Policy on combatting money laundering and terrorist financing

Board of Directors' Meeting of 20/11/2019

1 INTRODUCTION

Money laundering and the terrorist financing are criminal actions which constitute a serious threat to the lawful economy, also since they can be transnational, and can cause destabilising effects, especially for the banking and financial system.

The changeable nature of the money laundering and terrorist financing threats, facilitated also by the continued development of technology and resources available to criminals, requires constant adaptation of the prevention and combatting controls.

The recommendations of the International Financial Action Task Force (GAFI) - the main international coordinating body - provide that the private sector and public authorities identify and evaluate the risks of money laundering and terrorist financing that they are exposed to in order to adopt adequate mitigation measures.

The prevention and combatting of money laundering is manifest by introducing controls aimed at ensuring full awareness by the customer, the traceability of financial transactions and the identification of suspicious transactions.

The intensity of the prevention and combatting controls is modulated in accordance with a risk based approach, focused on hypotheses worthy of greater scrutiny and carried out by making the monitoring more effective and making the allocation of resources more efficient. This approach represents the cornerstone of the behaviour of the obliged parties and the control actions by the Authorities.

Banca Mediolanum S.p.A. (hereinafter also referred to as the "**Bank**" or the "**Parent Company**") and the Mediolanum Banking Group companies (hereinafter also the "**Group**") are strongly committed to ensuring that the products and services on offer are not used for the criminal aims of money laundering or terrorist financing, promoting a culture based on full compliance with prevailing law and the efficient fulfilment of passive cooperation obligations in order to guarantee greater awareness by customers, storage of the documents relating to the transactions carried out and active cooperation in order to identify and report suspected money laundering transactions.

The Board of Directors has to identify governance policies for said risks that are adequate with respect to the extent and type of risk profiles that the Bank's business is actually exposed to, taking into account the outcomes from the self-evaluation process applied to the money-laundering and financing of terrorism risks which represents the necessary condition for the definition and maintenance of the controls over these risks.

The CEO prepares the procedures needed to implement said policies; the Anti-Money Laundering Function continuously checks the suitability of the procedures in order to ensure adequate monitoring of said risks, coordinating with the other corporate control functions. The Internal Audit Function continuously monitors the level of adequacy of the corporate organisational set-up and its compliance with the applicable regulations, and monitors how well the overall system of internal controls functions.

However, the efficient prevention of risks cannot be left to the control functions only, but must first be carried out where the risk is generated, especially within the scope of the operational lines. The operational facilities are therefore the first to be responsible for the risk management process: during daily operations, these

facilities must identify, measure or assess, monitor, mitigate and report the risks arising from routine company activities in compliance with the risk management process.

In this context, financial advisors in the Sales Network are very important, along with the employees of the organisational units in charge of the administration and actual management of customer relations: these parties will be responsible for monitoring operations and reporting any suspicious transactions in accordance with the guidelines prepared by the Bank.

In order to ensure effective prevention of the risks of non-compliance with the regulations, it is essential that the different company facilities guarantee the timely involvement of the Anti-Money Laundering Function when new products and services are being offered, so that it can make its assessments before the fact.

1.1 APPLICABLE CONTEXT

The "*Provisions applicable to organisation, procedures and internal controls aimed at preventing the use of intermediaries for the purpose of money laundering and financing of terrorism"* issued by the Bank of Italy with a regulation dated 26 March 2019 (hereinafter also "**Provisions**") provide for the obligation, for the corporate bodies of each recipient, to define and approve a reasoned policy which must indicate the measures that the recipient has adopted in the area of organisational structures, procedures and internal controls, proper data auditing and storage.

In order to fully comply with the Provisions – issued by the Supervisory Authority pursuant to article 7 of Legislative Decree no. 231 of 21 November 2007, as amended by Legislative Decree no. 125 of 4 October 2019 (hereinafter also "**Anti-Money Laundering Decree**") – the Bank has adopted this policy (hereinafter also the "**Policy**") which takes into account the uniqueness of the different members of the Group and of the risks inherent in the carried out activities, consistent with the principle of proportionality and with the actual exposure to money-laundering risks.

The Policy takes also into account the specificities and complexities of the operations carried out by the Parent Company and the other companies of the Group, the products and services provided, the types of customers, the distribution channels used for the sale of products and services and the developments expected in these areas.

In particular, the strategy of the Bank currently aims at offering products and services on an off-premise basis to retail customers residing in Italy through a network of exclusive financial consultants trained in off-premise sales.

On a residual basis, there is the possibility of establishing banking relationships through an identification process carried out remotely or through a video-identification by resident customers, or at the Bank's main branch. The transactions of customers not associated with financial consultants are monitored, in all cases, by a special office of the Bank.

This policy forms part of a broader system of internal Bank controls aimed at ensuring compliance with prevailing law, and constitutes the base document in the entire anti-money laundering and anti-terrorism control system of the Banking Group.

In drafting this Policy, the Bank has taken into account also the outcomes of the annual process for the self-assessment of money laundering risk; future updates of the Policy shall, all together, also take into account the outcomes of the annual self-assessment, carried out each time.

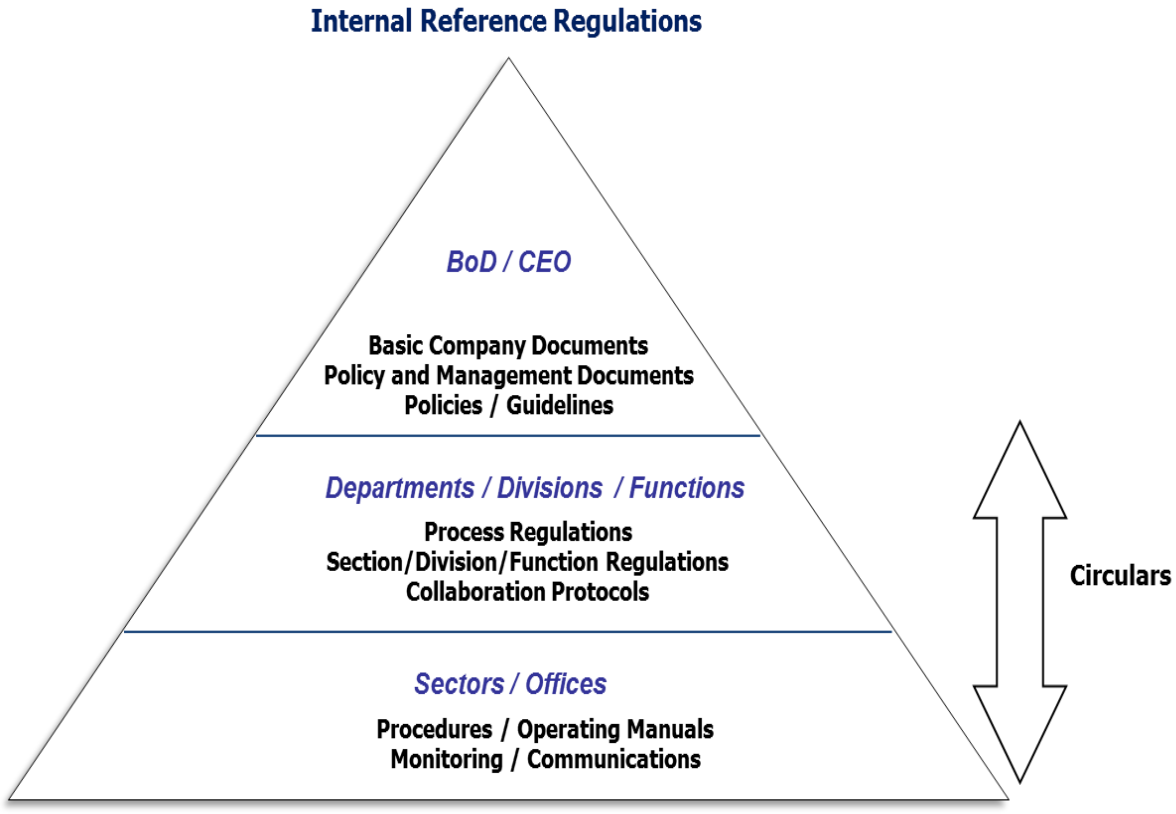
1.2 SCOPE OF THE DOCUMENT

The main goal of this Policy is to define:

- the measures to be actually adopted in terms of organisational structures, procedures and internal controls, proper data auditing and storage;
- the governance rules and roles and responsibilities for combatting the risks of money laundering and terrorist financing to be adopted by the Group;
- the Group guidelines for combatting the risks of money laundering and terrorist financing, as well as the principles for the management of relationships with the customers who are classified as high risk.

The principles stated in this Policy are reflected in the internal detailed documentation (e.g. process regulations, operating procedures, etc.) where the tasks and the operating and control activities are better described in compliance with the principles and regulations applicable to the monitoring of money-laundering and anti-terrorism risks. Please refer, in particular, to the process Regulations – prepared and updated by the Anti-Money Laundering Function – as regards Due Diligence, Reporting of Suspicious Transactions and second level Controls carried out by the Anti-Money Laundering Function which, overall, defines, in detail, the responsibilities, tasks and operational methods applied to the management of money-laundering risk and contained in the so-called “Anti-Money Laundering Manual”. This document is at the top level of the pyramid shown here below, which represents the logical model of corporate regulations.

Figure 1. Model of corporate regulations



1.3 DOCUMENT STRUCTURE

In addition to the first chapter containing the introduction, the applicable context and the scope of the document, this Policy comprises the following chapters, for which a brief description of the main issues covered is provided below:

- chapter 2: identifies the target audience of the document and defines the responsibilities for updating and revising it;
- chapter 3: gives a summary of the concepts of “money laundering” and “terrorist financing” and contains a glossary of the main terms used;
- chapter 4: describes the breakdown of roles and responsibilities to ensure the correct monitoring of the risks of money laundering and terrorist financing;
- chapter 5: illustrates the standards to adopt, at Group level, to combat the risks of money laundering and terrorist financing;
- chapter 6: describes the main applicable national, international and internal regulatory provisions.

2 APPLICABILITY

2.1 TARGET READERS

This document is approved by the Board of Directors of Banca Mediolanum S.p.A., Parent Company of the Mediolanum Banking Group and is aimed at all employees and associates of the Bank.

The policy is therefore sent for the approval, in accordance with the standard of proportionality, and taking account of local regulations and specific issues, to the Bodies in charge of the Strategic Supervision of the Companies forming part of the Banking Group on the basis of the following range of application:

- to all Italian companies subject to the provisions of the measures to use to combat money laundering and terrorist financing;
- to the banks and financial intermediaries who belong to the Banking Group with offices abroad, in accordance with and compatible with local regulations in effect.

This policy is also sent to the investee Mediolanum Vita S.p.A., Parent Company of the Mediolanum Insurance Group (hereinafter also "**Mediolanum Vita**") so it can take account of it when preparing its own policy, with a view to developing a global approach to the Money-Laundering Risk within the Mediolanum Conglomerate, in compliance with the specificities and reference regulatory provisions.

Incorporation of the guidelines and standards contained in this policy at the level of the Mediolanum Conglomerate is aimed at encouraging adequate coordination between the local anti-money laundering controls and the Anti-Money Laundering Function of the Bank, and ensuring the efficient circulation of information at Conglomerate level, in order to combat the risk of money laundering and terrorist financing.

The Bank, within the scope of its role of giving guidance and coordination, can authorise, if required by the specific operational characteristics, the individual Bank Group companies to partially apply them or incorporate them on a gradual basis.

2.2 RESPONSIBILITY FOR THE DOCUMENT

The Policy has been approved by the Board of Directors of the Bank which will also approve any amendment and/or update thereto.

The CEO defines the Policy that is subsequently submitted for approval to the Board of Directors, and ensures its implementation.

The Anti-Money Laundering Function participates in the update and periodical review of this Policy.

3 DEFINITIONS

3.1 DEFINITION OF "MONEY-LAUNDERING" AND "FINANCING OF TERRORISM"

The definition of "**money laundering**" adopted by the Anti-Money Laundering Decree consists of the following activities:

a) the conversion or the transfer of goods carried out with the knowledge that they come from a criminal activity or from a participation in this activity, in order to conceal or dissimulate the unlawful origin of said goods or to help anybody who is involved in said activity to avoid the legal consequences of said actions;
b) the concealment or dissimulation of the real nature, origin, location, placement, transfer, property of the goods or the rights held on them, carried out with the knowledge that these goods come from a criminal activity[1] or a participation therein;
c) the purchase, retention or use of goods with the knowledge, at the time of their receipt, that they originated from a criminal activity or a participation therein;
d) the participation in one of the actions under the previous paragraphs, the association to committing such actions, any attempt to commit them, the actual help, instigation or advice given to somebody in order to incite him/her to commit such action or to facilitate its execution.

Money-laundering is considered as such even if the actions that have generated the goods to be laundered were carried out abroad.

Money-laundering is normally a process consisting of three stages:

placement: any revenue from an offence, even if carried out with no malicious intent, through a number of transactions, is collected and placed with financial and/or non-financial institutions;

layering: it is carried out through the performance of a set of complex financial transactions, even if not apparently related to each other, aimed at hindering the reconstruction of the financial flows;

integration: any revenue obtained from criminal activities is re-used in the legal economy, making it appear as legally originated.

The three stages are not static and they can overlap: the use of the financial institutions for criminal purposes may occur in any of the afore-described steps.

"**Financing of terrorism**" means any activity aimed, with whatever means, at the provision, collection, funding, intermediation, deposit, maintenance or granting of funds and financial resources, however generated, for the purpose of being used, directly or indirectly, in full or in part, for the conduct of one or more acts of terrorism, according to the criminal laws, regardless of the actual use of the funds and financial resources for exhibiting the afore-mentioned conducts.

The Ministry of Economy and Finance, upon a proposal issued by the Financial Security Committee, stated, by issuing its own decree, the freezing of the funds and financial resources held, also through a natural or legal person, by natural or legal persons, groups or entities, designated, according to criteria and procedures set forth in the same resolutions, by the United Nations Security Council or one of its Committee.

Pending the adoption of the designation provisions set forth by the United Nations and in compliance with the obligations set out by the United Nations Security Council and with the specific restrictive measures set forth by the European Union as well as by the initiatives undertaken by the judicial authority within the scope of criminal proceedings, the Ministry of the Economy and Finance, upon proposal by the Financial Security Committee, has set forth, by issuing its own decree, for a period of six months, renewable in the same form as

long as conditions are met, the freezing of the funds and financial resources (so-called national freezing measures) held, also by a natural or legal third party, by natural or legal persons, groups or entities who display or try to display a conduct aimed at acts of terrorism, according to criminal laws, or aimed at the financing of programmes for the proliferation of weapons of mass destruction or that threaten the peace and national security.

