special attention is paid to due diligence for international transactions (correspondent banks and pre-validation at the request of trade finance transactions), follow-up and account monitoring (AML alerts) and alerts related to risk transactions (which follow prior, adaptable limits and definitions).

The measures taken may, for example, result in the requirement for additional background information and the submission of supporting documentation, such as the Declaration of Source of Funds (DOF) or others.

6.9 SUSPICIOUS ACTIVITY REPORTS (SARs)

The bank has internal policies and procedures in place for reporting suspicious transactions to the competent authorities, in compliance with legal and regulatory provisions in force[14]:

i) DCIAP (Central Investigation and Penal Action Department of the Attorney General's Office;

ii) UIF (Financial Information Unit) – Judicial Police.

These notices fall under the Obligation of Refusal (article 50), the Obligation of Communication (article 43) and the Obligation to Abstain (article 47), established in Law no. 83/2017 of 18 August.

6.10 COOPERATION WITH AUTHORITIES

Due to different analytical and monitoring processes and operational diligence in the area of preventing MLTF, and in fulfilling the obligations of communication (Section IV – article 43), abstention (Section V – article 47) and cooperation (Section VI – Other Obligations - article 53) of Law 83/2017 of 18 August, responses to requests from competent and sectoral authorities are provided in a complete and perceptible manner, within the deadlines established by these authorities[15].

In this regard, the types of proceedings, among others, are primarily related to PMLTF investigations, within the scope of criminal proceedings, and miscellaneous requests from Banco de Portugal.
The bank's timely fulfilment of this obligation is a highly demanding exercise in terms of compiling reference information and making it available.

[14] Pursuant to article 43 of Law no. 83/2017 of 18 August – Reporting of Suspicious Transactions.

[15] Established in articles 43, 53 and 47 of Law no. 83/2017 of 18 August.

6.11 KNOW YOUR PROCESS (KYP)

6.11.1 RISK MODEL MANAGEMENT

For the purposes of managing the Risk Model, several organization-wide processes have been implemented to detect vulnerabilities, likelihoods of occurrence, potential impacts and mitigation factors for risks involving new accounts, information updating and operating processes for performing banking transactions, among other things.

6.11.2 HIGH-RISK CUSTOMERS

From the standpoint of managing PMLTF risk, multidisciplinary teams have been established at the Compliance Department to constantly monitor customers and transactions classified as high risk in the areas of *KYC*/*KYT,* along with a strategic plan specifically designed to control and oversee these types of customers and transactions, including: i) online filtering, and; ii) specific risk scenarios, custom-made and supported by a computer application (AML Manager). High-risk regions and risk groups on different continents have also been distinguished.

Using an RBA (***Risk Based Approach***) matrix, NBG monitors high-risk customers from two different aspects:

1) Recurrences Project – which includes an analysis of customers based on interactions with competent authorities (reports, official letters);

2) High Risk-Customers Project – which includes various aspects of AML risk, such as: i) customers requiring close monitoring; ii) jurisdictions considered as having risk; iii) certain business sectors (e.g. money remitters, virtual currencies, gambling); iv) certain corporate structures and groups.

6.11.3 CONSIDERATION OF COMPLIANCE RISK

The area of KYP (*Know Your Process*), in addition to a compliance risk assessment as previously explained, includes procedures for continuous and periodic monitoring (*backtesting*), the review of established content and adequacy vis-à-vis new legal and regulatory requirements, and the management of general risks in the context of PMLTF.

6.11.4 CLOSING OF ACCOUNTS BY COMPLIANCE DEPARTMENT REQUEST

In carrying out its functions of control, monitoring, oversight and the prevention of general MLTF risks, the Compliance Department may, under certain circumstances, request the closing of customer accounts as a last-resort risk mitigation measure.

These requests undergo regular monitoring, as well as analysis at Risk Committees attended by DCOMPL and the bank's management, and are included under internal company norms.

This practice falls under Law 83/2017 of 18 August (article 50 - 3b) – Obligation of Refusal) and BdP Notice no. 02/2018 of 26 September (article 39 – Obligation of Refusal), justifying the termination of the business relationship with the customer, whenever a potential MLTF risk is found which cannot be managed otherwise by the bank.

