Banca Popolare di Sondrio

This translation of the original Italian document is provided for convenience only. In case of discrepancy, the Italian version prevails.

Level I - General Regulations

Policy on the Prevention of Money Laundering and Terrorist Financing of Banca Popolare di Sondrio and the Banking Group Banca Popolare di Sondrio

ID Code:	DDI_066_E2R1_02052024
Issuing unit:	Group Anti-Money Laundering Service
Approved by:	Managing Director
Edition:	E2R1
Revision date:	02/05/2024
Circulation regime:	PUBLIC

Document versions

Date	Version	Description
06/2023	E1	First edition
03/2024	E2	- General update in implementation of the innovated *Provisions on Organization, Procedures and Internal Controls to Prevent the Use of Intermediaries for the Purposes of Money Laundering and Terrorist Financing of the* Bank of Italy, as amended by order dated August 1, 2023 (effective November 15, 2023); in particular, Introduction of the figure of the exponent responsible for AML; - Integration of paragraph 3.1 with the express mention of the figure of the *compliance officer* at the Monte Carlo branch of Banca Popolare di Sondrio SUISSE; - Acknowledgement of the amendments to Legislative Decree No. 231/2007 made following the publication of Law No. 136 of October 9, 2023, "*Conversion into law, with amendments, of Decree Law No. 104, on urgent provisions for the protection of users, on economic and financial activities and strategic investments*," implementing the provisions of the *Guidelines on Policies and Controls for the Effective Management of Money Laundering and Terrorist Financing Risks in Providing Access to Financial Services,* published by the *European Banking Authority* (EBA/GL/2023/04), effective November 3, 2023.
04/2024	E2R1	- Revision of the table in paragraph 3.1, item b. "Periodic reports." - Review of attention thresholds (triggers) within the ML/FT risk management of the subsidiary BPS (SUISSE); - Revised Attachment 1 - INTERNAL INFORMATION FLOWS, inserted the Risk Committee as the recipient of flows under 4. Quarterly Group Indicators.

Approval of the document

Prepared by:	**Group Anti-Money Laundering Service**		**26/04/2024**
		[Constantine Tornadu].	**Date**
Approved by:	**Managing Director**		**02/05/2024**
		[Mario Alberto Pedranzini].	**Date**

INDEX

1. INTRODUCTION, REGULATORY BACKGROUND AND OBJECTIVES

1.1. Introduction

Money laundering and terrorist financing are criminal phenomena that, partly because of their possible transnational dimension, pose a serious threat to the economy and can lead to destabilizing effects, especially on the banking and financial system.

The phenomena of money laundering, through the reinvestment of illicit proceeds in legal activities and the presence of economic operators and bodies colluding with crime, profoundly alter market mechanisms, undermine the efficiency and fairness of financial activity and weaken the economic system itself. Terrorist financing activities, on the other hand, involve the allocation for terrorist purposes of funds whose origin may be both licit and illicit.

The changing nature of the threats of money laundering and terrorist financing, also facilitated by the continuous evolution of technology, requires constant adaptation of prevention and countermeasures.

The recommendations of the Financial Action Task Force (hereinafter also referred to as "FATF"), the main international coordinating body in this area, require public authorities and the private sector to identify and assess the money laundering and terrorist financing risks to which they are exposed in order to take appropriate mitigation measures.

Action to prevent and combat money laundering (hereafter also AML) and terrorist financing (hereafter also CTF or CFT) is carried out through the introduction of safeguards aimed at ensuring full customer knowledge, traceability of financial transactions, and detection of suspicious transactions.

The intensity of prevention and countermeasures must be modulated according to a *risk-based* approach (so-called *risk-based approach*), focused on the hypotheses deserving of greater investigation and carried out by making monitoring activities more effective and efficient. Such an approach is the cornerstone for the prevention activities of obligated parties and for the control actions of the competent supervisory authorities.

Banca Popolare di Sondrio (hereinafter also the "bank" or the "Parent Company") and the companies of the Banking Group are strongly committed to preventing the products and services offered from being used for the purposes of money laundering and terrorist financing, promoting within them a culture marked by full compliance with the provisions in force and the effective fulfillment of the obligations of passive cooperation, aimed at ensuring in-depth knowledge of customers, the preservation of documents relating to transactions carried out and active cooperation aimed at identifying and reporting suspicious money laundering transactions. For this reason, the bank and the companies of the Banking Group have adopted this *policy* (hereinafter also the "Document") at the general level as an expression of its commitment to combating the aforementioned criminal phenomena.