These Funds and Financial Resources under a freezing order, may not be transferred, placed or used.

The **freezing** of "funds" and/or of "financial resources" (so-called financial embargo) is aimed at the presumed terrorists ("designated subjects", or "natural persons, legal persons, groups and entities designated as recipients of the freezing based on EU regulations and national laws") by requiring that the Financial Intermediaries inhibit any act related to the movement and/or transfer, as well as any act of placement, sale, leasing, rent, establishment of security interest or even to an access that would modify the volume, the amount, the placement, the ownership, the possession, the nature, the destination or any other change that would allow for the use of the funds, including the management of the portfolio.

The freezing or "financial embargo" differs from the so-called "economic embargo" related to the prohibition of trading with sanctioned countries, in order to isolate and place their governments in a difficult internal political and economic position.

3.2 GLOSSARY

Due diligence: activities involving:

- checking the identity of the customer, any representative or any beneficial owner on the basis of documents, data or information obtained from a reliable, independent source;
- acquiring information on the expected scope and nature of the business relationship, and when there is an occasional transaction in accordance with a risk-based approach;
- exercising constant control during the business relationship.

Executive: a member of the Board of Directors or the General Manager or another employee delegated, by the corporate body with management responsibilities or by the General Manager, with the maintenance of relationships with high risk customers; the executive has a thorough knowledge of the level of money laundering risk or terrorism financing risk to which the recipient is exposed and is sufficiently independent in terms of making decisions that may impact this risk level.

Single Computer Archive: an archive, created and managed by computer systems, where all the information acquired in fulfilling the identification and registration obligations is kept on a centralised basis, in accordance with the standards of Legislative Decree 231/07, and the implementing orders issued by the Bank of Italy.

Institutional activity: the activity by which the recipients have obtained a registration or an authorisation from a Public Authority.

Shell bank: a bank or entity that carries out functions that are similar to a bank but does not have a significant staff or management structure in the country where it was established and authorised to exercise its business, and is not part of a financial group subject to effective supervision on a consolidated basis.

Beneficiary of the insurance services:

1) a natural person or entity who is not a natural person who, on the basis of the designation made by the contracting party or the insured party, has the right to receive the insurance amount paid by the insurance company;

2) any natural person or entity who is not a natural person in favour of whom payment is made by order of the designated beneficiary.

Customer: the party who has a business relationship or carries out transactions with financial intermediaries or other parties who exercise financial activities and with other targets of the obligations pursuant to the Anti-Money Laundering Decree, normally also identified with other terms such as users, investors, insured parties, contracting parties, purchasers, assignees, etc.

Compliance Risk: specific requirement of a certain law that may involve direct or indirect harm for the Bank of a financial or reputational nature or a sanction if is not fulfilled.

Freezing of funds: the prohibition, in accordance with EU laws and national laws, of the movement, transfer, modification, use or management of funds or access to them, that could change the volume, amount, placement, ownership, possession, nature, destination or any other alteration that permits use of the funds, including portfolio management

Freezing of economic resources: the prohibition, due to EU laws and national laws, of the transfer, ordering, or, in order to obtain funds, goods or services in any way, use of economic resources, including but not limited to the sale, rental, hire or establishment of pledges.

Financial conglomerates: groups of companies, significantly active in the insurance, banking or investment services sectors, which include at least an insurance company and a company operating in the banking or investment services sectors, and are controlled by a regulated company or carry out activities primarily within the financial sector; for the purpose of this document, please refer to the Financial Conglomerate under the control of Banca Mediolanum S.p.A.

Correspondent accounts and similar accounts: accounts held by the banks to settle interbank services and other relationships of any nature, between credit entities and financial institutions, used to settle transactions on behalf of the customers of the corresponding entities.

Through accounts: cross-border correspondent bank accounts between banking and financial intermediaries, used to carry out transactions in their own names or on behalf of customers.

Line controls (known as "level one controls"): all the controls aimed at ensuring that the transactions are properly carried out. These are carried out by the same operating structures (e.g. hierarchical, systematic and sample controls), also through units that are exclusively responsible for performing control or monitoring tasks and that report to the managers of the operational structures, or are carried out as part of back office activities; as far as possible, they are incorporated into the IT procedures.

Controls on risks and compliance (also called "second-level controls"), all controls set up for the purpose of ensuring, *inter alia:*

- the correct implementation of the risk management process;
- compliance with the operating limits assigned to the various functions;
- compliance of the company's operations with all provisions of the law, including self-regulatory provisions.

The functions that are responsible for these controls are separate from the operational functions; they help define the risk governance policies and the risk management process.

Counterparty: natural persons and legal persons who initiate business relations (that are not long-term contractual relationships that are part of the exercise of the corporate activities of financial intermediaries or other parties who exercise financial activities) with the Bank or a Mediolanum Group Company (even if not subject to the obligations set out under Legislative Decree 231/07).

Cover Payment: the transfer of funds used when there is no direct relationship between the payment service provider (PSP) of the ordering party and the beneficiary, and a chain of correspondent accounts therefore have to be used through a PSP. Three or more payment service providers are involved in a cover payment.

Identification data of the customer, related actual beneficial owner and representative: the name and surname, place and date of birth, the registered residence and domicile if different from the registered residence, the details of the identifying document and, where assigned, the tax code of the customer, and where assignation is provided, also the related beneficial owner and representative. In the event of subjects other than the natural person, the name, the registered office, the enrolment number in the register of companies or in the register of legal persons, where required.

Identification data of the beneficiary, related actual beneficial owner and representative: name, surname, place and date of birth. In the event of subjects other than the natural person, the name, the registered office, the enrolment number in the register of companies or in the register of legal persons, where required. In both cases, at the time of the provision of the service, also the place of residence and, if different, the domicile, the details of the identification document, the tax code of the beneficiary and, if such assignment is required, also of the related beneficial owner and representative.

Cash: banknotes and metal coins, in euros and foreign currencies that are legal tender.

Employee: all Banca Mediolanum employees who belong to the organisational units and/or the local and/or central structures.

Representative: the party who is authorised to act in the name and on behalf of the customer (or the beneficiary of the insurance service) or who was given the powers of representation that allow it to operate in the name of and on behalf of the customer (or of the beneficiary of the insurance service)[1]..

[1] The subjects entrusted by a public authority with the management of the assets of and the relationships with the customer or with its representation (such as, for instance, the insolvency practitioners) are considered representatives.

Family Banker®: the financial consultants of Banca Mediolanum in charge of an off-premises offer, according to article 31, paragraphs 1 and 2, Legislative Decree no. 58 of 24 February 1998 (Consolidated Finance Act).

Funds: the activities and financial benefits of any nature, also held through third parties who can be natural persons or legal persons, including but not limited to:

- cash, cheques, monetary claims, bills, transfers and other payment instruments;
- deposits with financial entities or other parties, settlements of accounts, receivables and bonds of any nature;
- public or private negotiable instruments and financial instruments as defined in article 1, paragraph 2 of the consolidated act on financial intermediation, pursuant to legislative decree no 58 of 24 February 1998;
- interest, dividends or other income and value added as a result of the activities;
- credit, right to offset, guarantees of any nature, security deposits and other financial commitments;
- letters of credit, bills of lading and other documents of title;
- document showing investments in funds or financial resources;
- all other export finance instruments;
- insurance policies relating to the life businesses pursuant to article 2, paragraph 1, of legislative decree of 7 September 2005, no. 209, containing the private insurance code.

Anti-Money Laundering Function: function which is an integral part of the level two internal control system, in charge of preventing and combatting the execution of money laundering or terrorist financing.

Company Control Functions: the Compliance Function, the Risk Management Function, the Internal Auditing Function and the Anti-Money Laundering Function.

Compliance Function: this function is responsible for overseeing, taking a risk-based approach, the management of compliance risks, at every level of the Company, and ensuring that all procedures are suitable to prevent said risks, entailing breaches of the external laws and regulations and self-regulatory rules such as codes of conduct and codes of ethics applicable to the bank. This function is an integral part of the internal control system.

Internal Audit Function: the function entrusted with the monitoring, within the scope of third level controls, also with on-site audits, of the regular performance of operations and development of risks, and with assessing the completeness, adequacy, functionality and reliability of the organisational structure and of other components of the Internal Control System, while bringing to the attention of the corporate bodies any possible improvements, with particular reference to the Risk Appetite Framework (RAF), to the risk management process and to the measurement tools and their controls. Based on the results of its controls, it puts forward recommendations to the corporate bodies.

Group: The Mediolanum Banking Group, as governed by article 60 of the Consolidated Finance Act and all applicable provisions.

Insurance intermediaries: natural persons or companies with residence or registered office in Italy – enrolled in the single insurance intermediary electronic registry in compliance with article 109, paragraph 2, letters a),

b) and d) of the Code – as well as natural persons or companies with residence or registered office in another Member state of the European Union or in another country belonging to the European Economic Area or in a third country, which operate in Italy under the right of establishment and are included in the list that was annexed to the register pursuant to a notice under articles 116-quater and 116-quinquies of the Code – limited to the distribution, within the Italian Republic territory, of insurance products within the business classes listed in article 2, paragraph 1, of the Code.

Means of payment: cash, bank cheques and postal cheques, banker's drafts and other similar or equivalent cheques, postal money orders, credit or payment orders, credit cards and other payment cards, transferable insurance policies, lien policies or other instruments available that allow for the transfer, movement or purchase, including via telecommunication, of funds, securities or financial resources.

Transaction: the movement, transfer or transmission of means of payment or negotiations involving property; a transaction is also the stipulation of a negotiation involving property, constituting the exercise of a professional or commercial activity.

Related transactions: transactions that are related to each other to pursue a single legal-property related goal.

Split Transaction: a single transaction, from an economic viewpoint, of an amount equal to or higher than the limits established by the Anti-Money Laundering Decree, put in place through a number of transactions, individually lower than the above-mentioned limits, carried out at different times and over a certain period of time set as seven days, without prejudice to the existence of the split transaction when the elements to consider it so are present.

Occasional Transaction: a transaction that is not related to a business relationship in place; an occasional transaction also comprises an intellectual or commercial service, including those that can be carried out on an instantaneous basis, given in favour of the customer.

Suspicious Transaction: an operation which, because of its characteristics, scope, nature and connection with other operations or because of its fragmentation or any other known circumstance as regards the functions carried out, taking also into account the financial standing and the activities performed by the subject to which it refers, and based on the elements acquired pursuant to the Anti-Money Laundering Decree, leads to believe, suspect, or have reasons to suspect that some money-laundering or financing of terrorism operations are being or have been carried out or there was an attempt to carry them out or that, in anyway, regardless of their scope, originate from criminal activities.

Company bodies: all the bodies with strategic supervision functions (Board of Directors), management (CEO or other management Body) and control (Board of Statutory Auditors).

EU countries: countries belonging to the European Economic Area.

Third countries: Countries not belonging to the European Economic Area.

High risk third countries: countries not belonging to the European Union, the regulatory systems of which show some strategic shortcomings in the respective national statutory schemes for the prevention of money

laundering and financing of terrorism, as identified by the European Commission in the exercise of powers governed by articles 9 and 64 of the IVth Anti-Money Laundering Directive.

Personnel: the employees and those who operate based on relationships that determine their joining the organisation, also in a form other than an employment relationship, including the financial consultants trained in off-premise sales, under article 31, paragraph 2, of the Consolidated Financial Act, as well as the direct manufacturers and the subjects entrusted with intermediation, under article 109, paragraph 2, letters c) and e), CAP.

PEP: the natural persons indicated in article 1, paragraph 2, letter dd) of the Anti-Money Laundering Decree, or the *"natural persons who hold or have ceased to hold, for less than one year, important public positions, as well as their family members and those who have a close relationship with these subjects, as hereinafter described:*

1) *natural persons who hold or held important public offices are those who hold or held the office of:*

1.1 President of the Republic, Prime Minister, Minister, Deputy Minister and Undersecretary, President of the Region, Regional Councillor, Mayor of the Provincial capital or metropolitan city, Mayor of a Municipality with a population of not less than 15,000 inhabitants, or similar offices in foreign countries;

1.2 deputy, senator, European parliament member, regional councillor or similar offices in foreign countries;

1.3 members of central governing bodies of political parties;

1.4 judges of the Constitutional Court, judge of the Court of Cassation or the Court of Auditors, councillor of State or other members of the Council of Administrative Justice for the Sicily Region or similar offices in foreign countries;

1.5 member of the governing bodies of central banks or independent authorities;

1.6 ambassador, chargé d'affaires or equivalent offices in foreign countries, top official in the armed forces or similar offices in foreign countries;

1.7 member of the board of directors, management or control of companies controlled, including indirectly, by the Italian State or by a foreign country or with investments, to a substantial or total extent, by the Regions, main Provincial municipalities or metropolitan cities or municipalities with a population of not less than 15,000 inhabitants;

1.8 general director of ASL or hospitals, university hospitals or other national healthcare service entities.

1.9 manager, deputy manager or member of the governing body or party carrying out equivalent functions in international organisations;

2) the following are family-members of politically exposed persons: parents, spouse or the person in a civil partnership or de facto co-habitant or similar situations of the politically exposed person, the children and their spouses or persons in civil partnerships or de facto co-habitants or similar situations with the children;

3) the following are persons with whom the politically exposed persons are known to have close ties:

3.1 natural persons who, pursuant to the Anti-Money Laundering Decree hold, jointly with the politically exposed person, the actual ownership of legal entities, trusts and relevant legal arrangements or maintain with the politically exposed person close business relationships;

3.2 natural persons who only formally hold total control of an entity which is known to have been established, on a de facto basis, for the interest and benefit of a politically exposed person.

Anti-money laundering Policy or the Policy: the document defined by the body with management functions and approved by the body with strategic supervisory functions, pursuant to the Provisions in the area of organisation, procedures and internal controls aimed at preventing the use of intermediaries for the purpose of money-laundering and financing of terrorism, adopted by the Bank of Italy on 26 March 2019 (see Part One, Sections II and III).

PSP: Payment Service Provider

Providers of digital portfolio services: any natural or legal person who provides to third parties, on a professional basis, also on-line, services for the safeguarding of private cryptographic keys on behalf of its customers, in order to hold, store and transfer virtual currencies.

Providers of services related to the use of virtual currency: each natural or legal person who provides to third parties, as a professional activity, also online, services related to the use, exchange, savings of virtual currencies and their conversion from or into legal tender currencies or in digital representations of a value, including those convertible into other virtual currencies as well as issuing, offer, transfer and clearance and any other service that is functional to the acquisition, negotiation or intermediation in the exchange of said currencies.