There are two means of closing contracts at the request of DCOMPL:

i) Resulting from an account opening process in which the decision is made to deny the contract;

ii) Resulting from due diligence in the area of transactions.

Closing requests by instruction from the bank and/or by decision from Compliance are executed and recorded by means of computer tools allowing the necessary tracking, and are done exclusively by employees responsible for this function. The status of requests is meticulously controlled and monitored until the account is actually closed.

6.12 APPROVAL OF NEW PRODUCTS AND SERVICES – SIGN-OFF PROCESS

The bank has a sign-off process prior to providing new products and services to customers over the course of its business, also extendable to NBG and managed by a specific area of the Compliance Department.

This process includes a set of company rules and procedures to be observed when designing and/or distributing products and services, for the purpose of identifying, evaluating and mitigating various associated risks from a preventive standpoint, including with regard to money laundering and terrorist financing.

6.13 HIGH RISK JURISDICTIONS

In view of risk indicators associated with high-risk countries or jurisdictions disseminated in documents published by leading international legal venues and similar entities, NBG does not intend to establish or maintain relationships with customers or counterparties, whether individual or collective, located in jurisdictions lacking effective systems for preventing money laundering and terrorist financing.

Of particular concern and note in terms of analysis and scrutiny, normally supported by enhanced due diligence measures and subsequent additional related actions and the collection of conclusive support documentation, are the risk qualities inherent to transactionality in centres considered offshore or whose parties have a specific quality entailing more exigent information requirements, such as PEPs and related persons, other holders of public positions as required by law, or even actual beneficiaries, namely when associated with complex corporate structures.

7 PENALTIES AND RESTRICTIVE MEASURES – FILTERING

Restrictive measures, also called sanctions, are a multilateral tool of a political, economic or diplomatic nature used by international institutions to exercise influence in matters such as preventing and repressing terrorism, promoting and defending human rights and public freedoms, discouraging armed conflicts and prohibiting the development of weapons of mass destruction.

In Portugal, Law no. 11/2002 of 16 February establishes the penal scheme for the breach of financial or commercial sanctions handed down by resolution of the United Nations Security Council or EU regulations with restrictions on establishing or maintaining financial or commercial relationships with

the States, other entities or individuals expressly identified.

The publication of Law no. 83/2017[16] of 18 August and Law no. 97/2017 of 23 August, and the provisions of the new MLTF Report, have reinforced and intensified the national legal and regulatory framework in this regard.
As a result, NBG is subject to domestic and international sanction schemes, namely those handed down by the European Union (Regulations and Directives), United Nations Security Council and ***OFAC*** – *Office of Foreign Assets Control (US Treasury Lists)* of *US President Executive Acts*, with regard to transactions in *USD* and the scope of secondary (extraterritorial) sanctions, when applicable.

AML processes also take FATF (OECD) lists and Portuguese legislation into account.

The filtering systems in place (database filtering) include consideration processes which constantly update and cross-reference the names of persons and entities on lists of sanctions and restrictive measures approved by key international organizations, with online filtering systems having been deployed for transactions, payments and transfers - SWIFT, SEPA and TARGET.

Also considering changes in records and international sanction schemes, and whenever deemed useful for the purposes of PMLTF operating security and clarity, the competent domestic authorities are consulted[17], and their interpretive recommendations are incorporated in this regard. Whenever applicable, and to more clearly define standards of commercial actions, these recommendations are also disseminated among job positions in the first line of defence (commercial areas) via publication at the bank's intranet.

Thanks to the growing concern for control, monitoring and the proliferation of lists and items tied to the filtering process, a higher number of hits have been generated, whose context and assumptions of generation are scrutinized, in an ongoing effort to lower the number of false positives and focus on relevant positive hits.

7.1 *WOLFSBERG AML QUESTIONNAIRE*

The bank follows the principles found in the Wolfsberg AML Questionnaire with regard to PMLTF. This document, which is updated periodically, has been published at the bank's website: www.novobanco.pt.

7.2 *USA PATRIOT ACT CERTIFICATE*

In accordance with the "*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 2001 (USA Patriot Act*), NB may be required to provide, whenever necessary, a *Certification Regarding Accounts for Foreign Banks*.
The USA Patriot Act has been published at the bank's website: www.novobanco.pt.