The bank reserves absolute commitment to ensure that the operational organization and the system of controls is complete, adequate, functional and reliable, in order to preserve the bank

and the Banking Group from conduct, even unconscious, of tolerance or admixture towards forms of illegality that may damage its reputation and jeopardize its stability. For these reasons, the bank and the Banking Group have equipped themselves with organizational and behavioral rules and monitoring and control systems aimed at ensuring compliance with current regulations by the Administrative and Control Bodies, staff, collaborators and consultants of the Banking Group companies.

1.2. Regulatory background on anti-money laundering and countering the financing of terrorism

AML/CFT legislation is contained in a complex and multifaceted system of sources at the international, EU and national levels.

At the international level, a key contribution in the process of legislative harmonization is made by the FATF, the main body active in combating money laundering, terrorist financing and the proliferation of weapons of mass destruction. The body has prepared a set of *standards*, the so-called "40 Recommendations," adopted in February 2012 and constantly updated, accompanied by "9 Special Recommendations" and "Interpretative Notes."

At the European level, the relevant regulations are contained in Directive (EU) 2015/849 of the European Parliament and of the Council (hereinafter also referred to as "IV Directive"), dated May 20, 2015, which repealed Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, followed by Directive (EU) 2018/843 of the European Parliament and of the Council (the "Fifth Directive"), dated May 30, 2018, which, in amending the previous one, also included providers of foreign exchange services between virtual and legal tender currencies and providers of digital wallet services among the addressees.

The following regulation is also relevant in the same area:

- Regulation (EU) 2015/847 of the European Parliament and of the Council of May 20, 2015 on information accompanying transfers of funds;
- Commission Delegated Regulation (EU) 2016/1675 of July 14, 2016, as amended and supplemented, supplementing Directive IV by identifying high-risk third countries with strategic shortcomings;
- Directive (EU) 2017/541 of the European Parliament and of the Council of March 15, 2017 on combating terrorism and establishing minimum rules relating to the definition of criminal offenses and sanctions in the field of terrorist offenses;
- Commission Delegated Regulation (EU) 2018/1108 of May 7, 2018, supplementing the Fourth Directive with regulatory technical standards on the criteria for the appointment of central contact points for electronic money issuers and payment service providers and rules regarding their functions;
- Regulation (EU) 2018/1672 of the European Parliament and of the Council of October 23, 2018 on controls on cash entering or leaving the European Union;
- Directive (EU) 2018/1673 of the European Parliament and of the Council of October 23, 2018

on combating money laundering by means of criminal law and establishing minimum rules concerning the definition of money laundering offenses and sanctions;

- Regulation (EU) 2018/1805 of the European Parliament and of the Council of November 14, 2018 on the recognition and execution within the European Union of freezing and confiscation orders issued by another member state in the context of criminal proceedings;
- Commission Delegated Regulation (EU) 2019/758 of January 31, 2019 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical standards for minimum action and the type of additional measures to be taken by credit and financial institutions to mitigate the risk of money laundering and terrorist financing in certain third countries.

Primary legislation is also complemented by guidelines that the *European Banking Authority* or EBA publishes periodically, implemented in Italy after a special declaration of compliance by the Bank of Italy, including in particular:

- *Guidelines pursuant to Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence measures and factors that credit and financial institutions should take into account when assessing the risks of money laundering and terrorist financing associated with individual ongoing relationships and occasional transactions ("ML/TF Risk Factor Guidelines")*, repealing and replacing JC/2017/37 Guidelines, dated March 1, 2021;
- *Guidance on policies and procedures on compliance management and the role and responsibilities of the AML officer under Article 8 and Chapter VI of Directive (EU) 2015/849* published by EBA on June 14, 2022.

At the national level, the legislative framework is Legislative Decree No. 231 of November 21, 2007, as amended and supplemented, and Legislative Decree No. 109 of June 22, 2007, as amended and supplemented.

These regulations are supplemented by the provisions of the competent supervisory authorities aimed at fully implementing the AML/CFT regulations defined at the primary level. In particular, they note:

- "Provisions on Organization, Procedures and Internal Controls to Prevent the Use of Intermediaries for the Purposes of Money Laundering and Terrorist Financing" by the Bank of Italy;
- "Customer Due Diligence Provisions for Combating Money Laundering and Terrorist Financing" of the Bank of Italy;
- "Provisions for Keeping and Making Available Documents, Data and Information for Countering Money Laundering and Terrorist Financing," Bank of Italy;
- "Instructions on Objective Reporting" from the Financial Intelligence Unit;
- "Provisions for sending aggregate data" of the Financial Intelligence Unit;
- "Supervisory Provisions on Sanctions and Administrative Sanction Procedure" of the Bank of Italy.