Service providers for companies and trusts: each natural person or legal person who provides, on a professional basis, one of the following services to third parties:

- establishes companies or other legal persons;
- acts as a manager or director of a company, a partner in an association or a similar position with respect to other legal persons or arranges for another person to take over the position;
- provides a registered office, business, administrative or postal address and other services related to a company, association or any other legal arrangement;
- acts as trustee in an express trust or similar legal party or related legal arrangement or ensures that another person occupies that position;
- exercises the role of shareholder on behalf of another person or arranges for another person to do so provided that it is not a listed company on a regulated market and subject to communication obligations in accordance with EU laws or equivalent international regulations.

Business relationship: a long-term relationship that falls within the exercise of the company activities carried out by obliged parties, which is not completed in a single transaction.

Money-laundering risk: the risk arising from the breaching of legal, regulatory and self-regulatory provisions, functional to the prevention of the use of the financial system for money laundering purposes, terrorism financing or financing of programmes for the development of weapons of mass destruction, as well as the risk

for involvement in money laundering and financing of terrorism episodes or financing of programmes for the development of weapons of mass destruction.

Economic resources: tangible or intangible assets of any nature and security or property assets, including accessories, appurtenances and results that are not funds but could be used to obtain funds, goods or services, owned, held or controlled, including partially, directly or indirectly, or through third natural or legal parties, by designated parties or natural persons or legal persons who are acting on behalf or under the guidance of the latter.

Internal Control System: the set of policies, functions, facilities, resources, processes and procedures that aim to ensure the following ends in accordance with the principles of sound and prudent management:

- assessment of implementation of the corporate strategies and policies;
- containment of the risk within the limits set out in the reference framework for determining the risk appetite of the bank (Risk Appetite Framework - "RAF");
- protection of the value of assets and protection against losses;
- efficacy and efficiency of the corporate processes;
- reliability and security of corporate information and IT procedures;
- prevention of the risk that the bank may be involved, even unintentionally, in illegal activities (especially those related to money laundering, usury and terrorist financing);
- compliance of all operations with the law and supervisory provisions, as well as with internal policies, regulations and procedures.

Operating structures: all remaining organisational units as set out in the company rules, which are not the company bodies or control functions.

Beneficial owner:

a) the natural or legal persons on behalf of which the customer establishes a business relationship or performs a transaction (in short, "sub-beneficial owner 1");
b) if the customer or the subject on behalf of which the customer establishes a business relationship or carries out a transaction, is not a natural person, or the natural or legal persons to which, ultimately, the direct or indirect ownership of the entity or the related control thereon is attributed or of which they are the beneficiaries (in short, "sub-beneficial owner 2"). In particular, if the company or other private legal persons, even if with registered office abroad, and expressed trusts, regardless of the related establishment place and of the law applicable thereto, the sub-beneficial owner 2 is identified according to the criteria set forth in articles 20 and 22, paragraph 5, of the anti-money laundering decree; the same compatible criteria apply in the case of partnerships and other legal, public and private subjects, even if with no legal personality.

Virtual currency: the digital representation of value, not issued nor guaranteed by a central bank or a public authority, not necessarily related to a currency of legal tender, used as a medium of exchange for the purchase of goods and services or for purposes of investment and transfer, electronically archived and negotiated.

4 ANTI-MONEY LAUNDERING MODEL GOVERNANCE

This model to combat money laundering and terrorist financing is managed, at Group level, through a specific process aimed at implementing and ensuring the maintenance of rules, procedures and organisational structures that can ensure the prevention and management of the risks in question, by all Group companies.

The model provides that the primary responsibility in terms of monitoring the risks of money laundering and terrorist financing is assigned to the Governing Bodies of each company of the Group, according to their respective duties, and in compliance with the directives of the Parent Company. The distribution of tasks and responsibilities in the area of compliance by the corporate bodies and functions must be clearly defined in each company.

In line with the authorised corporate governance standards, the model acknowledges for each Company of the Group, the centrality of the Board of Directors with respect to the risk governance policies in question: it is responsible for the approval of the anti-money laundering policy as provided for in the Provisions (in line with the principles of this Policy, and the responsibility for the adoption of a system that is suitable to the characteristics of the company; to this end, it is organised so as to be able to address the issue of the risks of money laundering and terrorist financing as carefully as possible and with the necessary level of detail.

The management Body is responsible for ensuring the implementation of the strategic guidelines and governance policies applied to the risk of money-laundering, approved by the Body with strategic supervisory authority, and is responsible for the adoption of all the measures necessary to ensure the efficacy of the organisation and of the anti-money laundering controls.

The control Body, within the scope of its responsibility to oversee the completeness, suitability, functionality and reliability of the internal control system, is also constantly in touch with the Anti-Money Laundering Function.

In compliance with the proportionality principle and if provided for in the specific reference regulations, each company of the Group must set up a specific Anti-Money Laundering Function aimed at preventing and combatting the execution of money-laundering activities.

In order to implement appropriate synergies and economies of scale, using highly specialised centres of expertise, the companies of the Banking Group and those of the Insurance Group may delegate to the Parent Company – based on specific outsourcing agreements, drawn up in compliance with the supervisory regulations, and in compliance with the principles set forth in the “Corporate policy on outsourcing” – activities specific to the anti-money laundering function pursuant to the applicable laws and/or the fulfilment of specific obligations as set forth in the same regulations.

Those agreements must also govern the following aspects:

- the objectives of the function and the content of the outsourced activities;
- the expected service levels;
- the minimum frequency of information flows;
- confidentiality obligations about the information acquired in carrying out the function or the activities;

- the possibility of reviewing the service terms in the case of changes in the operations and organisation of the Company.

The companies of the Group appoint their own manager entrusted with the anti-money laundering function, and their own delegated person responsible for the reporting of suspicious transactions, in line with the principles established in this Policy (as defined below).

The subsidiary Mediolanum Vita – parent company of the insurance group – sets up its own Anti-Money Laundering Function, and appoints a Manager of this Function and a Delegate responsible for reporting any suspicious transactions. Mediolanum Vita approves its own policy that defines the actual measures adopted in terms of organisational structures, procedures and internal controls, proper data auditing and storage, in line with the principles contained in this Policy and consistent with the regulatory provisions specific of the sector to which it belongs.

From a Group perspective, the good organisation of the work and the circulation of information assume crucial importance so that any intra-company issues related to the provisions on anti-money laundering and combatting terrorist financing are discussed with the support of appropriate preparatory work, the outcome of which will also be submitted to the Risk Committee of the Parent Company.

Within the scope of the group guidance and coordination activities, the corporate bodies of the Bank (in the capacity of Parent Company) adopt the approved strategic guidance in the area of money laundering risk and anti-money laundering controls. The Parent Company ensures that the corporate bodies and the other companies belonging to the Group implement, in their own corporate environment, the strategies and policies of the Group.

In order to pursue a full and concrete implementation of the Group model, the consolidated subsidiaries adopt a policy consistent with the principles and the guidelines described in this Policy, according to a principle of proportionality and based on the specific character of their activities.

Pursuant to the applicable Provisions, in order to increase the homogeneity of the assessments carried out on the customers, shared by the members of a group, and to increase the capacities of the same to prevent and manage money-laundering risks, the Parent Company is required to establish – through the creation of a centralised register – a shared information base that allows all the companies belonging to a group to consistently evaluate the customers.

In implementing the above provisions, based on the principle of a risk-based approach, the Bank establishes a shared information base used by all the companies controlled (directly or indirectly) by the Bank itself where information concerning a customer with a high money laundering risk is shared, maintained and properly updated (e.g. a customer subject to a prior reporting to FIU).

The Anti-Money Laundering Function identifies additional types of information that may be shared where there are relationships based on placement/distribution activities (or other relevant business relationships) between the Parent Company and the individual subsidiaries (or among the latter).

The Parent Company adopts appropriate technical and organisational measures in order to guarantee that the data contained in the shared information database is handled in compliance with the applicable national laws on personal data protection.

The Anti-Money Laundering Functions of the subsidiaries activate appropriate periodical information flows toward the parent company regarding the main performed activities, the outcomes of the carried out controls and the main initiatives undertaken in order to eliminate any identified dysfunction.

The Manager of the Anti-Money Laundering Function of the Bank is in all cases promptly informed on the results of the control activities carried out at the companies belonging to the financial conglomerate, as well as on any relevant event.

4.1 PARENT COMPANY BANCA MEDIOLANUM S.P.A.[2]

In line with the Provisions, the duties and responsibilities for reducing the risk of involvement by the Bank in money laundering or terrorist financing will first be referred to the Corporate Bodies.

More specifically, the Board of Directors will have to identify governance policies for said risks that are adequate with respect to the extent and type of risk profiles that the Bank and the Group activities are actually exposed to. In this perspective, it will carry out its functions with reference to both the Bank and also assessing the overall operations of the Group and the risks that it is exposed to. The CEO will prepare the procedures needed to implement said policies; the Anti-Money Laundering Function will continuously check the suitability of the procedures to ensure adequate monitoring of said risks, coordinating with the other corporate control functions. The Internal Audit Function continuously monitors the level of adequacy of the corporate organisational set-up and its compliance with the applicable regulations, and monitors how well the overall system of internal controls functions.

The efficient prevention of risks cannot, in any case, be left to the control functions only, but must be carried out firstly where the risk is generated, especially within the scope of the operating lines, which is the main responsibility of the risk management process.

The model to combat money laundering and terrorist financing therefore provides for involvement by the organisational units of each Group company in accordance with the organisation of the roles and responsibilities reported below.

Board of Directors

The Board of Directors:

- approves and reviews periodically the strategic guidelines and the governance policies on risks related to money-laundering and financing of terrorism;

[2]The main attributes on compliance with the regulations governing anti-money laundering and anti-terrorism are listed below. Please refer to the internal rules on corporate governance for a full analysis of the duties.

- approves this Policy and is responsible for the periodical review thereof, in order to ensure its efficacy over time;
- approves the establishment of the Anti-Money Laundering Function, identifying tasks and responsibilities as well as the methods to be used for the coordination and collaboration with the other Corporate Control Functions;
- approves the guidelines of an organic and coordinated internal control system, essential for the prompt identification and management of money-laundering and financing of terrorism risks and ensures their periodic review in order to guarantee their efficacy over time;
- approves the principles for the management of relationships with the customers classified as “high risk”;
- ensures over time that the tasks and responsibilities in the areas of anti-money laundering and combatting the financing of terrorism are allocated in a clear and appropriate manner, thus guaranteeing that the operating and the control functions are maintained separate and that the functions themselves are provided with adequate qualitative and quantitative resources;
- ensures that an adequate, complete and prompt information flow system, toward the corporate bodies and among the control functions, is effectively set up;
- ensures that the gaps and anomalies identified during the controls at various levels, are promptly brought to its attention, and promotes the adoption of appropriate corrective measures of which it assesses the efficacy;
- ensures the preservation of confidentiality within the process adopted for reporting suspicious transactions;
- reviews, at least on an annual basis, the report issued by the Manager of the Anti-Money Laundering Function on the audit activities carried out, on the undertaken initiatives, the identified dysfunctions and related corrective actions to be performed, as well as on activities for the training of personnel and the members of the sales network, and finally on the communications provided by the Board of Statutory Auditors and/or by the Supervisory Body; if these communications refer to breaches that are considered as relevant, all related information is provided at the next meeting of the Anti-Money Laundering Function;
- reviews, at least on an annual basis, the document applicable to the results of the self-assessment, regarding money-laundering risks, carried out by the Anti-Money Laundering Function;
- assesses the risks related to operations carried out with third countries associated with higher risks for money laundering, and identifies the controls for attenuating them, monitoring their efficacy;
- upon consulting with the Board of Statutory Auditors, appoints and revokes the Manager of the Anti-Money Laundering Function and the Delegate responsible for Reporting of Suspicious Transactions;
- defines and approves the criteria for coordinating and managing the companies of the Group, and for determining the criteria for the execution of instructions issued by the Bank of Italy.

Risk Committee

The Risk Committee provides support to the Board of Directors regarding risks and internal controls system. With specific reference to protecting against the risk of money laundering and terrorist financing:

- assists, by expressing its opinion, the Board of Directors at least on an annual basis, on the compliance, suitability and actual functioning of the Internal Control System, the corporate organisation and the requirements that must be met by the Corporate Control Functions, and ensures that they are properly compliant with the directives and guidelines issued by the Board of Directors;
- brings any significant weaknesses to the attention of the Board of Directors, recommending appropriate remedial measures and ensuring that the principal risks faced by the company are identified and measured correctly and managed and monitored adequately. In particular, it expresses an opinion regarding the qualitative and quantitative adequacy of the Anti-Money Laundering Function, and whether it is independent enough;
- assists the Board of Directors in determining corporate "guidelines" and "policies" regarding risks and internal controls system, also consistent with the chosen risk appetite. In particular, it formulates proposals regarding:
    - the methods of exercise of strategic control, management and technical-operational activities with respect to individual companies and the Group;
    - the control structure of the Group, with particular reference to the centralisation choices of specific control functions in accordance with Supervisory regulations;
    - the organisational model to support control functions, the guidelines on respective activities necessary for the determination of the relevant regulations, the coordination of the various functions;
- makes a prior examination of the plan of activities and annual report of the Anti-Money Laundering Function, and periodic reports relating to the evaluation of the internal control and risk management system, including the results of the Self-evaluation of the risks of money laundering and terrorist financing carried out by the Anti-Money Laundering Function, and those of particular importance prepared by the Internal Audit Function or by the Board of Statutory Auditors. If necessary, it can request the Internal Audit Function to carry out checks on specific operational areas, giving immediate notice to the Board of Directors and the Board of Statutory Auditors.

Board of Statutory Auditors

With specific reference to protecting against the risk of money laundering and terrorist financing, the Board of Statutory Auditors:

- monitors compliance with the regulations and the completeness, efficiency and adequacy of the anti-money laundering controls, using the internal facilities to make the checks and assessments necessary, and using the information from the other Company bodies, the Anti-Money Laundering Function Manager and the other corporate control functions. In this context:
    - it carefully assesses the suitability of the procedures in place to carry out customers' due diligence, record and keep the information and report on the suspicious transactions;
    - stimulates the in-depth investigation of the reasons behind any shortcomings, anomalies or wrongdoing found and encourages the adoption of suitable corrective measures;
- expresses on opinion on the appointment and revocation of the appointment of the Anti-Money Laundering Function Manager;

- its opinion is sought on the definition of the elements of the overall architecture of the management and control system for the risk of money laundering and terrorist financing;
- monitors, in accordance with article 46 of Legislative Decree 231/2007, compliance with the regulations in the decree within the scope of its characteristics and duties;
- promptly communicates to the Bank of Italy all the facts brought to its attention while exercising its function that may involve serious breaches or repeated or systematic or multiple violations of the applicable laws and related implementation provisions; sends, to the Delegate responsible for reporting suspicious transactions, any reports of transactions found on an independent basis in the exercise of its duties.