[16] Article 21 - Restrictive Measures; article 18 - Information systems and procedures in general; article 169 – Administrative offences and Annex III – Non-exhaustive list of potentially higher risk factors and types, (3) – Risk factors associated with geographic location, sub-paragraph c) *Countries and jurisdictions subject to sanctions, embargoes or other restrictive measures or additional countermeasures, imposed by the United Nations and European Union,* and d) *Countries and jurisdictions providing financing or support to terrorist acts or activities, or where terrorist organizations operate.*

[17] Ministry of Foreign Affairs and Ministry of Finance.

8 TRAINING

Engagement in the first line of defence (commercial areas) is assumed as a strategic action related to the phenomena of money laundering and terrorist financing. In this regard, there are annual training cycles, subject to final certification, through the e-learning platform for all the bank's employees.

In addition, in-person training sessions are held at the areas of the bank most exposed to MLTF risk, such as the Business Centres and similar structures.

The Compliance Department also updates specific knowledge and job training, on a regular basis, for employees and technical staff allocated to the prevention and detection of money laundering and terrorist financing.

9 CODE OF CONDUCT, POLICIES FOR CONFLICTS OF INTEREST, RELATED PARTIES AND ANTI-CORRUPTION [18] - WHISTLEBLOWING POLICY

NBG's Compliance Department encourages all NBG entities and employees to fulfil all applicable legal, regulatory, statutory, operational, tutelary, ethical and behavioural requirements within the institutional control and supervision environment defined by competent regulatory authorities and the legal norms to which they are subject, by acting with the utmost integrity, honesty, diligence, competence, transparency and neutrality.
To this end, a Code of Conduct, Conflict of Interest Policy, Policy for Transactions with Related Parties, Regulation for the Reporting of Irregularities (Whistleblowing) and Anti-corruption Policy have been disseminated to NBG and its employees.

The Code of Conduct has a specific chapter on obligations for detecting and preventing money laundering and terrorist financing, focusing on procedures in place for identifying customers and monitoring business relationships, analysing transactions performed during these relationships and verifying compliance with information previously obtained and knowledge of the customer in view, among other factors, of significant changes in account transaction patterns and consistency between the transactions performed and the customer's profile.

The purpose of the anti-corruption policy, which recently underwent updating and development, is to prevent and mitigate the risk of corruption, bribery and related practices, reaffirming NB's commitment to build a more upright society.

The policy addresses practices such as corruption, the receipt of improper advantages, influence peddling, embezzlement, economic participation in business, extortion, abuse of power, bribery,

[18] The Code of Conduct, Conflict of Interest Policy and Policy for Transactions with Related Parties are available at NB's website https://www.novobanco.pt/site/cms.aspx?plg=3AE91E8E-AAFB-4BD0-8C6A- 07823384AEE3.

violation of secrecy and facilitation payments. Prohibited payments have been defined for this purpose, together with applicable rules for entering into consortiums and joint ventures and their associated rules and obligations.

At the same time, with a view to constantly monitoring the behaviour of its customers, customer transaction profiles are also analysed from the standpoint of market risk to detect potential situations of insider trading or the abuse of confidential information, conflicts of interest, corruption, incentives received ("Gift Policy"), ethics and conduct.

10 MONITORING OF BRANCHES AND SUBSIDIARIES

In the context of preventing money laundering and terrorist financing, there are policies and procedures in place ("*Compliance Policies and Guidelines for NB Group Financial Entities")* to ensure conformity with base domestic legislation, with the same applicable defining principles and action and diligence parameters for the compliance function.

10.1 APPLICATION TO NOVO BANCO GROUP ENTITIES

Novo Banco ensures that its subsidiaries adopt the defining principles and action and diligence parameters established by these policies, with the approval of their respective managing boards.

10.2 COORDINATION MODELS

At the same time, with a view to clearly defining responsibilities and operating methods between the compliance areas of NBG's various structures (branches and subsidiaries), bilateral Coordination Models have been defined, subject to periodic review and monitoring by a specific unit within the Compliance Department.

11 INFORMATION RETENTION

Original documents, copies, references and any other durable mediums provided by customers or counterparties in relation of to the identification and due diligence process, together with any documents, transaction records and support analyses demonstrating compliance with applicable legal and regulatory provisions, are kept in accordance with legally established deadlines after the time of the identification process, performance of the transaction and end of the business relationship.