In addition to these provisions, which are of a secondary nature, there are measures and notices from the Bank of Italy and the FIU containing anomaly indicators and patterns of anomalous behavior.

1.3. Regulatory background on embargoes and international financial sanctions

The UN Charter gives the UN Security Council the power to decide, in a manner binding on all members, on restrictive measures designed to promote the maintenance or restoration of international peace and security. The Treaty on European Union and the Treaty on the Functioning of the European Union require member states to take a common position in interrupting or restricting economic and financial relations with one or more third countries. Such measures, which may be imposed against sovereign states, regimes, individual terrorists, terrorist organizations, and entities producing and disseminating weapons of mass destruction, are intended to:

- To safeguard the common values, fundamental interests, independence and integrity of the European Union in accordance with the principles contained in the United Nations Charter;
- Strengthen the security of the European Union;
- Preserve peace and strengthen international security;
- Promote international cooperation;
- Develop and consolidate democracy, respect for the law and human rights and fundamental freedoms.

The relevant legislation for embargo management can be divided into the following categories:

- UN Security Council resolutions;
- European regulations;
- National primary and secondary legislation.

The main legislation issued by the UN can be found in the following sources:

- Resolutions adopted by the Security Council under Article 41 of Chapter VII of the Charter of the United Nations, by which restrictive measures relating to subjects and/or countries are imposed.

The main European legislation is contained in the following measures:

- Council Regulation (EC) 2580/2001 of December 27, 2001 establishing a freezing of funds and a prohibition on the provision of financial services to certain natural persons, legal persons, groups or entities committing or attempting to commit acts of terrorism and to legal persons, groups or entities controlled by them;
- Council Regulation (EC) 881/2002 of May 27, 2002 imposing specific restrictive measures directed against certain persons and entities (listed in the Annex to the Regulation) associated with Usama bin Laden, the Al-Qaeda network and the Taliban;
- Regulation (EU) 2021/821 of the European Parliament and of the Council of May 2021 setting

up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items.

There are, likewise, other sources originating from the international and European context that establish a particular regime of prohibition to invest in certain industries or to import/export from and to certain countries, which are constantly updated.

Italian primary legislation is contained in the following provisions:

- Law No. 185 of July 9, 1990, as amended and supplemented on new regulations on the control of export, import and transit of armament materials;
- Legislative Decree No. 221 of December 15, 2017, as amended and supplemented, which reorganized and simplified the regulation of export authorization procedures for dual-use items and technologies and trade embargo sanctions, as well as for all types of export transactions of proliferating materials[1] .

The main secondary legislation is contained in the following regulatory source issued by the Bank of Italy:

- Provision of May 27, 2009 on operational guidance for the exercise of enhanced controls against the financing of WMD proliferation programs.

Also of relevance is the legislation issued by the U.S. Authorities, contained - in addition to the *U.S. Patriot Act*[2] - in the measures relating to economic and trade sanctions decided from time to time by the U.S. Government, through the *Office of Foreign Asset Control* ("OFAC"), as part of foreign policy and national security choices.

The relevant regulatory framework, which has correlations with that in the area of combating money laundering and terrorist financing, provides for restrictive and sanctioning measures against both governments of third countries and non-state entities, individuals or legal entities in the area of:

- arms embargoes;
- Other specific or general trade restrictions (export and import bans);
- financial restrictions (freezing of assets and resources, prohibitions regarding financial transactions, restrictions regarding export credits or investments);
- penalties on those who finance terrorist or subversive associations and those who engage in export transactions of goods in violation of *dual-use* regulations.

[1] The regulations previously contained in Legislative Decree No. 96 of April 9, 2003, Legislative Decree No. 11 of January 12, 2007, and Legislative Decree No. 64 of May 14, 2009, which have been repealed, were merged into that decree.

[2] *U.S. Patriot Act* (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* - 2001) which, enacted in the wake of the September 11, 2001 terrorist attacks, extended the requirements of the *Bank Secrecy Act* ("BSA" - 1970) by requiring financial institutions to prepare *due diligence* procedures and improving information sharing between financial institutions and the U.S. government.