Supervisory Board

The Supervisory Board contributes, before the fact, to the definition of the Organisation, Management and Control Model pursuant to Legislative Decree no. 231/2001, and continuously monitors compliance with the processes provided for therein. In any case, if a predicate offence is committed, it will analyse the causes to identify the more suitable corrective measures. In order to carry out said activities, the Supervisory Board will receive suitable information flows from the various company functions and may access, without limitation, all the relevant information in order to fulfil its obligations.

The Supervisory Board will also send the Party Authorised to report suspicious transactions any reports of suspicious transactions found on an independent basis in the exercise of its duties.

Chief Executive Officer

The Chief Executive Officer will:

- ensures the implementation of the strategic guidelines and governing policies on money-laundering risks, approved by the Board of Directors, and is responsible for the adoption of all interventions necessary to ensure the efficacy of the organisation and the anti-money laundering control system;
- takes into account, in setting up operating procedures, the recommendations and guidelines issued by the competent authorities and the international bodies;
- defines and ensures the implementation of an internal control system that is essential for the prompt identification and management of money-laundering risk and oversees its continued efficacy over time, in compliance with the results obtained from the self-assessment of the risk process;
- ensures that the operating procedures and the information systems allow for the correct fulfilment of the obligations for a customers' due diligence and for the retention of documents and information;
- as regards the reporting of suspicious transactions, defines and ensures the implementation of a procedure suitable to the specific nature of the activity at issue, the size and complexity of the Bank, according to a proportionality principles and to the risk-based approach; this procedure is capable of guaranteeing a reference certainty, homogeneity in the behaviours, with a generalised application to the entire structure, full use of relevant information and ability to reconstruct the assessment process;

- in reference with the same issue, adopts measures aimed at ensuring compliance with the requirements of confidentiality applied to the reporting procedure as well as the use of tools, including electronic ones, for the identification of abnormal operations;
- defines and ensures the implementation of initiatives and procedures necessary to guarantee the prompt fulfilment of reporting obligations toward the competent Authorities, as set forth in the anti-money laundering laws;
- defines this Policy and ensures its implementation;
- defines and ensures the implementation of information procedures aimed at guaranteeing the knowledge of risk factors applicable to all the involved corporate structures and bodies entrusted with control functions;
- defines and ensures the implementation of the procedures for the management of relationships with customers that are classified as “high risk”, in compliance with the principles set forth by the Board of Directors;
- sets forth training and instruction programmes for the personnel regarding the obligations set forth in the applicable anti-money laundering laws; training activities are provided on an on-going and systematic basis and take into account any developments in the regulations and procedures set up by the Bank;
- defines the tools to be used for assessing the activities performed by the personnel so as to ensure the identification of any anomaly that may emerge in their behaviour, in the quality of the communications sent to the authorised subjects and corporate bodies as well as in the relationships maintained by the personnel with the customers;
- ensures, in the cases of remote operations (e.g. through the use of digital channels) the adoption of specific electronic procedures for guaranteeing compliance with anti-money laundering regulations, in particular as regards the automatic identification of abnormal operations.

General Manager

The General Manager is at the top of the internal structure and as such participates in the management department to whom he/she reports. In particular, the General Manager, also with respect to combatting money laundering and the terrorist financing:

- supervises the routine management of the Bank under the directives set by the CEO, guaranteeing that it functions in compliance with prevailing laws and regulations;
- supports the CEO in definition of the responsibilities of the company facilities and functions involved in the various company processes so that the relative duties are clearly assigned and any potential conflicts of interest are prevented; this person will also ensure that the relative activities are managed by qualified staff, with an adequate level of independence of assessment and who have the experience and awareness to match the duties to be carried out;
- issues, including through the applicable company functions, internal orders in accordance with the rules system defined by the Board of Directors.

Service, Operations and ICT Management

The Service, Operations and ICT Management is responsible for the management of processes applied to the Bank operations, provided through the Customer Banking Center, Product Operations, Sales Support Center and ICT Divisions.

It oversees and maintains the IT systems of the Bank and the companies to which the services shall be provided. It maintains relationships with the outsourcers, oversees and monitors their activities while evaluating the provided services and their levels.

Manages the direct contacts of existing and prospective customers with the Bank, for IT and devices purposes, through the services available on different channels: telephone (Banking Center, Automatic Digital Receptionist, SMS, Mobile Banking) and the Internet network (mail, chat, internet banking).

Management also provides a telephone and written support service to the Sales Network (Sales Support Center) in order to ensure a fast response to Customers' claims, through its financial consultants.

Through the Product Operations Division, Management is responsible for the reception and the archiving of incoming documents, the customers' master data, the execution, management and termination of business contracts for all products placed by the Bank which operates in support of the "specialised" organisational units of the Bank and of the Product Factories, in compliance with the distribution assignments.

Applies the contractual and financial conditions, both in terms of income and expense, concerning the services and products of the Bank and the Group, in compliance with the methods and the limits set forth by the Board of Directors and communicated by the CEO and the General Manager.

Within the Service, Operations and ICT Management, the management support organisational unit, called "Service Policy and Procedures":

- is responsible for the definition and the maintenance of the policies, the internal documentation and the control of the bank processes, including the processes related to credit and debit cards, while operating in close cooperation with the Product Operations Division;
- oversees the credit cards fraud monitoring service, assessing the implementation of new rules and/or updating the alert rules;
- performs an on-going monitoring on the operations carried out by Customers not assigned to a financial consultant, for the purposes of carrying out a first level control in the area of anti-money laundering;
- oversees, also for the purpose of an enhanced due diligence process, business relations, professional services and operations involving high risk third countries;
- draws up the results of preliminary checks carried out on Trusts, Fiduciaries, Foundations and companies characterised by complex corporate chains, for the identification of the beneficial owner for the purpose of opening business relationships or in support of the Corporate and Special Account Office, in the event of a change in the corporate structure, subsequently to the opening of the business relationship;
- carries out preliminary checks for the purpose of an enhanced due diligence process applied to existing or prospective customers who fall under the definition of Politically Exposed Persons which

require the establishment of a business relationship, a professional service or the carrying out of an occasional transaction;

- performs the preparatory check, for the purpose of an enhanced due diligence process, for the maintenance of relationships with the Customers who acquire the qualification of Politically Exposed Persons during the course of a business relationship that was previously established;
- provides support to the subjects holding administrative or management powers, or to their delegates, in order to assess and subsequently decide on the authorisation of the establishment, maintenance and/or termination of the relationship/s, professional services and/or carrying out of an occasional transaction with existing/prospective customers, qualified as Politically Exposed Persons.

The Head of the Service, Operations & ICT Management authorises the start, continuation and maintenance of a business relationship or the carrying out of an occasional transaction with Politically Exposed Persons.

In the event of an absence or impediment of the Head of the Service Operations & ICT Management , the Manager of the Product Operations Division is granted the power of authorising the start, continuation or maintenance of a business relationship or the carrying out of an occasional transaction with Politically Exposed Persons The actual exercise of this delegation of power confirms in itself the absence or impediment of the main delegated person and exempts third parties from any assessment or responsibility in this regard.

Internal Auditing Function

The Internal Auditing Function continuously monitors, in accordance with a risk-based approach, the level of adequacy of the corporate organisational set-up and its compliance with the applicable regulations, and monitors how well the overall system of internal controls functions.

With specific reference to the provisions on the prevention and combatting the use of the financial system for money laundering or terrorist financing, the Internal Auditing Function will check to ensure:

- continuous compliance with the due diligence obligations, both when initiating the relationship and as it develops over time;
- the actual acquisition and ordered storage of the data and documents required by law;
- the correct functioning of the Single Computer Archive and alignment between the various management accounting procedures and the procedure for entering data and managing the Archive;
- the actual degree of involvement of the employees and associates and the people in charge of the central and decentralised facilities in fulfilling the “active collaboration” obligation;

With a specific reference to the Sales Network, the Internal Audit Function consistently monitors compliance, by said network, with the rules of conduct, including those applicable to money-laundering and financing of terrorism, as set forth in the agreements and in all related provisions and guidelines, contained in the corporate governance.

Carries out control activities on the operations performed by the Sales Network, including in loco checks and assessments carried out at the premises of the Sales Network collaborators and at the administrative offices of the financial consultants. Carries out investigative activities and submits to the Sales Network Disciplinary Committee recommendations on the actions to be undertaken against the Sales Network collaborators who

have not been compliant with legal and regulatory provisions, as well with the procedures and rules of conduct set up internally.

The Internal Auditing Function is responsible for the whistleblowing process, where the Bank has identified the Whistleblowing Manager (hereinafter "Whistleblowing Manager or "WB Manager"), appointed in person by the Board of Directors.

The Function carries out follow-ups to ensure that the corrective actions have been adopted for any shortcomings or wrongdoing found and their suitability to avoid similar situations in the future.

The Function informs the Corporate Bodies about the activities carried out and relative outcomes, subject to compliance with the principle of confidentiality with respect to reporting suspicious transactions.

Compliance Function

The Compliance Function supervises management of the risks of non-compliance with the rules according to a risk-based approach with regard to all company activities, except for the regulatory areas referred to the other Control Functions pursuant to the law. Specialised units specifically singled out in the Group Compliance Policy are used to monitor certain regulatory areas, for which forms of specialised monitoring are required, and they are assigned certain compliance process phases.

Anti-Money Laundering Function

According to a risk-based approach, the Anti-Money Laundering Function is responsible for monitoring the risk of money laundering and terrorist financing and for adjusting the processes in accordance with developments in the applicable regulatory and procedural environment.

It checks that the company procedures are consistent with the objective of preventing and fighting infringement of external regulations (regulatory laws and rules) and of self-regulation on the subject of money laundering and terrorist financing.

It pays particular attention to the adequacy of the internal systems and procedures on the subject of adequate checking of the customers and recording, as well as of the systems for observing, assessing and reporting suspicious transactions.

The Anti-Money Laundering Function:

- is a specialised second level control function and falls under the category of the Company Control Functions;
- is independent from the operational facilities and its resources are capable of carrying out their duties from a qualitative and quantitative standpoint, including the economic duties, which can be initiated if necessary on an independent basis;
- there must be enough employees with the necessary updated technical-professional skills, including through the provision of ongoing training programmes;
- reports directly to top management bodies;
- has access to all the company activities, including any relevant information for it to carry out its duties.

With a specific reference to the activities concerning customers' due diligence, in order to guarantee, at the same time, the efficacy and effectiveness of the processes, the direct involvement of the Anti-Money Laundering Function is required on a risk-based approach, taking into account any objective, environmental or subjective circumstances which significantly elevate the money-laundering risk.

For the purpose of implementing the above provisions, the organisational and operational model defined by the Bank provides that the Anti-Money Laundering Function fulfils its customer due diligence requirements – with the support of the Personnel responsible for the management of relationships with customers, according to the provisions stated in the following paragraph **Errore. L'origine riferimento non è stata trovata.** of this Policy – in those cases considered as high risk, as identified in the same paragraph **Errore. L'origine riferimento non è stata trovata.**. Within the scope of the Anti-Money Laundering Function, some appropriate escalation mechanisms are also defined in those cases where the money-laundering risk is particularly high.

In cases other than those described above, the Anti-Money Laundering Function verifies – with methods set up by said Function – the efficacy of a customer due diligence process carried out by the financial consultants or other subjects responsible for the management of the relationship and related outcomes, identifying – where necessary – any control and/or support activities to be attributed to the internal structures of the Bank, other than those carried out by the anti-money laundering function.

More specifically, the Anti-Money Laundering Function:

- identifies the applicable regulations in terms of monitoring the risk of money laundering and combatting terrorism financing and evaluates their impact on the internal processes and procedures;
- provides advisory and support activities to the Corporate Bodies, senior management and the organisational units of the Bank, regarding issues under its competence, especially in the case of a supply of new products and services, with a particular attention placed on the identification and assessment of risks associated with a new generation of products and business practices which include the use of innovative mechanisms of distribution and technologies;
- cooperates in the definition of the internal control system, the procedures and the controls aimed at preventing and combatting money-laundering risk;
- cooperates in the definition of the governance of money-laundering risk policies and of the various steps composing the process for managing this risk;
- checks the suitability of the process for managing the money-laundering risk and the suitability of the internal control system and procedures, and proposes organisational and procedural modifications needed or advisable to ensure adequate coverage of the risks;
- ensures the definition and maintenance of the control system aimed at guaranteeing compliance with the obligations related to the customer due diligence, according to a risk-based approach which provides for an adjustment of such obligations according to the money-laundering risk profile attributed to the customer;
- may carry out an enhanced due diligence process only in those cases when – for objective, environmental and subjective circumstances – the money-laundering risk is quite significant;

    - verifies the reliability of the information system for the fulfilment of the obligations related to the due diligence of the customer, storage of data and reporting of suspicious transactions.
- verifies the correct functioning of the information system for the fulfilment of the obligations regarding the forwarding of objective communications;
- analyses and investigates the exogenous and endogenous reports received on alleged suspect transactions to be submitted to the Delegate responsible for the reporting of Suspicious Transactions, for the evaluation of any necessary reports to the FIU;
    - examines the evidence that comes from the automatic recognition systems or specific recognition systems of the Anti-Money Laundering Function and investigates the results for possible submission to the “Delegate responsible for reporting Suspicious Transactions” to assess whether to send the reports to the Financial Intelligence Unit (FIU);
    - supports the Delegate responsible for reporting Suspicious Transactions in sending the reports found to be warranted to the Financial Intelligence Unit (FIU);
- carries out, in cooperation with the Delegate responsible for the reporting of Suspicious Transactions, some assessments on the effectiveness of the reporting system and the correctness of first level evaluations carried out on customers' operations;
    - monitors the monthly sending to the Financial Intelligence Unit (FIU) of the aggregate data registered in the Single Computer Archive by the computer outsourcer;
- forwards to FIU, based on the instructions issued thereby, the objective communications;
- cooperates, as regards anti-money laundering issues, with the Authorities under Title I, Paragraph II of the Anti-Money Laundering Decree and fulfils the requests for information received therefrom;
- ensures, in cooperation with the other corporate functions, competent in the area of personnel training, the setup of an effective training programme aimed at achieving an on-going updating of the personnel;
- at least once a year prepares a Report on the initiatives undertaken, the deficiencies identified and the relevant corrective actions to be undertaken, as well as on personnel training activities, to be submitted to the Board of Directors, the Risk Committee, the Board of Statutory Auditors and the Chief Executive Officer;
- carries out, in cooperation with the other involved corporate functions and according to the methods and time frames defined by the Bank of Italy, a Self-assessing process about the money laundering and financing of terrorism risks, the results of which are included in the annual Report described above;
- promptly informs the Corporate bodies about relevant breaches or deficiencies identified during the performance of related tasks;
- prepares proper information flows for the Corporate Bodies;
- performs, in outsourcing, for the Companies of the financial Conglomerate with which there are service agreements in effect, specific activities aimed at combatting the risk for money-laundering, according to methods defined in said agreements;
- collects and reviews the information flows coming from the same functions of the foreign subsidiaries belonging to the financial Conglomerate;

- within the area of its responsibility, prepares/validates and updates the internal regulations, the Policies and provisions on anti-money laundering and anti-terrorism and prepares, if necessary, the related Group guidelines.