12 DATA PROTECTION

Preventing and combating money laundering and terrorist financing are expressly recognized as a domain of protecting a public interest, including with regard to the processing of personal data based on Law no. 83/2017 of 18 August[19], and as referenced in the General Data Protection Regulation

[19] Pursuant to article 57 - Objective and purpose of the law

(GDPR) approved by the European Parliament on 27 April 2016 with mandatory enforcement as of 25 May 2018 in all European Union Member States, substituting Law no. 67/98[20] of 26 October in Portugal (transposition of Directive 95/46/EC).

13 INTERNAL CONTROL AND AUDITS (INTERNAL AND EXTERNAL)

To supplement the control function performed by the third line of defence (Internal Auditing), and within the scope of systematically assessing the effectiveness of NBG's Internal Control System, annual effectiveness tests are performed on the Process for Preventing and Detecting Money Laundering and Terrorist Financing[21].

Compliance with legal and regulatory provisions in force with regard to the Compliance Department's control functions is also assessed, per the terms and frequency established by External Auditors – External Auditing, subject to a specific opinion and notification to the supervisory authority, including in annual reports on the money laundering and terrorist financing prevention function[22].

14 PARTICIPATION IN SECTORAL WORKGROUPS

Participation in meetings and sectoral working groups (Portuguese Banking Association/APB, Financial Information Unit/UIF, International Chamber of Commerce/ICC) also aims to encourage NBG to continue to comply as a generator of knowledge and sharing of best practices in PMLTF matters.

15 NBG STRATEGIC PROJECTS

NBG has been focusing on strategic projects which, by their nature, appositeness and goals, directly impact issues involving MLTF, particularly General Policies for Managing the Risks of Money Laundering and Terrorist Financing.

These include the Digital Bank Project, the 2018-2021 Talent and Merit Project, and the APIC Project.

15.1 DIGITAL BANK PROJECT

The purpose of this project is to give the bank the necessary tools for modern digital banking, in line with domestic and international trends and markets, and applicable to all operating processes and channels.

[20] Personal Data Protection Act

[21] The methodology used by DAI is based on Effectiveness Tests as required in article 44 (d) of BdP Notice no. 5/2013, involving the use of measures of a preventive and repressive nature in combating money laundering and terrorist financing, as provided for in Law no. 83/2017 of 18 August.

[22] Pursuant to the terms of BdP Notice no. 9/2012 of 17 May, approving the Money Laundering and Terrorist Financing Prevention Report (RPB), which must be completed annually and sent to BdP through the BPnet system.

Novo Banco has also named a *Chief Digital Officer* (CDO), whose role is to lead the required deployments, and to provide a comprehensive inter-departmental vision.

The goal is to make Novo Banco a cutting-edge digital bank, namely through the following projects:

- Marketplace, a new concept of "going to market" virtually
- Homebuying, reinventing the home buying experience
- Small Business Finance (SFB), to enhance the financing experience for the business segment;
- Onboarding, improving the experience in the customer's first contact with the bank.

15.2 2018-2021 TALENT AND MERIT PROJECT

The main goal of this project is to lay out a strategic future path for NBG, founded on several cornerstones for transforming processes and technologies, in particular those of "IT" and "Risk Adjustment". The program is aimed at achieving differentiation, digitalization and optimization.

This analysis includes a refocusing of IT tools to support AML processes. This will be done through functional improvements, and through supplementary and/or alternative solutions allowing integrated information management (transaction and database filtering, monitoring, risk case analysis, reporting and data management), the communication of intra-application information and a single integrated customer vision. This is essential in tackling the mounting complexity of risk scenarios and circuits.

15.3 APIC PROJECT

This multi-departmental project involves the ongoing updating of NB customer information to comply with regulatory obligations in force.

Since the project applies to the bank's entire technology area and operations, the solution was designed from the standpoint of fully capitalizing on the use of digital channels, while at the same time keeping analogue support features, when justified.

The solution aspires to incorporate legal requirements on information collection and updating into NB's normal business relationship with its customers, turning them into opportunities.