1.4. Purpose

This Document is prepared in accordance with Articles 15 and 16 of Legislative Decree 231/2007, the "Provisions on Organization, Procedures and Internal Controls to Prevent the Use of Intermediaries for the Purposes of Money Laundering and Terrorist Financing," the "Provisions on Customer Due Diligence for Combating Money Laundering and Terrorist Financing." the "Provisions for the storage and making available of documents, data and information for the purpose of combating money laundering and terrorist financing," issued by the Bank of Italy and the FIU, and the "Guidelines on Policies and Procedures on Compliance Management and the Role and Responsibilities of the AML Officer," issued by EBA. The same defines the guidelines regarding the AML/CFT risk management system of the Parent Company and the Banking Group, in terms of:

- General principles of the risk management model and strategic guidelines;
- responsibilities and duties of corporate bodies and corporate structures, both of the Parent Company and subsidiaries;
- operating procedures for managing the risk of money laundering and terrorist financing in the context of due diligence, *for on-boarding* high-risk customers, for retaining and making available documents, data and information, and for reporting suspicious transactions, reasonably homogeneous at the Group level;
- sharing among the various Group companies, consistent with existing regulatory limitations in foreign jurisdictions, of information useful in assessing the money laundering and terrorist financing risks to which the Banking Group is exposed.

1.5. Responsibility and entry into force of the Document

This Document is approved by the Board of Directors of Banca Popolare di Sondrio after consultation with the Board of Statutory Auditors and is addressed to all employees and collaborators of the bank and its subsidiaries Banca della Nuova Terra Spa, Factorit Spa and Banca Popolare di Sondrio (SUISSE) SA.

The Document is revised at least every two years and, in any case, following significant changes in the relevant regulations, the organizational and governance structures of the Banking Group, and the operations carried out by the individual companies to which it belongs.

Any relevant amendments and/or additions to the Document are approved by the bank's Board of Directors, after consultation with the Board of Statutory Auditors. Where the adjustments are merely reconnaissance of intervening board resolutions or organizational revisions, as well as in the case of further amendments of a purely formal nature, approval is referred to the Managing Director.

Without prejudice to the powers of the Board of Directors in approving any relevant amendments and/or additions to the Document, its update and periodic review shall be prepared by the bank's AML structure and subsequently validated by the Managing Director.

Prior to approval, the Document is submitted to the Audit and Risk Committee for its consideration.

The *policy* or its amendments take effect on the 1st day of the month following the month of approval.

1.6. Addressees of the Document

The head of the Group AML department is assigned the task of disseminating this *policy* to the banking group companies for subsequent approval, according to a principle of proportionality and taking into account local regulations and specificities, by the relevant Bodies with strategic supervisory functions, based on the following scope of application:

- to all Italian companies subject to AML/CFT regulations;
- to banks belonging to the Banking Group that are headquartered abroad, subject to and consistent with applicable local regulations.

The subsidiaries of the Banking Group shall inform the Parent Company of the outcomes of the transposition process of this Document in the manner provided for in the "Management Regulations of Corporate Regulations" dated June 30, 2023 .

The Document is also made available and easily accessible to all employees and associates of both the bank and Banking Group companies, including by posting on their respective company *intranets*.

The transposition of the guidelines and principles contained in this *policy* at the Banking Group level is preparatory to fostering adequate coordination between local AML principals and the Group AML department and ensuring effective circulation of information at the Group level in order to counter the risk of money laundering and terrorist financing.

1.7. Definitions and acronyms

- "*Senior manager*" means a Director or the General Manager or other employee delegated by the Management Body or the General Manager to oversee high-risk customer relationships; the senior manager has appropriate knowledge of the level of money laundering or terrorist financing risk to which the recipient is exposed and has a sufficient level of autonomy to make decisions that can affect this level of risk;
- "*AML*": an acronym, commonly used internationally, for Anti Money Laundering;
- "*Standardized archives*" means archives through which the data and information provided for in the Bank of Italy's "Provisions for the storage and making available of documents, data and information for combating money laundering and terrorist financing" are stored and made available; they include the single computer archives already established as of the effective date of Legislative Decree No. 90 of May 25, 2017;
- "*Sector supervisory authorities" means* the Bank of Italy, CONSOB and IVASS as the national authorities responsible for the supervision and control of banking and financial