The Anti-Money Laundering Function employees must be in a sufficiently independent position to be able to express their assessment, give their opinions and provide recommendations on an impartial basis; regardless of their hierarchical position within the organisation, they must not have any conflicts of interest, arising from professional or personal relationships, or from monetary or any other type of interest that may jeopardise the duties to be fulfilled; additionally, they must be protected from undue interference that could limit or change their scope of action or the performance of their jobs, or that could significantly affect or influence their opinions or the content of their work.

The staff remuneration and inducement system in the Anti-Money Laundering Function must be compliant with supervisory regulations and internal policies.

Anti-money Laundering Function Manager

The Manager of the Function (hereinafter also referred to as the **Anti-Money Laundering Manager**) is appointed by the Board of Directors, in agreement with the Board of Statutory Auditors. The Anti-Money Laundering Manager must meet the necessary independence, authority, professionalism and integrity requirements identified in this policy, the fulfilment of which – at the appointment time and consistently thereafter – are assessed by the Board of Directors.

In order to guarantee the necessary independence and authority, the Anti-Money Laundering Manager is placed in the appropriate hierarchical-functional position, without any direct responsibilities in neither operational areas nor hierarchically reporting to the managers of these same areas.

As regards professionalism requirements, the Anti-Money Laundering Manager must demonstrate the following characteristics:

- an in-depth knowledge of the legal and regulatory provisions in effect in the areas of anti-money laundering and anti-terrorism and or a previous experience in risk management and/or in Control Functions;
- an in-depth knowledge of the banking-financial sector;
- the capacity of relating to the Supervisory Authorities, the Investigating Authorities and the Corporate Bodies.

As regards the integrity profile, the Anti-Money Laundering Manager must meet the integrity requirements set forth by the Ministry of the Economy and Finance, implementing the provisions of article 26 of the Consolidated Banking Act applicable to the subjects performing administration, management and control functions at banks.

The Board of Directors assesses the characteristics of the candidate and upon consultation with the Control Body, authorises the assignment.

The Anti-Money Laundering Manager:

- participates, if required, in the meetings of the Corporate Bodies and reports directly to them, with no restrictions or intermediations;
- can access all the necessary corporate documentation in order to perform the tasks set out in the Supervisory regulations;
- verifies the effectiveness of procedures, structures and systems, providing support and advice on management decisions;
- represents the interlocutor of FIU for all issues concerning the forwarding of objective communications and for the requests for information.

Delegate responsible for reporting Suspicious Transactions

The owner of the business, the legal representative of the company or his/her representative is in charge of assessing the suspicious transaction reports that arrive, and sending any reports considered to warrant attention to the Financial Intelligence Unit (FIU).

In order to guarantee the appropriate independence of the reporting subject and the fulfilment of the professionalism and integrity requirements, the role of Delegate responsible for the Reporting of Suspicious Transactions is assigned to the Anti-Money Laundering Manager; this choice, in addition to guaranteeing the appropriate independence of the reporting subject, allows for optimising the specific competences of the manager in the area of anti-money laundering, as well as his/her knowledge of the procedures for an effective customers due diligence and profiling adopted by the Bank.

The Board of Directors may appoint a replacement of the Delegate responsible for the Reporting of Suspicious Transactions – notwithstanding the fulfilment of professionalism and integrity requirements set forth for the Anti-Money Laundering Manager – who, in the case of absence or impediment of the Delegate responsible for the reporting of Suspicious Transactions, takes over the powers and tasks assigned thereto.

The role and responsibilities of the Delegate must be properly formalised and made public within the structure of the Bank and the Sales Network.

The Delegate responsible for reporting Suspicious Transactions:

- has free access to the information flows to the Company Bodies and facilities involved in combatting money laundering and terrorist financing;
- may permit, with the required confidentiality precautions and without mentioning the name of the reporting party, the Managers of the company facilities to learn the names of the customers that have been reported, also by using suitable information reports, is said information could be significant with respect to the acceptance of new customers or to assess the operations of pre-existing customers.
- manages, to the extent of his/her authority, relations with the Financial Intelligence Unit (FIU) and promptly responds to any requests for further information that it may make;
- gives advice to the operating facilities with respect to the procedures to adopt to report any suspicious transactions and any abstention from performing the transactions;

- reviews, based on all available information, the reports on suspicious transactions received from the first level Operating Structures and the communications received from the Board of Statutory Auditors, the Supervisory Body and/or the Internal Audit Function as well as those that have been brought to his/her attention within the scope of his/her activities;
- forwards to FIU the reports deemed as well-founded, omitting the names of the subjects involved in the process of reporting an operation;
- files, giving adequate written reasons, the reports not considered to warrant further investigation;
- also uses, in his/her assessments, any elements that he/she may retrieve from freely accessible information sources;
- communicates, by applying organisational methods suitable to ensure compliance with the confidentiality obligations set forth in the Anti-Money Laundering Decree, the outcome of his/her assessments to the first level subject who has originated the reporting;
- helps identify the measures needed to ensure the confidentiality and storage of the data, the information and the documentation relating to the reports, to submit for approval by the Board of Directors.

The Delegate, when assessing the suspicious transactions, may obtain useful information from the Anti-Money Laundering Manager, and use the support of the Anti-Money Laundering Function.

The Delegate may authorise the Anti-Money Laundering Function employees to operate, under its responsibility, (1) within the system for reporting suspicious transactions (infostat-FIU), in accordance with the instructions given by the Financial Intelligence Unit (FIU), (2) within the profiling system in order to operatively implement the increase/decrease of the profile of the subjects analysed, as decided thereby; (3) within the system for communicating breaches on the circulation of cash and bearer instruments (SIAR) and (4) within the GE.SA.FIN. system, of prior requests for authorisation to conduct operations/payments according to documents related to merchandise in the case of embargoed/sanctioned/under restrictions and/or, within the S.I.G.M.A system, to conduct operations/payments referring to weapons materials, as well as to operate, under its own responsibility, within the system for the management of aggregate reports (S.A.R.A.).

Operational Facilities

The Operational Facilities are the first in line to be responsible for the risk management process. During daily operations, these structures are called upon to identify, measure or assess, monitor, mitigate and report the risks arising from routine company activity in compliance with the risk management process. Moreover, these structures must meet the operational limits assigned to them consistently with the risk objectives and procedures into which the risk management system breaks down.

All employees and associates of the Operational Facilities, within the scope of their corporate roles, are required to be informed of the law, regulations and rules issued by the Bank, and comply with them. The corporate documents governing organisational and behavioural aspects of compliance with prevailing regulations, both of the law and defined in the Bank, must be brought to the attention of all employees and associates by publishing and disseminating them according to the methods set forth by each Company of the Group.

If the employees and associates, while carrying out their activities, find that the operating processes in place are not in line with the applicable regulations or the controls adopted are not effective enough to prevent the involvement, including without being aware, of the Bank or the Group companies in money laundering or terrorist financing, they must promptly inform their managers.

If the Operational Facilities are in charge of the administration and actual management of customer relations, they will also be in charge of the identifying and performing due diligence on the customers assigned to them as the first level of control, to get to know the customer, and ensure the continuous monitoring during the relationship in accordance with the underlying risk. The Operational Facilities are also in charge of carrying out the enhanced due diligence in the cases provided for by law, and if required by the Anti-Money Laundering Function, and are in charge of promptly reporting [3], where possible before carrying out the transaction, any suspicious transactions in accordance with the internally defined procedures and methods, if they have any suspicions or have reasonable reason to suspect that money laundering or terrorist financing has been carried out, is being carried out, or is being attempted.

The Managers of the Facilities must focus effectively on personnel management and on the use of operating tools, provided to them, in order to ensure the constant pursuance of the company's objectives, and they must, within the area of their competence, comply and ensure compliance with all applicable provisions, both of the law and those issued by the company.

Each Manager is responsible for the overall compliance and effective functioning of the first level controls in his/her facility.

If the Managers, while carrying out their activities, find that the operating processes in place are not in line with the applicable regulations or the controls adopted are not effective enough to prevent the involvement, including without being aware, of the Bank or the Group companies in money laundering or terrorist financing, they must, having carried out the necessary investigations, promptly involve the Anti-Money Laundering Function so that it can make the assessments it is responsible for.

To that end, the Bank provides its employees and associates with operating tools and procedures, including computerised, that can help them fulfil their relative anti-money laundering obligations, and sets up specific training and permanent professional training programmes for them to ensure they are aware of the applicable regulations and related responsibilities, and can properly use the support instruments and procedures to help them fulfil the requirements.

Sales Network

The financial advisors in the Sales Network (known as Family Banker®) are personally in charge of the identification process and due diligence of the customer assigned to them as the first level of control, to get to know the customer, and ensure the continuous monitoring during the relationship in accordance with the

[3]This is without prejudice to the cases where the transaction has to be carried out since there is a legal obligation to receive the document, or the cases where the transaction cannot be postponed taking account of normal operations, or the cases where postponement of the transaction could hinder investigations.

underlying risk. They are also in charge of carrying out the enhanced due diligence in the cases provided for by law, and if required by the Anti-Money Laundering Function.

The Financial Advisers, within the scope of the activities carried out on behalf of the Bank, are required to be informed of and comply with the laws, the regulations and provisions issued by the Bank, as provided under the agency contracts.

The Bank provides its financial advisors with operating tools and procedures, including computerised, that can help them fulfil their relative anti-money laundering obligations, and sets up specific training and permanent professional updating programmes for them so they become adequately aware of the applicable regulations and related responsibilities, and can use the support instruments and procedures to help them fulfil the requirements.

the Bank constantly monitors compliance, by the Sales Network, with the rules applied to the anti-money laundering conduct, as set forth in the applicable regulations and agreements, also through periodical assessments carried out at the administrative offices of the financial consultants.

Since the Family Bankers® are actually in charge of the administration and management of relations with the customers assigned to them, they constitute the first reporting level to all effects.

Therefore, the financial advisors will be in charge of promptly reporting [4], where possible before carrying out the transaction, any suspicious transactions in accordance with the internally defined procedures and methods, if they have any suspicions or have reasonable reasons to suspect that money laundering or terrorist financing has been carried out, is being carried out, or is being attempted.

4.2 ITALIAN COMPANIES BELONGING TO THE BANKING GROUP

With reference to monitoring the risk of money laundering and terrorist financing, in order to pursue the full and concrete implementation of the Group model, the outlying Subsidiaries will adopt a policy that takes account of the Group guidelines, in accordance with a principle of proportionality and on the basis of the specific nature of its activities.

If required by secondary regulations, the body responsible for the strategic supervisory functions (upon consultation with the control functions) of each Italian company belonging to the Group, appoints its own Manager/Representative/Contact person of the Anti-Money Laundering Function.

4.3 FOREIGN COMPANIES BELONGING TO THE BANKING GROUP

In order to pursue the full and concrete implementation of the Group model, the procedures in effect at the foreign subsidiaries and branches must be in line with the Group standards and ensure sharing of the information at the consolidated level, subject to compliance with the specific requirements provided by the law

[4] See note 5

of the country in question. Therefore, foreign Subsidiaries that fall within the range of application of this document will adopt this policy in accordance with a principle of proportionality and taking account of the specific nature of the business and local laws.

In the foreign companies where local laws require this figure, and in any case in compliance with local regulatory provisions, an Anti-Money Laundering Manager will be appointed to ensure the correct management of risk arising from the requirement to comply with all applicable provisions of the law, also as regards the different areas of international operations. The Anti-Money Laundering Manager will ensure compliance with the policies approved by the Parent Company.

5 GROUP STANDARDS FOR COMBATTING MONEY LAUNDERING AND TERRORIST FINANCING

The Bank and the companies of the Group adopt procedures and methods commensurate to the nature of the performed activities and to their sizes for the analysis and assessment of money-laundering and financing of terrorism risks to which they are exposed in the performance of their duties, taking into account multiple risk factors.

The Bank has defined certain Group guidelines based on the highest standards for combatting money laundering and terrorist financing, to which the members of the company Bodies, the employees and the associates must comply with to avoid the involvement, including unwillingly, of the Bank itself and the Group companies in any money laundering or terrorist financing.

The guidelines for fulfilling the obligations in accordance with the regulatory provisions are provided below, and are organised, to ensure implementation, into the specific process rules and internal procedures adopted by each company in the Group.

5.1 CUSTOMER DUE DILIGENCE

The Bank adopts customer due diligence measures that are proportional to the extent of the risk of money laundering and terrorist financing, taking account of specific factors relating to the customer, transaction or business relationship.

The acquisition of the information must aim at the assessment, throughout the duration of the relationship, of the consistency of the transactions with the knowledge of the customer, its activities and its risk profile.

The KYC - Know Your Customer principle, which translates into rules for an effective due diligence, assumes a special relevance in relation to the principle of “active collaboration” and to the obligation of reporting suspicious transactions (see par. 5.7). The identification of the customer, its representative and beneficial owner, if any, with the related verification of identity and the collection of information, must take place within the scope of a discussion which is necessary, on the one hand, for the customer in order to become familiar with the Bank and to declare the scope and nature of the business relationship that it intends to establish, and

on the other hand, for the Bank and its personnel in order to better know the Customer, its banking, financial and insurance needs, and to offer the products and services that are most suitable to meet its requirements.

To this purpose, the Bank sets up appropriate training sessions for its Personnel, based on the contents of the following paragraph **Errore. L'origine riferimento non è stata trovata.**.