It has several different goals, including: i) definition of an automatic solution, prioritizing digital supports to deploy the process; ii) design of a versatile solution combining the bank's various documentation areas and systems; iii) design of a flexible solution to process control data on ongoing results; iv) structuring the process following a rationale of efficiency and minimum impact on commercial areas; v) design of a solution to reduce operating costs, mitigate operating risks and improve customer relations.

Key implementations target NB's relationship in customer onboarding through the Digital Novo Banco Project, and the KYC deployments under Law 83/2017 of 18 August.

16 CRITICAL ANALYSIS OF MLTF MODEL IMPLEMENTED – FUTURE GOALS

NBG performs a constant critical analysis of the MLTF model implemented, bearing numerous enveloping factors in mind, domestic and international current events, changes in the legal framework, market trends and practices, technology developments and new strategic projects, among other factors.

As such, and orienting the vision of exigency and mounting importance of PMLTF towards the goals of the strategic programs in progress, DCOMPL, in its independent control function, is responsible for focusing its attention on the aspect of KYP (*Know Your Process*) vis-à-vis market demands and a complex legal framework, obviously without overlooking the supplementary aspects of KYC (*Know Your Customer*) and KYT (*Know Your Transaction*).

The main strategic goal for the future is managing a single, integrated view of the customer at any given time, together with information produced by the various base processes of PMLTF (counterparty analysis, filtering – operations and database, monitoring and risk case analysis, reporting and data management). Process orientation entails particular attention to mechanisms, circuits, production and validation of statistical data, the overall quality of the results obtained, procedural control and meticulous risk analysis.

NBG has the goal of focusing on inter-related IT developments and AML solutions as audit trail tools, the incorporation of new risk scenarios, and auxiliary statistical models for PMLTF analysis and management decisions.

17 GENERAL RISKS ASSOCIATED WITH CASH TRANSACTIONS

This issue becomes particularly important with regard to PMLTF circuits; as such, it is pertinent to have an approach of reinforced control, identifying the depositors and parties in general transactions of exchanging cash in accordance with the specific circumstances of the transaction. Within this context is the mechanism for requesting the Statement of Origin and Justification of Funds (DOF) for certain types of transactions, together with the current duties of identifying the depositors. The same rules are followed for cash exchange transactions classified as Sporadic Transactions.

18 MLTF PREVENTIVE DUTIES - BANK AND EMPLOYEES

Law 83/2017 of 18 August establishes measures of a preventive and repressive nature for combating MLTF, expanding the scope and reinforcing compliance with the 10 Preventive Obligations of MLTF to be observed by financial institutions (NBG) and their employees.

These obligations are also addressed in the new Annual MLTF Report.

18.1. OBLIGATION OF CONTROL

Requires financial institutions to apply actual policies, procedures and controls to effectively manage the risks of money laundering and terrorist financing, and to comply with legal and regulatory norms in this regard.

18.2. OBLIGATION OF IDENTIFICATION AND DUE DILIGENCE

Requires procedures to be fulfilled in this regard under any of the following circumstances:

- Establishment of a business relationship;
- Performance of sporadic transactions of €15,000.00 or more (regardless of whether through a single transaction or several transactions that appear to be related) or constituting a transfer of funds of an amount greater than €1,000.00;
- It is suspected that the transactions may involve ML or TF;
- There are doubts with regard to the accuracy or suitability of previously obtained customer identification data.

This obligation also applies to other entities, namely: i) third parties; ii) credit brokers; iii) promoters and intermediation relationships; iv) outsourcing.

18.3. OBLIGATION OF COMMUNICATION

This entails the obligation to report whenever it is known, it is suspected or there are sufficient reasons to expect that funds or assets originate from criminal activities or are related to the financing of terrorism, including all transactions proposed, attempted, in progress or executed in this regard.

18.4. OBLIGATION TO ABSTAIN

Requires the denial to perform transactions known or suspected to be associated with funds or other assets originating from or related to criminal activities or terrorist financing.

18.5. OBLIGATION OF REFUSAL

This entails refraining from starting a business relationship, or performing a sporadic or other transaction, under any of the following circumstances:

- Failure to obtain identification information and respective proof of identity from the customer, representative or actual beneficiary, including information needed to ascertain the capacity of actual beneficiary and ownership structure of the customer;
- Information on the nature, aim and purpose of the business relationship;
- Identification and due diligence procedures cannot be fulfilled, including data updating procedures.