intermediaries, and *the European Banking Authority;*

- *"Shell bank" means* a bank or institution that performs similar functions to a bank that does not have a significant organic and management structure in the country in which it is incorporated and licensed for operation, nor is it part of a financial group subject to effective supervision on a consolidated basis;
- *"Customer" means* the person who establishes or has ongoing relationships or performs occasional transactions; in the case of ongoing relationships or occasional transactions co-owned by more than one person, each of the co-owners is considered a customer;
- *"Freezing of funds" means* the prohibition, under EU regulations and national legislation, of the movement, transfer, modification, use or management of funds or access to them, so as to change their volume, amount, location, ownership, possession, nature, destination or any other change that allows the use of funds, including *portfolio* management*;*
- *"Freezing of economic resources" means* the prohibition, under EU regulations and national law, of the transfer, disposition or, for the purpose of obtaining funds, goods or services in any way, use of economic resources, including but not limited to the sale, lease, rent or establishment of security interests;
- *"Correspondent accounts and similar relationships" means* accounts maintained by banks for the settlement of interbank services, used for settlement of transactions on behalf of customers of correspondent institutions;
- "*Pass-through accounts" means* cross-border correspondent banking relationships, held between banking and financial intermediaries, used to carry out transactions in their own name and on behalf of customers;
- *"Line controls":* controls carried out by operational structures (e.g., hierarchical, systematic and spot checks), including through units dedicated exclusively to control tasks that report to the heads of operational structures, or performed as part of the *back office*, incorporated into IT procedures and directed at ensuring the proper conduct of operations;
- *"Risk and compliance controls":* aim to ensure, among other things:
  - The proper implementation of the risk management process;
  - Compliance with the operational limits assigned to the various functions;
  - The compliance of corporate operations with regulations, including self-regulatory regulations;
- "*CTF*": acronym, commonly used internationally, for *Counter* Terrorism Financing, or prevention of the financing of terrorism; alternatively, the acronym CFT - *Combating the Financing of Terrorism* - is also used;
- *"Identifying data" means* the first and last name, place and date of birth, registered residence and domicile, if different from the registered residence, and, where assigned, the tax code or, in the case of entities other than natural persons, the name, registered office and, where assigned, the tax code*;*

- *"Anti-Money Laundering Decree" means* Legislative Decree No. 231 of November 21, 2007, as amended and supplemented;
- *"Anti-Terrorism Decree" means* Legislative Decree No. 109 of June 22, 2007, as amended and supplemented;
- *"Suspicious Transaction Reporting Delegate" means* the person designated by the Strategic Supervisory Board of Banca Popolare di Sondrio to assess suspicious transactions and subsequently transmit them to the Financial Intelligence Unit, if they are deemed to be founded;
- *"Cash" means* banknotes and coins, in euros or foreign currencies, which are legal tender;
- *"Anti-Money Laundering Directive" means* Directive (EU) 2015/849 of the European Parliament and of the Council of May 20, 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, amending Regulation (EU) No. 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC as amended by Directive (EU) 2018/843, of the European Parliament and of the Council of May 30, 2018 *;*
- *"Embargo": a* ban on trade and commerce with sanctioned countries, aimed at isolating and putting their government in a difficult domestic political and economic situation;
- *"Executor" means* the person delegated to act in the name and on behalf of the client or who is otherwise granted powers of representation enabling him/her to act in the name and on behalf of the client;
- *"Exponent responsible for AML":* is appointed by the Board of Directors from among its members; constitutes the main point of contact between the head of the Group AML department, the Board of Directors and the Managing Director in the capacity of the Management Body. He also ensures that the same Bodies have the necessary information to fully understand the significance of the money laundering risks to which the bank is exposed, for the purpose of exercising their respective powers;
- *"Exponent responsible for Group AML":* is appointed by the Board of Directors of the Parent Company from among its members and may coincide with the exponent responsible for AML of Banca Popolare di Sondrio; constitutes the main point of contact between the head of the Group AML service, the Bodies with strategic supervisory and management functions of the Parent Company and ensures that the latter have the information necessary to fully understand the relevance of the money laundering risks to which the Group is exposed, for the purposes of exercising their respective powers. The exponent also ensures that the head of the Group's Anti-Money Laundering Service effectively performs his or her duties;
- *"Financing of terrorism": for* the purposes of Legislative Decree 109/2007, as amended, "financing of terrorism" means any activity directed, by any means, to the provision, collection, provision, intermediation, deposit, custody or disbursement of funds and economic resources, howsoever carried out, intended to be, directly or indirectly, in whole or in part, used for the perpetration of one or more conducts with the purpose of terrorism,

as provided for by criminal laws, this regardless of the actual use of the funds and economic resources for the commission of the aforementioned conducts;