The employees of the Operational Facilities in charge of the management and actual administration of customer relations and the financial advisors authorised to sell through indirect sales channels, will fulfil the due diligence obligations by complying with the measures, methods and internal procedures adopted by the bank to develop and keep their customer awareness updated, and to report any suspicious transactions.

In order to ensure the correct execution of customer due diligence, the financial advisors and Operating Facilities of the Bank, which are responsible for the management and administration of the relationships with the customers, will oversee:

- identification of the customers, any representatives or beneficial owners and acquisition of the relative identifying documents and additional information needed to determine the risk profile to assign the customer, as provided in the Bank forms and the companies whose products are placed by the Bank;
- the identification of the beneficiary, in the hypotheses set forth in the regulations applicable at any given time, as soon as it is identified or designated, regarding the insurance service provided by the policies placed by the Bank, in its capacity as insurance intermediary, as well as of the actual recipient of the settled amount and of the respective beneficial owners;
- the verification of the identity of the customer, the beneficiary, the representative, if any, and the beneficial owner[5] of the customer and of the beneficiary, based on the documents, data or information obtained from a reliable and independent source;
- the census carried out on the customers, of the representatives, if any, and the beneficial owners, available in the Master Database of the Bank and the retention of the documentation acquired for identification and verification purposes, according to the confidentiality provisions and measures dictated by internal regulations;
    - the acquisition and assessment of information on the scope and nature of the business relationship and the relations between the customer and the representative or the customer and the beneficial owner;
    - the constant control of the business relationships in order to keep the knowledge of the customer and the declared scope of the relationship up to date, and to assess any “unexpected” or anomalous transactions, or transactions that are not consistent with the economic or financial profile of the customer known beforehand, or news of significant events;

[5]In support of the requirements concerning the due diligence of the beneficial owner, the Bank may also access the related section of the Register of Companies; in these cases, it acquires and retains a proof of the enrolment of the beneficial owner in this Register or an excerpt of the Register suitable to prove such enrolment.

- the update of the data and information gathered, at a frequency that depends on the risk profile previously associated with the customers (see par. 5.2), asking them to provide, under their own responsibility, all the up to date information needed to allow the due diligence obligations to be fulfilled.

The customer enhanced due diligence measures apply to the times and to the circumstances described here below:

- when a business relationship is established or when the beneficiary of an insurance policy is designated;
- at the time of the execution of an occasional transaction, arranged by the customer, which involves the transmission or the handling of payment instruments in an amount equal to or exceeding Euro 15,000, regardless of the fact that it is carried out with a single or multiple transactions which appear to be connected in order to perform a fragmented transaction or that it consists in a transfer of funds, as defined in article 3, paragraph 1, point 9, of the (EU) regulation no. 2015/847 of the European Parliament and the Council, exceeding one thousand euros;
- when there is a suspicion of money-laundering, regardless of any derogation, exemption or applicable threshold, based also on indicators of anomalies and patterns that are representative of abnormal behaviour, issued by the FIU in compliance with the Anti-Money Laundering Decree;
- when there are doubts on the completeness, reliability or truthfulness of the information or documentation previously acquired by the customers.

The collection of data and information is obtained through a guided process for the completion of the Personal Data and Anti-Money Laundering Record.

A due diligence process is not required for activities aimed at or related to the organisation, the functioning or the administration of the Bank, taking into account that they do not fall under the institutional activities thereof and that, in carrying them out, the counterparties of the Bank are configured as providers of goods or services upon an initiative taken by the Bank, rather than as customers who ask to establish a business relationship or to carry out an occasional transaction.

Relationships and transactions carried out upon an initiative by the manager as regards the provision of an individual portfolio management service are also excluded.

In no event, the obligations of a due diligence may be transferred to shell banks or intermediaries located in high risk third countries.

Remote operations

Remote operations refer to those transactions carried out without the physical co-presence of the Customer and the Personnel entrusted by the Bank (e.g. through the telephone or electronic systems); if the customer is a subject other than a natural person, it is considered to be present when the representative is.

The Bank pays particular attention to remote operations in consideration of the absence of a direct contact with the customer or the representative, also due to the growing risk of frauds related to identity theft, including when resorting to the use of public databases.

In the case of remote operations, the Bank acquires the identification data of the customer and of the representative and issues evidence on a copy – obtained through fax, mail, in electronic format or with equivalent methods – of a valid ID document, pursuant to the applicable laws.

In order to provide additional evidence about the acquired data, the remote identification process is followed by a bank transfer, set up by the Customer, from an intermediary bank located in Italy or in a EU country, notwithstanding the possibility, for the customer, to take advantage of the possibility of a *de visu* identification though a financial consultant of the Bank or through electronic identification procedures that are secure and regulated, i.e. authorised or recognised by the Digital Agency for Italy.

With a view to minimizing exposure to possible money-laundering and/or fraud risks, the establishment of remote relationships is not allowed for subjects:

- other than natural persons;
- not residing in Italy;
- showing FATCA indications (US Person);
- falling under the category of Politically Exposed Persons;
- characterised by a "negative reputational indicators" based on "name lists" and databases used by the Bank.

In these cases, the process for the establishment of the relationship can exclusively occur through the Bank Personnel which is directly responsible for the customer's due diligence process.

Any request for payment instruments by customers who establish remote relationships, involves in all cases, the forwarding of a specific communication to a physical address with return receipt, with the activation of special verifications, in the event of a failed delivery of the correspondence to the address that was communicated.

In consideration of the afore-described limitations and the controls adopted by the Bank, the Anti-Money Laundering Function has carried out special verifications and has found, overall, that the risk associated with the remote identification process is overall quite contained.

5.2 CUSTOMER PROFILING

In order to adjust the depth and extension of the obligations for a due diligence process, the Bank adopts procedures aimed at profiling each customer according to their money-laundering and financing of terrorism risks, and that consider the following risk factors:

- risks related to the customer, the representative and the beneficial owner;
- risks related to products, services, transactions or distribution channels;
- geographic risks.

This approach is an application of the broader principle of proportionality referred to by prevailing regulatory provisions, with the goal being to maximise the efficiency of the company controls, and streamline the use of resources.

To that end, the information on the profile of the risk of money laundering and terrorist financing will be made available to the financial advisors of the sales network, and the Operating Facilities in charge of the actual management and administration of the customer relations.

The electronic controls available to the Bank[6] allow the determination - on the basis of the data processing and the information acquired when recording of information on the register to initiate the business relationship, execute occasional transactions or monitor the operations put in place - of a "score" representing the level of risk of money laundering or terrorist financing and to classify the customers into four classes.

In order to assess the risks related to a customer, the representative and the beneficial owner, the Bank takes into account additional risk factors (see 5.3), optimising all available information, assessing any negative information coming from the media or other information sources considered as well-founded and reliable, reviewing reports on abnormal behaviours from the Sales Network or the employees of the Operating Structures that actually concretely manage and handle the relationships with customers.

In order to ensure a correct assessment of the risks related to products, services, transactions or distribution channels, the corporate competent functions of the Bank ensure the involvement of the Anti-Money Laundering Function starting from the preliminary analysis phases and feasibility studies. The risk must be carefully assessed, in particular, in the case of products and commercial practices of the new generation that include the use of innovative distribution mechanisms or technologies for new or pre-existing products.

In order to assess the geographic risks, the Bank considers the following risk factors:

1) third countries that high-standing and independent sources believe they lack of effective controls for the prevention of money-laundering (such as the countries included in the EU/GAFI list);
2) countries and geographic areas that finance or support terrorist activities or where terrorist organisations operate (such as those countries included in the EU/GAFI lists);
3) countries subject to sanctions, embargo or similar measures adopted by competent national and international authorities;
4) countries assessed by high-standing and independent sources as non-compliant with international standards in terms of transparency and exchange of information for tax purposes;
5) countries and geographic areas assessed with a high level of corruption or susceptible to other criminal activities, as determined by high-standing and independent sources.

The Bank considers the afore-described risks of a geographic nature based on the different level of criticality attributed thereto. Implementing this risk-based approach:

[6]The Bank uses GIANOS GPR® software to profile the customers in accordance with the risk of money laundering and terrorist financing.

- the Bank considers, in all cases, at high risk all the customers and/or the relationship that show significant ties with the countries included at number 1) and 2) of the previous list, as well as those with names that correspond with the lists of the associated persons or entities for the purpose of applying freezing obligations set forth by the Security Council of the United Nation, the EU Regulations or the decrees adopted pursuant to Legislative Decree no. 109 of 22 June 2007 or that of the Office of Foreign Asset Control (OFAC) of the Treasury Department of the United States[7].
- the geographic risk factors under numbers 3), 4) and 5) do not automatically involve the attribution of a high risk profile to the customers, but are assessed for the purpose of a possible increase of the risk level, together with additional relevant factors, using a specific index calculated by an independent and non-profit centre of competence[8], specialised in combatting corruption and other financial crimes.

The Anti-Money Laundering Function may propose, in all cases, to the CEO, to suspend the establishment of new relationships and the performance of transactions with countries characterised by one or more of the geographic risk factors described above. The CEO assesses the opportunities to implement this proposal and may identify specific relationships and transactions (or specific classes/types of relationships and/or transactions) concerning which this blockage would not apply.

The updated list of the countries considered of a higher risk and those with which operations have been suspended, is periodically made available to the Board of Directors, within the scope of the information periodically produced by the Anti-Money Laundering Function.

The table below shows possible risk profiles that can be given to the customers and how often the due diligence data should be updated.

Ref.	Risk class	Frequency of updates
I	Irrelevant	Every 48 months
B	Low	Every 36 months
M	Medium	Every 24 months
A	High	Annual (every 12 months)

[7] In order to identify these names, the Bank uses the infoprovider Worldcheck of the company Refinitiv.

[8] Reference is made to the "Basel AML Index", calculated by the "Basel Institute on Governance", an independent, non-profit centre of competence, specialised in combatting corruption and other financial crimes.

The Bank will monitor and periodically update the scores and rules given to the risk profiling system, also referring to developments in the area of reference and leading practices in the market.

As part of a Group, the Bank (as the other companies of the Group) takes on, in all cases, for the same customer, the highest profile among those assigned by all the companies of the Group.

The profiling system ensures that the scores assigned by the electronic system, are consistent with the knowledge of the customer. In all cases. the Anti-Money Laundering Manager may, if necessary, decide to automatically raise the risk profile also following acquisition and review of any reports received from financial consultants of the Sales Network or the employees of the Operating Structures who manage or administer the relationships with the customers (see 5.3), while maintaining evidence of the carried out assessments. The Anti-Money Laundering Manager may also decrease, following assessment made in the course of analysis carried out on specific positions, the assigned scores, while maintaining evidence of the completed analyses. In all events, it is not allowed to autonomously change the scores assigned by the rest of the Personnel.

5.3 CUSTOMER ENHANCED DUE DILIGENCE PROCESS

In the presence of a high risk in money laundering and financing of terrorism, the Bank adopts strict measures concerning customer due diligence by acquiring additional information on the customer, on the beneficial owner and on any representative, analysing in depth all elements on which the assessments were based as regards the purpose and nature of the relationship, and intensifying the frequency of the application of procedures aimed at guaranteeing the constant control carried out on the business relationship.

As part from a more general process concerning the due diligence and an in-depth analysis of the knowledge of the customer, the application of stricter measures regarding the customer due diligence is of a particular importance also in connection with the principle of “active cooperation” and the obligation of reporting suspicious transactions (see 5.7).

In particular, the Bank considers being at a higher money laundering risk

a) the customers, the beneficial owners and the representatives about which negative reputational indexes have been identified, based on:
   - the recurrence of their names in the lists of persons or associated entities for the purpose of fulfilling the freezing obligations set forth by the Security Council of the United Nation, the EU Regulations or the decrees adopted pursuant to Legislative Decree no. 109 of 22 June 2007 or that of the Office of Foreign Asset Control (OFAC) of the Treasury Department of the United States;
   - negative news provided by the media or other information sources;
   - negative news directly provided by the Customer or the reference financial consultant concerning criminal proceedings for tax defaults, administrative liabilities of entities (ex Legislative Decree 231/01), etc.[9];

[9]These cases are subject to the opening of a preliminary investigation by the Anti-Money Laundering Function following which a possible increase of the score is assessed.

- requests/provisions originated by the Judicial Authority, pursuant to the AntiMafia Code (assessments required by the Criminal Authority pursuant to Legislative Decree 159/2011 - AntiMafia - preliminary investigation phase) or to the anti-money laundering regulations (assessments required by the Penal Authority pursuant to the Anti-Money Laundering Decree - preliminary investigation phase);
- attachments decrees, precautionary and prevention measures adopted by the Judicial Authority;

b) customers, beneficial owners and representatives, subject matters of reports sent to FIU;

c) customers whose funds originate from voluntary disclosure transactions or similar procedure for capital repatriation due to tax evasion or other crimes;

d) cross-border payable-through accounts involving payments with a credit institution or corresponding financial institution of a third country;

e) business relationships, professional services and occasional transactions with customers and related beneficial owners who are politically exposed people, except in those cases when said politically exposed people act on behalf of bodies of the Public Administration[10];

f) business relationships, professional services and transactions involving high risk third countries, as well as the customers and beneficial owners residing or with registered offices in high risk geographic areas, as identified above (see 5.2);

g) qualifiable structures, as vehicles of equity intermediaries, such as trusts, fiduciary companies (regardless of the related enrolment in the Register ex article 106 of the Consolidated Finance Law), foundations, companies the share capital of which is held, in full or partially, by a fiduciary company, a trust, an entity or similar legal person; companies controlled by fiduciaries;

h) customers with an unusual or excessively complex corporate structure, given the nature of the performed activity;

i) customers carrying out a type of economic activity characterised by a high use of cash or with an involvement in sectors that are particularly exposed to corruption risks;

j) customers who benefit from services with a high degree of customisation, offered to customers with a significant equity amount;

k) customers who carry out:
   - transactions in cash, frequent and unjustified, characterised by the use of high denomination banknotes in euro or the presence of banknotes that are damaged or counterfeited;
   - transactions involving cash or other cash equivalents originated from abroad, in a total amount of or exceeding Euro 10,000;
   - transactions related to oil, weapons, precious metals, tobacco products, cultural artifacts and other moveable properties of an archaeological, historical, cultural, religious importance or of a rare scientific value, as well as ivory and protected species.

[10]The qualification of PEP is important for both the customer (and the beneficiary, in the case of insurance products) and for the beneficial owners and not for representative.

l) the products and the business practices of a new generation, including innovative distribution mechanisms and the use of innovative or in development technologies for new or pre-existing products.