18.6. OBLIGATION OF RETENTION

Requires archiving for seven years from the time of processing the customer's identification or, in the case of business relationships, after their end.

18.7. OBLIGATION TO INVESTIGATE

Entails the obligation to examine with particular care and attention, intensifying the degree and nature of monitoring, in the event of finding conduct, activities or transactions whose constituent nature makes them potentially related to funds or other assets originating from criminal activity or related to terrorist financing.

Following are some specific examples of characteristic features to take into account:

a) The nature, purpose, frequency, complexity, unusualness or atypicality of the conduct, business activity or transactions;

b) The apparent non-existence of an economic goal or lawful purpose associated with the conduct, activity or transactions;

c) The amounts, source and destination of the transactions;

d) The place of origin and destination of the transactions;

e) The payment methods used;

f) The nature, business activity, transaction pattern, the economic-financial situation and profile of the parties involved;

g) The type of transaction, product, business structure or charitable organization without legal status, which could especially favour anonymity.

18.8. OBLIGATION OF COOPERATION

Requires prompt, full cooperation when requested by competent authorities (DCIAP-PGR / UIF-PJ), judicial and police authorities, tax and customs authorities, and sectoral authorities.

18.9. OBLIGATION OF NON-DISCLOSURE

Requires the non-disclosure of information to customers or third parties, namely information related to communications made, in progress or to be made to competent authorities, or on information requests from them, or that investigations, inquiries, inspections, analyses or legal procedures by these authorities are in progress. It requires prudence with customers related to the performance of particularly suspicious transactions, avoiding any measures which, for any reason, may raise suspicions that any procedures are in progress aimed at investigating suspected practices related to MLTF.

Any breach of this obligation by employees or the financial institution may result in criminal offences subject to prison sentences and fines.

18.10. OBLIGATION OF TRAINING

Requires the performance of regular, specific training initiatives to teach employees how to recognize transactions potentially involving MLTF and act according to the law and its associated regulatory norms.

19 DOCUMENT MANAGEMENT

19.1 ADEQUACY, INTERPRETATION, VALIDITY AND PERIODIC REVIEW

Novo Banco, S.A.'s managing board is responsible for approving this document.

The Compliance Committee is in charge of the interpretation and suitability of its content.

Its content and suitability must be reviewed periodically, simultaneously with the review and updating of Novo Banco's risk model, and whenever there are legal, regulatory or other relevant changes to the MLTF risk control function.

Please contact the Compliance Department's Money Laundering Prevention and Detection Unit (UPBCFT) for any clarifications with regard to these policies.

19.2 MANAGEMENT OF RELATED DOCUMENTS

Within the scope of all powers and jurisdictions of the Unit for the Prevention and Detection of Money Laundering and Terrorist Financing (UPDBCFT of the Compliance Department), in addition to the General Risk Management Policies for MLTF in this document, there exists one effective and integrated consideration within the scope and context of each operating process of the evaluation of compliance risk, commonly called *Risk Assessment,* following the latest market practices and recent legal standards in force, which is addressed in a separate related document, the Risk Management Model for the Prevention of Money Laundering and Terrorist Financing.

The Risk Management Model was developed with the main goal of creating a model in line with legislation and regulations in force, simultaneously tailored to the bank's reality, based on the following:

- An identification and assessment of the risk factors applicable to the Bank, taking into account legislation, regulations and best industry practices;
- Evaluation of the bank's internal control system for PML/TF and sanctions, with mapping of risks and controls, in order to identify areas where the Internal Control System needs to be strengthened;
- Mapping and solution from recommendations of internal and external audits done on the internal control system.

ANNEXES

A. LIST OF NON-COOPERATING COUNTRIES PUBLISHED BY FATF

The Financial Action Task Force (FATF) works to identify jurisdictions with strategic deficiencies in the area of money laundering and terrorist financing, and still lacking sufficient progress in overcoming these deficiencies and/or failing to agree on an action plan with the FATF to this end.

Three times per year, the FATF issues "Bulletins" identifying jurisdictions considered "high-risk" and "uncooperative"[26].