Furthermore, the Bank considers customers to be high risk based on the customer profiling system internally adopted and on indexes of risks set forth in the applicable laws or upon request from the Delegate responsible for reporting suspicious transactions, following a prudent assessment thereby, as well as any other case when the financial consultant or the designated employee identifies, during the finalisation of a transaction or the opening of a new business relationship, a greater money-laundering or financing of terrorism risk. In particular, the behaviour displayed by the customer or the representative, must be carefully assessed by the financial consultant or the designated employee, e.g.:

- the reluctance to provide the required information;
- repeated changes to the provided information or the fact that incomplete or erroneous information are provided,
- the non-availability or impossibility to produce documentation as regards their identity (except when requesting asylum),
- the reluctance to opening a business relationship preferring the execution of one or more occasional transactions, although the opening of a business relationship could be financially more reasonable,
- the execution or intention to execute transactions characterised by unusually high amounts or about which there are some doubts regarding the actual set out purposes thereof,
- the receipt of payments by third parties who do not have any connection with the customer or its activities,
- the reasonable level of the transaction based on normal operation/equity/revenue of the customer,

while assessing the submission of a specific report made to the Anti-Money Laundering Function for an in-depth analysis thereof.

This without any prejudice to the possibility by the Anti-Money Laundering Function to ask to the reference financial consultant or to the Operating Structure which manages and handles the relationships with the customers, to carry out a due diligence process in all cases, including those not listed above, where the money-laundering or financing of terrorism risks appear to be particularly high.

In the case of business relationships or transactions with Politically Exposed Persons, the Bank requires that the subjects holding administration or executive powers or their delegated persons, or any other subject who performs similar operations, must be authorised before starting, continuing or maintaining a business relationship or carrying out an occasional transaction with these customers, applying adequate measures for determining the origin of the assets and the funds used in the business relationship or in the transaction and ensuring a constant and strict professional control on the business relationship or the professional service.

In addition, the Bank requires that an authorisation is issued to the subjects holding administration or executive powers or to their delegates, or in all cases, to those subjects who perform an equivalent function, before they start or continue or maintain a business relationship, provide a professional service or carry out a transaction

that involves third countries at high risk, and that they also acquire additional information on the purpose and nature of the business relationship or of the professional service, on the origin of the funds and the economic-equity position of the customer and the beneficial owner, on the reasons for carrying out the planned or completed transactions while ensuring a constant and strict control on said business relationship or professional service.

The Bank assesses, based on the ascertained risk, whether to apply strict measures of due diligence to subsidiaries or affiliates, operating in high risk third countries, that are controlled by subjects obliged to have their registered office in the Republic or another member state, to ensure that said subsidiaries or affiliates comply with the policies and procedures of the Group, pursuant to article 45 of the Directive.

Based on the model adopted by the Bank, the activities related to the customer due diligence are primarily assigned to financial consultants or to the designated employees, who are required to:

- complete a specific enhanced due diligence questionnaire, made available to them by the Bank;
- acquire additional information on the customer and the beneficiary owner;
- acquire/update and review information on the reputation of the customer and/or the beneficial owner (including any prejudicial elements obtained by consulting open sources, through, for instance, the use of Internet research engines);
- carefully assess the information provided by the Customer on the purpose and nature of the relationship, combining it with all the other information already available at the opening of the relationship, or in the case of customers who have already established a relationship with the Bank, with the activities already identified; to this regard, the following elements are taken into consideration: the number, size and frequency of the carried out transactions, the origin/destination of the funds, the nature of the activity carried out by the customer and/or the beneficiary owner, the reasonableness of the carried out transaction according to the customer's overall profile;
- perform in-depth assessments on the origin of the assets and funds used in the business relationship, through a structured process that takes into consideration, primarily, the reliability of the information available to the financial consultant and to the Bank, as well as the availability of financial-equity information – produced directly by the customer or inferred from changes occurring in the relationships (e.g. emolument or dividend crediting, etc.) or to be retrieved through open sources or from public databases (e.g. financial statements, VAT declarations and income statements, notary public deeds, succession declarations, declarations/documents coming from the employer or other intermediaries); in this regard, some aspects, such as the degree of knowledge of the customer and/or the length of the relationship, the consistency of the profile of the customer with its financial-equity position, are of a particular importance;
- carry out more frequent assessments and updates of the master database information and of the information collected for acquiring a better knowledge of the customer.

As indicated in the previous paragraph **Errore. L'origine riferimento non è stata trovata.**, under objective, environmental or subjective circumstances which may increase the risk for money-laundering, the activities related to the customer due diligence are performed directly by the Anti-money Laundering Function. These cases, deemed to be of a higher risk, are identified (and properly updated also according to the

operations carried out by the Bank) within the scope of specific, corporate operational procedures for the implementation of this Policy.

These refer in particular to the hypotheses listed in previous letters a), b), c) and d) of this paragraph**Errore. L'origine riferimento non è stata trovata.**.

The Anti-Money Laundering Function must also be involved in the activities carried out by the financial consultants and the employees of the Operating structures which are entrusted with the handling and management of the relationships with the customers when some anomalies are identified in the behaviour displayed by the customers or by the beneficial owner, as described above.

In these cases, the enhanced due diligence process provides for the acquisition of information through the financial consultant or the employee of the Operating Structure who manages and handles the relationships with the customers.

the Anti-Money Laundering Function carries out additional in-depth analyses in order to verify the consistency of the transactions under scrutiny and of the collected information with the information in possession of the Bank and, if necessary, shall request the Customer, through the financial consultant or the designated employee, to provide some specific documentation.

The Anti-Money Laundering Function may identify hypotheses that require the involvement of additional Operating Structures of the Bank which must support the financial consultants or the employees responsible for carrying out the assigned assessments on the outcomes of said activities.

5.4 CUSTOMER SIMPLIFIED DUE DILIGENCE MEASURES

In the presence of a low money-laundering and financing of terrorism risks, the Bank may apply some simplified due diligence measures applicable to the customer under the profile of an extension and frequency of obligation fulfilments, toward:

- companies listed on a regulated market and subject to disclosure obligations that require the obligation of ensuring an adequate transparency of the actual ownership;
- public administrators, or institutions or bodies that carry out public functions, in compliance with the EU laws;
- banking and financial intermediaries listed in article 3, paragraph 2, of the Anti-Money Laundering Decree - except for those under letters i), o), s), v) - and banking and financial intermediaries operating in the EU or in a third country with an effective system for combatting money-laundering and financing of terrorism.

For the correct fulfilment of the obligations above, the Bank makes a distinction between “active counterparties” and “passive counterparties”

The so-called “active” counterparties are the customers, i.e. the companies that have business relationships with the Group (e.g. placement and/or distribution agreements) or that carry out occasional transactions (e.g. treasury transactions, very short term money transactions).

This includes, but is not limited to, the following “active” counterparties:

- institutions/companies holding giro and/or regulatory accounts;
- companies managing investment mutual funds;
- institutions/companies issuing securities on the market through the public offer to which the Bank directly adheres;
- the institutions/companies with which some professional relationships are in place for the placement of electronic money or financing/investment products;

The Bank excludes from the obligations of due diligence, the so-called “passive” counterparties, i.e. the financial intermediaries (domestic and international) with which it maintains business relationships but which it uses for the finalisation of transactions on behalf of its own customers, holders of relationships (security dossier transfer transactions, purchase/sales of securities, etc.). Within this scope, the “passive” counterparties assume the role of “service providers” upon the initiative of the Bank and not as customers requiring the establishment of a business relationship or to carry out an occasional transaction. The “passive” counterparties include, but not limited to, depository banks and companies censured as issuers of securities.

Notwithstanding the necessity of ensuring the correct identification of the customer and of the beneficial owner before initiating the business relationship or carrying out the transaction, the simplified due diligence measures consist of the possibility of:

- carrying out an audit of the sub-beneficial owner 2, acquiring a declaration with the confirmation of data, signed by the customer, under its own responsibility;
- using assumptions for the identification of the purpose and the nature of the business relationship, where the product offered is intended for a specific use;
- adopting a frequency of 48 months, for the purpose of updating the data collected for the due diligence, notwithstanding the necessity to ensure it in the case of the opening of a new business relationship or of an increase in the money laundering risk profile, due, for example to the identification of negative reputational indexes concerning the customer and/or the beneficial owner;

The Bank verifies the persistence of the assumptions for the application of the simplified procedure, according to the methods and frequency set forth according to the risk-based approach.

In particular, the measures for a simplified due diligence do not apply when:

- the conditions for the application of the simplified measures, based on the indexes of risks set forth in the Anti-Money Laundering Decree and the Provisions, cease to exist;
- the monitoring activities on the overall operations carried out by the customers and the information acquired during the course of the relationship lead to the exclusion of the presence of a low risk situation;
- there is always the suspicion of money-laundering or financing of terrorism

5.5 OBLIGATIONS TO ABSTAIN

If the Bank finds it objectively impossible to perform due diligence on the customer, it cannot start, continue or pursue the relationship, transactions or professional services (known as the obligation to abstain) and, if necessary, must terminate the business relationship already in place and decide whether to make a suspicious transaction report to the Financial Intelligence Unit (FIU). Before making the suspicious transaction report to the Financial Intelligence Unit (FIU), and in order to exercise any right to terminate, the Bank may not carry out transactions that it suspects have a connection with money laundering or with terrorist financing.

If it is not possible to abstain since there is a legal obligation to receive the document, or execution of the transaction may not be postponed due to its nature, or if abstaining could hinder the investigations, there is an immediate obligation to make a suspicious transaction report.

The Bank will not initiate any relationships, carry out transactions or provide professional services and will end any business relationships or providing professional services already in place with:

- customers or potential customers who reside or have registered offices in countries that are "under embargo" as identified by the Bank and made available, on a quarterly basis, by the branch employees and the financial advisors;
- credit or financial institutions situated in a non-EU country that does not impose equivalent obligations to those provided under the EU directives issued in these areas;
- shell banks in any location;
    - subjects who are, directly or indirectly, part of fiduciaries, trusts, anonymous companies (or controlled through bearer shares) located in high risk third countries;
- companies that have issued bearer shares;
- trusts where the information available is inadequate, inaccurate or not updated with respect to the beneficial owners of the trust or its nature or scope or who show subjective or objective circumstances which may indicate the use of a trust in order to conceal anomalous behaviours, also in view to indications provided by the competent authorities;
- relationships held in the name of trusts where the information available is inadequate, inaccurate or not updated with respect to the beneficial owners of the trust or its nature or scope;
- payment service providers (agents and/or money transfer companies) who do not carry out financial activities on an exclusive basis;
- operators that carry out significant commercial activities in the gold-buying area, exercised on an exclusive basis, or on a secondary basis with respect to their main business, who are not validly registered on the gold-buyer operator registry, if necessary established at the Agent and Mediatory Organisation (OAM)[11];
- providers of services related to virtual currency;
- companies involved in the manufacturing of weapons or ammunitions;

[11]In accordance with article 3 of Legislative Decree 92/2017 "Rules for exercising the gold-buying business in implementation of article 15, paragraph 2, letter l) of law no. 170 of 12 August 2016"

- game service providers not included in the gaming licensees that have formally adopted the procedures and controls referred to in the guidelines issued by the Customs Agency, pursuant to article 52, paragraph 4 of the Anti-Money Laundering Decree;
- legal persons who are directly or indirectly invested in by one of the above-mentioned parties.

The Bank abstains from offering products/services or carrying out transactions that may favour anonymity, or the concealment of the identity of the customer or the beneficial owner, as well as from establishing business relationships or remotely carrying out occasional transactions, not assisted by electronic identification procedures that are safe and regulated or authorised or recognised by the digital Agency for Italy.

Pursuant to article 50 of the Anti-Money Laundering Decree, it is also prohibited to open or use anonymous bank or saving accounts or accounts under fictitious names as well as to issue or use anonymous electronic money products.

.

5.6 CONTROLS TO COMBAT TERRORIST FINANCING

In order to ensure the correct fulfilment of the obligations and prohibitions provided under prevailing law on anti-terrorism matters, the Bank:

- will automatically control the data registers and compare names against names on the lists of parties designated by the UN Security Council, the European Union, decrees by the Ministry for the Economy and Finance, and the Office of Foreign Asset Control (OFAC) of the Treasury Department of the United States;
- will refuse to carry out any transactions that involve parties on the lists described in the previous paragraph (presenters, representatives, ordering parties or beneficiaries);
- will not make cover payments[12] in US currency;
- will apply the restrictions provided for in relationships with all companies where correspondence has been found with the lists described in the first paragraph;
- will inform the Financial Intelligence Unit (FIU) of the measures applied in accordance with Legislative Decree 109/2007, indicating the parties involved, the amount and nature of the Funds or economic resources, within thirty days from the date of entry into effect of the EU regulations, the decisions of international bodies and the European Union, and decrees by the Ministry of Economic Affairs and Finance, or if later, from the date the funds or economic resources have been held.

5.7 NOTIFICATION OF SUSPICIOUS TRANSACTIONS TO THE FINANCIAL INTELLIGENCE UNIT (FIU)

The Bank will promptly send the Financial Intelligence Unit (FIU) a suspicious transaction report when it knows, suspects, or has reasonable grounds to suspect that money laundering or terrorist financing transactions are

[12]Cover payments are the transfer of funds used when there is no direct relationship between the payment service provider (PSP) of the ordering party and the beneficiary, and a chain of correspondent accounts therefore has to be used through a PSP. Three or more payment service providers are involved in a cover payment.

taking place or were carried out or attempted, or in any case that the funds, regardless of the amount, derive from criminal activities.

The financial advisors of the Sales Network and the employees of the operational facilities who are actually in charge of the administration and management of relations with the customers constitute the first reporting level in accordance with prevailing law. They shall therefore be in charge of continuously monitoring the progression of the relationship and the transactions put in place, including through the instruments and procedures available on the BmedNet Portal, and will promptly send the Anti-Money Laundering Function, in accordance with the internally established procedures and methods, a suspicious transaction report before carrying out the transaction: this is without prejudice to the cases where the transaction has to be carried out since there is a legal obligation to receive the document, or in the cases where the transaction cannot be postponed taking account of the normal operations, or in the cases in which postponement of the transaction could hinder the investigations.

In order to facilitate the identification of the suspicious transactions, the Bank will refer in particular to the anomaly indicators issued and periodically updated by the Financial Intelligence Unit (FIU), preparing appropriate guidelines and training and continuing professional education plans for the financial advisors of the Sales Network and the employees of the operating facilities.