According to the last bulletin published in the wake of the plenary meeting of 21 February 2020 (Paris), the following jurisdictions have been identified and updated:

FATF PUBLIC STATEMENT			*IMPROVING GLOBAL AML/CTF COMPLIANCE*	
Jurisdiction subject to applicable countermeasures		Jurisdiction subject to a special associated risk weighting	Jurisdiction subject to monitoring	Jurisdiction no longer subject to monitoring
Plenary Meeting of 23 October 2020 (Paris)	Democratic People's Republic of Korea (North Korea) Islamic Republic of Iran	-	Albania The Bahamas Barbados Botswana Cambodia Ghana Jamaica Mauritius Myanmar Nicaragua Pakistan Panama Syria Uganda Yemen Zimbabwe;	Iceland Mongolia

The information shown here should be confirmed at the website referred to in note 23, in view of periodic updates to bulletins issued by FATF.

25 Disclosed through a Banco de Portugal circular letter.

26 Bulletins available for consultation at "http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)", which includes a history of "high-risk non-cooperating jurisdictions" identified over the years.

B. THIRD COUNTRIES WITH STRATEGIC DEFICIENCIES IN MLTF, NON-COOPERATING TAX JURISDICTIONS AND OFFSHORE LEGAL SYSTEMS

List of third countries with strategic deficiencies in their frameworks for combating money laundering and terrorist financing, published by the European Commission on 13 February 2019

- Afghanistan
- American Samoa
- Bahamas
- Botswana
- Democratic People's Republic of North Korea
- Ethiopia
- Ghana
- Guam
- Iran
- Iraq
- Libya
- Nigeria
- Pakistan
- Panama
- Puerto Rico
- Samoa
- Saudi Arabia
- Sri Lanka
- Syria
- Trinidad and Tobago
- Tunisia
- U.S. Virgin Islands
- Yemen

List of non-cooperating tax jurisdictions, also published by the European Commission (last updated on 06 october 2020):

- American Samoa
- Anguila
- Barbados
- Fiji
- Guam
- Palau
- Panamá
- Samoa

- Trinidad and Tobago
- U.S. Virgin Islands
- Vanuatu
- Seychelles

*List of Offshore Legal Systems**, published in Annex III to Banco de Portugal Notice no. 8/2016***

- Anguilla
- Antigua and Barbuda
- Netherlands Antilles
- Aruba
- Bahamas
- Bahrain
- Barbados
- Belize
- Bermuda
- Bolivia
- Brunei
- Cape Verde
- Channel Islands
- Cayman Islands
- Cocos (Keeling) Islands
- Cyprus
- Cook Islands
- Costa Rica
- Delaware
- Dominica
- Egypt
- United Arab Emirates
- Falkland Islands
- Fiji
- Philippines
- The Gambia
- Granada
- Gibraltar
- Guam
- Guatemala
- Guyana
- Honduras
- Hong Kong

- Yemen
- Indonesia
- Iran
- Jamaica
- Djibouti
- Jordan
- Kiribati
- Kuwait
- Lebanon
- Liberia
- Liechtenstein
- Special Administrative Region of Macau
- Malaysia
- Maldives
- Isle of Man
- Northern Mariana Islands
- Marshall Islands
- Mauritius
- United States Minor Outlying Islands
- Myanmar
- Monaco
- Montserrat
- Nauru
- Christmas Island
- Nevada
- Nigeria
- Niue
- Norfolk Island
- Oklahoma
- Oman
- Federated States of Micronesia
- Palau
- Panama
- Pakistan
- Pitcairn Islands
- French Polynesia
- Puerto Rico
- Qatar
- Solomon Islands
- American Samoa
- Samoa

- Saint Lucia
- Saint Helena, Ascension and Tristan da Cunha
- Saint Kitts and Nevis
- San Marino
- São Tomé and Príncipe
- Saint Pierre and Miquelon
- Saint Vincent and the Grenadines
- South Georgia and the South Sandwich Islands
- Seychelles
- Singapore
- Swaziland
- Switzerland
- Svalbard Islands
- Tokelau
- Tonga
- Trinidad and Tobago
- Turks and Caicos Islands
- Turkmenistan
- Tuvalu
- Ukraine
- Uruguay
- Uzbekistan
- Vanuatu
- British Virgin Islands
- United States Virgin Islands
- Wyoming

C. LIST OF POLITICALLY EXPOSED PERSONS (PEPs) AND LIST OF HOLDERS OF OTHER POLITICAL OR PUBLIC POSITIONS.

. LIST OF POLITICALLY EXPOSED PERSONS (PEPs)

i) Heads of state, heads of government and government members, namely ministers, secretaries and deputy secretaries of state;

ii) Commissioners;

iii) Judges of the Constitutional Court, the Supreme Court of Justice, Supreme Administrative Court, the Court of Auditors and members of supreme courts, constitutional courts and other high-level judicial bodies from other states and international organizations;

iv) Representatives of the Republic and members of government bodies of the Autonomous Regions;

v) Ombudsmen, Councillors of State, members of the National Commission for Data Protection, the Superior Council of the Judicature, the Superior Council of Administrative and Tax Courts, the Attorney-General of the Republic, the Superior Council of the Public Prosecutor's Office, the Superior Council of National Defence, the Economic and Social Council and the Regulating Entity for the Media;

vi) Heads of diplomatic missions and consular posts;

vii) Generals of the Armed Forces on active duty;

viii) Presidents and councillors with executive functions in local councils;

ix) Members of the board of directors and supervisory boards of central banks, including the European Central Bank;

x) Members of the boards of directors and supervisory boards of public institutes, public foundations, public establishments and independent administrative entities, regardless of their title;

xi) Members of the boards of directors and supervisory boards of entities belonging to the public business sector, including local and regional business sectors;

xii) Members of executive bodies of national or regional political parties;

xiii) Directors, assistant-directors and members of the board of directors or people who perform equivalent functions in an international organization.

. . LIST OF HOLDERS OF OTHER POLITICAL OR PUBLIC POSITIONS

i) The positions listed in article 4 (3) of Law no. 4/83 of 2 April, Public control of the wealth of holders of political positions, as amended by Law no. 38/83 of 25 October, Law no. 25/95 of 18 August, Law no. 19/2008 of 21 April,

Law no. 30/2008 of 10 July and Law no. 38/2010 of 2 September, when not

classifying the respective holder as a “politically exposed person”;

a. Members of management bodies of State owned companies, when appointed by the State;

b. Members of independent public entities provided for by the Constitution or by law;

c. Members of the governing bodies of public institutions;

d. Public administrators;

e. Directors and officers of companies that are part of the local business sector;

f. Top level management officers and similar.

ii) Members of the representative or executive body of a metropolitan area or other forms of municipal associations;

D. ANNEX III TO LAW NO. 83/2017 OF 18 AUGUST - NON-EXHAUSTIVE LIST OF POTENTIALLY HIGHER RISK FACTORS AND TYPES, IN ADDITION TO SPECIFIC SITUATIONS PROVIDED FOR BY LAW

1 – Risk factors associated with customers:

a) Business relationships which develop into unusual circumstances;
b) Customers residing or doing business in higher-risk geographic zones, as determined in (3) of this annex;
c) Legal persons or charitable organizations without legal status which are structures for the holding of personal assets;
d) Companies with fiduciary shareholders (nominee shareholders) or whose share capital is represented by bearer shares;
e) Customers whose business activities involve intensive cash transactions;
f) Structures owned or controlled by the customer which seem unusual or excessively complex given the nature of the activity pursued.

2 – Risk factors associated with products, services, transactions or distribution channels:

a) Private Banking;
b) Products or transactions favourable to anonymity;
c) Payments received from unknown third parties or not associated with the customer or the activity pursued by customer;
d) New products and new business practices, including new distribution mechanisms and payment methods, and the use of new technology or technology under development, for both new and existing products.

3 – Risk factors associated with geographical location

a) Companies identified by reliable sources (such as published mutual evaluation reports, detailed evaluation reports or monitoring reports) as lacking effective systems for preventing money laundering and terrorist financing, notwithstanding the provisions of this law with regard to high-risk third countries;
b) Countries or jurisdictions identified by credible sources as having significant levels of corruption or other criminal activities;
c) Countries or jurisdictions subject to sanctions, embargoes or other restrictive measures or additional countermeasures imposed by the United Nations and the European Union;
d) Countries or jurisdictions that provide funding or support for terrorist activities or acts, or in whose territory terrorist organizations operate.