The Bank, within the scope of its organisational independence, can also use automatic identification procedures for "anomalous" transactions[13]The Anti-Money Laundering Function will give instructions on all the files relating to the reports received and submit them to the Delegate responsible for reporting Suspicious Transactions and if this person believes that the suspicions are warranted in view of all the elements available and the evidence that can be assumed from the data and information kept, will send them to the Financial Intelligence Unit (FIU), without the name of the reporting party.

The Bank and the companies of the Group adopt measures suitable to ensure the confidentiality of the identity of the authors of reports of a suspicious transaction; the name of the reporting person may only be revealed when the Judicial Authority, by issuing a reasoned decree in this regard, deems it indispensable for the purpose of assessing offences to be prosecuted.

It is also prohibited to the subjects required to report any suspicious transaction and anybody who has knowledge thereof, to communicate to the involved customer or to third parties the submitted report, to forward additional information requested by FIU or information on the initiated, or the probability of initiating investigations on money-laundering or financing of terrorism issues. This prohibition applies:

- to the communications carried out by the Supervisory Authorities of the sector during the performance of functions set forth in the Anti-Money Laundering Decree;

[13]For example, GIANOS INATTESI and GIANOS USURA.

- to the communications concerning the sharing of information at the level of banking and financial intermediaries belonging to the Conglomerate, suitable to guaranteeing full compliance with the provisions set forth on the prevention of money-laundering and financing of terrorism;
- to the communications with other banking and financial intermediaries, external to the Group, belonging to a member State or located in third countries, as long as they apply measures that are equal to those provided for in the Anti-Money Laundering Decree, in the cases related to the same customer or to the same transaction, for the exclusive purpose of preventing money-laundering or financing of terrorism.

5.8 COMMUNICATION OF INFRACTIONS TO THE MINISTRY OF ECONOMIC AFFAIRS AND FINANCE

The Anti-Money Laundering Function and applicable operating facilities who, in the exercise of their functions or activities, have news of infractions of the provisions regarding limitations in the use of cash and bearer securities and the prohibition of anonymous accounts and savings books or with false names (articles 49 and 50 of the Anti-money laundering decree) will fulfil the notification obligations to the Ministry of Economic Affairs and Finance within thirty days.

This notification will also have to be made by the members of the Board of Statutory Auditors when they find breaches of the above-mentioned provisions in the exercise of their control and supervisory functions.

If the transfer has already been subject to a suspicious transaction report in accordance with article 35 of the Anti-Money Laundering Decree, there is no obligation to inform the Ministry of Economic Affairs and Finance.

5.9 OBJECTIVE COMMUNICATIONS

The Manager of the Anti-Money Laundering Function is responsible for forwarding to FIU, in compliance with the instructions provided thereby, objective communications, pursuant to ex article 47 of the Anti-Money Laundering Decree.

He/She must ensure the correct functioning of the information system for fulfilling the obligations to provide objective communications and represents the receiving party of the FIU for all issues related to the transmission of objective communications and any requests for information.

The Manager of the Anti-Money Laundering Function can entrust other subjects, natural persons, under its own responsibility, with the entry and transmission of objective communications.

5.10 OBLIGATION TO STORE THE DATA

In order to fulfil the data storage obligations on the business relationships and the transactions carried out, the Bank will use appropriate storage systems[14], where the business relationships with the customers are

[14]In order to keep the system properly, the Bank and Group companies will use, in accordance with an applicable outsourcing agreement, the outsourcer CEDACRI S.p.A., subject to the logical distinguishing and separation of the records of each recipient.

registered, in addition to the connections and transactions that exceed the materiality thresholds, including any split transactions.

Given the above, the Bank continues to use, on a voluntary basis, the AUI; this decision allows for maintaining processes and controls already fully consolidated, in addition to ensuring the timely availability of the information acquired during the due diligence process, for both fulfilling reporting obligations and for in-depth analyses of the individual positions.

The aggregate data recorded will be sent to the Financial Intelligence Unit (FIU) every month, which will analyse it in order to identify any money laundering or terrorist financing activities.

With regard to fulfilling storage obligations, the Bank will keep:

- the copy or reference of the documents requested for due diligence purposes, for a period of ten years from the end of the business relationship;
- the records and registrations of the transactions and business relationships, entailing the original documents or copies that have the same evidentiary validity in legal proceedings, for ten years from execution of the transaction or termination of the business relationship.

5.11 TRAINING OF EMPLOYEES

The activity for the professional qualification and update of the Personnel assumes a continuity and systematic character within the organic programmes that take into account the development of laws and procedures.

To this end, the Bank uses training programmes and professional continuing education courses in order to correctly apply the provisions set out under the Anti-Money Laundering Decree, recognise transactions related to money laundering or terrorist financing and adopting the right behaviour and procedures.

Particular attention is given to the consultants of the Sales Network and the employees of the Operational Structures who handle and manage the operations carried out by the customers.

Specific training programmes are implemented for the staff who works in the Anti-Money Laundering Function.

The qualification and professional updating of staff is carried out on a continuous, systematic basis within the scope of the internal programmes that take account of developments in the rules and procedures.

5.12 THE INTERNAL SYSTEMS FOR REPORTING INFRINGEMENTS

The Bank adopts specific procedures for internal reporting by employees and collaborators, regarding potential or actual infringements of the provisions governing money-laundering and financing of terrorism (so-called *whistle-blowing*).

These procedures guarantee:

- the protection of the confidentiality of the identity of the whistle-blower and the assumed author of the infringement, notwithstanding the rules that govern the investigations and the proceedings initiated by the judicial authority, concerning the subject matter of these reports;

- the protection of the whistle-blower against retaliatory, discriminatory or in any case dishonest conduct following the report;
- the development of a specific reporting channel, anonymous and independent, proportionate to the nature and size of the obliged subject.

5.13 SANCTIONING AND REPUTATIONAL RISKS

The obligations described in this Policy, aimed at the correct fulfilment of the requirements related to combatting money laundering and terrorism financing, must be strictly complied with, based on the respective areas of competence, by all personnel and in particular by those who manage and administer relationships with the customers, given the correlation set out by the Anti-Money Laundering Decree between the level of money-laundering and terrorism financing risk and the preventive measures adopted by the recipients of the provisions; and this not only during the start of a new relationship or the execution of an occasional transaction, but for the entire duration of the relationship with the customer. It must be noted that, pursuant to the provisions of the Anti-Money Laundering Decree:

- if the Bank is held responsible, exclusively or concurrently, for serious breaches, repeated systematic or multiple, of the provisions set forth as regards the obligation of a proper assessment of the customers, retention and reporting or, in the area of organisation, procedures and internal controls, as well as all related implementation provisions adopted by the Supervisory Authorities, an administrative pecuniary penalty applies, in an amount from Euro 30,000 to 5,000,000, or 10% of the annual overall turnover, if this percentage exceeds Euro 5,000,000 and the turnover is available and measurable;
- notwithstanding the provisions set forth in the previous point, the administrative pecuniary penalty from Euro 30,000 to 5,000,000 is applied to subjects who perform administrative, management and control functions for the Bank and that, by not fulfilling, entirely or partially, requirements directly or indirectly related to their functions or responsibilities, have enabled, facilitated or made possible the breaches under the previous point, or have considerably affected the exposure of the Bank to the risk of money-laundering or terrorism financing. If the advantage obtained by the author of the breach exceeds Euro 5,000,000, the administrative pecuniary sanction may reach twice the amount of the obtained advantage as long as this amount has been determined or is determinable.

It should also be noted that, in the event of an incorrect application of the obligations set forth in the anti-money laundering regulations, additional risks are related to sanctions applicable to the Bank in terms of the administrative liability of legal persons, in compliance with Legislative Decree 231/2001.

5.14 COORDINATION BETWEEN THE ANTI-MONEY LAUNDERING FUNCTION AND THE OTHER CONTROL FUNCTIONS

The interaction between the Anti-Money Laundering Function and the other Control Functions falls within the more general coordination among all the departments and bodies with control responsibilities, as defined by the Board of Directors in order to ensure the correct functioning of the internal control system.

Therefore, reference should be made to the specific document "Guidelines and basic principles for the coordination among Governing standards and Control Functions", approved by the Board of Directors of the Bank.

Said document refers to the basic principles of the Internal Control System and was drawn up in the broadest process of implementing supervisory provisions on the subject of Internal Control Systems and in order to promote and guarantee proper functioning of the Internal Control System as a whole through profitable interaction between the company bodies, committees formed within them, the parties responsible for the audit of the accounts and the control functions.

The document is defined and organised in accordance with the regulatory requirements established by the Bank of Italy and incorporates the documentation in effect of the Banking Group, rationalising the illustration.

6 APPLICABLE REGULATIONS

All the provisions relating to combatting money laundering and terrorist financing are aimed at setting out measures that protect the integrity of the economic and financial system and the honesty of behaviour of the operators who have to comply.

These measures are proportional to the risk in relation to the type of customer, the business relationship, the professional service, the product or the transaction and their application, taking account of the specific nature of the activities, the size and the complexity of the parties who have to fulfil these obligations.

6.1 FOREIGN REGULATIONS

Following are the main reference laws adopted at the EU and national levels:

Preventing and combatting money laundering and financing of terrorism

EU laws

Within the EU, the main laws concerning prevention and combatting of money-laundering and financing of terrorism are found in the Directive (EU) 2018/843 issued by the European Parliament and the Council on 30 May 2018 *"which modifies the Directive (EU) 2015/849 concerning the prevention of the use of the financial system for the purpose of recycling or financing terrorism and that amends Directives 2009/138/EC and 2013/36/EU"* (so called Vth Anti-Money Laundering Directive) and in the Directive 2015/849/EC issued by the European Parliament and the Council on 20 May 2015 *"concerning the prevention of the use of the financial systems for the purpose of money laundering and financing of terrorism, which amends regulation (EU) no. 648/2012 issued by the European Parliament and the Council and repeals Directive 2005/60/EC issued by the European Parliament and the Council, and Directive 2006/70/EC issued by the Commission"* (so-called IVth Anti-Money Laundering Directive).

National laws

At the national level, the main reference laws currently in effect are:

- Anti-Money Laundering Decree and implementation provisions issued by the Supervisory Authorities in the area of:
    - organisation, procedures and internal controls;
    - customer due diligence;
    - objective communications;
    - storage and use of the data and information for anti-money laundering purposes;
- Legislative Decree no. 109 of 22 June 2007, as amended, setting forth measures for the preventing, combatting and suppressing the financing of international terrorism.

The decrees issued by the Ministry of Economy and Finance (MEF) and the schemes representative of anomalous behaviours issued by FIU, complete the reference framework at the national level.

Management of the embargoes

European laws

The main European regulations are set forth in the following provisions:

- Regulation 2580/2001/EC issued by the Council on 27 December 2001 which sets forth the obligation for the freezing of capital and the prohibition of providing financial services to certain natural persons, legal persons, groups or entities who commit or attempt to commit acts of terrorism and of legal persons, groups or entities under the control of the latter;
- Regulation 881/2002/EC issued by the Council on 27 May 2002 which sets forth specific restrictive measures against certain persons and entities (listed in the attachment to the Regulation) associated to Osama bin Laden, Al-Qaeda and the Taliban;
- Regulation 428/2009/EC issued by the Council on 5 May 2009 which establishes an EU framework for the control of exports, the transfer, the intermediation and the transit of dual-use products (recasting of the original Regulation 1334/2000/EC of the Council of 22 June 2000, amended by Regulation 1382/2014 of 22 October 2014);
- Regulation (EU) no. 753/2011 of the Council of 1 August 2011, concerning additional restrictive measures against certain people, groups, companies and entities "in consideration of the situation in Afghanistan" and the decisions taken by the "Sanction Committee" and the "Committee 1267" established within the Security Council of the United Nations[15].

National laws

The main Italian regulations are set forth in the following provisions:

- Law no. 185/1990, amended by Legislative Decree. no. 105/2012 issued by implementing Directive 2009/43/EC entitled "New regulations on the control of export, import and transit of weapons materials". This law represents, to date, the basis of the regulations in terms of the transfer of goods classified as "weapons materials";

[15] The "Sanction Committee" has been established within the Security Council of the United Nations (UNSC) pursuant to point 30 of the 1988 (2011) resolution issued by the UNSC whereas the "Committee 1267" has been established at the UNSC pursuant to resolutions 1267 (1999) and 1333 (2000) of the Security Council of the United Nations.

- Legislative Decree no. 221/2017 which has reorganised and simplified the regulations applied to authorisation procedures for the export of products and technologies with dual use and the sanctions in the area of commercial embargoes, as well as any types of transactions involving the export of proliferating materials. This decree includes the provisions previously contained in Legislative Decree no. 11/2007, Legislative Decree no. 64/2009 and Legislative Decree no. 96/2003 which have been repealed. This decree provides (articles 18 to 21) for the application of penal and administrative sanctions applied to those who perform export transactions of "dual use" goods in violation of the regulations.

As regards secondary laws, a special reference should be made to the Provision issued by the Bank of Italy on 27 May 2009, with operating directives for exercising enhanced controls against the financing of the proliferation of weapons of mass destruction programmes.

6.2 INTERNAL RULES

This Policy is part of the broader context of internal documentation which includes:

- the Code of Ethics;
- the Organisational Model pursuant to Legislative Decree 231/2001 which specifies the preventive control mechanisms and subsequent controls adopted to identify the conduct that could fall into the money laundering and terrorist financing risk area, and to implement timely actions if any anomalies are found;
- the Guidelines and basic standards for Group coordination between Control Bodies and Functions
- the internal whistle-blowing policy
- the Regulation concerning the process for managing Politically Exposed Persons;
- the Anti-Money Laundering Function Rules that illustrate the main guidelines, organisational architecture, processes and instruments adopted by the Anti-Money Laundering Function to carry out its duties;
- the Rules for the due diligence process describing the due diligence process stages, including enhanced due diligence and simplified due diligence, the logic underlying assignment of the risk profile, continuous due diligence;
- the Rules on the process for reporting suspicious transactions that describe the internal process stages before reporting the suspicious transactions;
- the Rules on the second level control process carried out by the Anti-Money Laundering Function that describe the stages of the processes relating to tracking the second level controls on anti-money laundering, including those relating to storage and registration, identifying any actions to reduce the risks found;
- the Rules on the process for the online opening of a new bank account;
- the internal operating manuals of the Anti-Money Laundering Function which describe in detail the operating processes and the elements that form the basis of the models to control the risk of money laundering and terrorist financing.

All these operating and procedural rules and regulations are aimed both at fulfilling mandatory legal provisions and avoiding the involvement, including unwilling, of the Bank in money laundering and terrorism events.