- *"Funds":* financial assets and utilities of any nature, including income derived therefrom, owned, held or controlled, even partially, directly or indirectly, or through nominees, or by natural or legal persons acting on behalf of or at the direction of nominees (such as cash checks, pecuniary credits, bills of exchange, payment orders and other payment instruments, deposits with financial institutions or other entities, balances on accounts, credits and bonds of any kind, publicly and privately tradable securities, financial instruments as defined in Legislative Decree February 24, 1998, no. 58, interest, dividends or other income and increases in value generated by the assets, credit, right of set-off, guarantees of any kind, sureties and other financial commitments, letters of credit, bills of lading and other securities representing commodities, documents showing an interest in funds or financial resources, all other instruments of export financing, insurance policies concerning life insurance, etc.);
- *"Corporate control functions":* the set of functions that by legislative, regulatory, statutory or self-regulatory provision have control tasks. At Banca Popolare di Sondrio these functions coincide with the Compliance function, the Group Anti-Money Laundering service, the Risk Control service and the Internal Audit service;
- *"Banking Group" means* the Banca Popolare di Sondrio Banking Group pursuant to Article 60 et seq. of Legislative Decree No. 385 of September 1, 1993 ("Consolidated Banking Act" or "TUB"), as amended and supplemented, consisting of the Parent Company and subsidiaries;
- *"Community banking and financial intermediaries" means those* entities referred to in Article 3(1) and (2) of the "AML Directive" that are based in an EU country;
- *"Means of payment" means* cash, bank and postal checks, cashier's checks and other checks assimilated or equivalent thereto, money orders, credit or payment orders, credit cards and other payment cards, transferable insurance policies, pledge policies, and any other instrument available to transfer, move or acquire, including by electronic means, funds, valuables or financial assets;
- *"Transaction" means the* activity consisting in the movement, transfer or transmission of means of payment or in the performance of negotiation acts with patrimonial content; the conclusion of a negotiation act, with patrimonial content, falling within the exercise of professional or commercial activity also constitutes a transaction;
- *"Fractional transaction" means* a unitary transaction in terms of economic value, of an amount equal to or greater than the limits established by the AML Decree, carried out through several transactions, individually lower than the aforementioned limits, carried out at different times and within a circumscribed period of time fixed at seven days, without prejudice to the existence of the fractional transaction when there are elements to consider it as such;
- *"Occasional transaction" means* a transaction that cannot be attributed to an existing ongoing relationship; an intellectual or commercial service, including those with instantaneous execution, rendered in favor of the customer also constitutes an occasional transaction;
- *"Suspicious transaction":* A transaction that by its characteristics, magnitude, nature and by its

connection with other transactions or by splitting of the same or by any other circumstance known by reason of the functions exercised, taking into account also the economic capacity and activity carried out by the person to whom it is referred, on the basis of the elements acquired in accordance with the anti-money laundering decree, leads to the belief, suspicion or reasonable grounds for suspecting that money laundering or terrorist financing transactions are being or have been carried out or attempted, or that in any case the funds, regardless of their magnitude, come from criminal activity;

- *"Related transactions" means* transactions related to each other in pursuit of a single objective of a capital legal nature;
- *"Corporate bodies" means* the set of bodies with strategic supervision, management and control functions*;*
- *"Supervisory Body" means* the Body established pursuant to Legislative Decree No. 231 of June 8, 2001;
- *"Body with control function":* the corporate body which is assigned, among other things, the responsibility for supervising the completeness, adequacy, functionality and reliability of the system of internal controls. At Banca Popolare di Sondrio, the Body with control function is represented by the Board of Statutory Auditors;
- *"Body with management function" means* the corporate body or its members to which management tasks are assigned or delegated, i.e., the implementation of the policies resolved in the exercise of the strategic supervision function. At Banca Popolare di Sondrio this body is represented by the Managing Director;
- *"Body with strategic supervisory function":* the Body in which the functions of direction and/or supervision of corporate management are concentrated (e.g.: through examination and deliberation regarding the company's industrial and/or financial plans and/or strategic operations). At Banca Popolare di Sondrio, the Strategic Supervisory Body is represented by the Board of Directors;
- "*Community countries*" means countries belonging to the European Economic Area;
- *"Third countries" means* countries outside the European Economic Area;
- *"High-risk third countries" means* non-European Economic Area countries whose systems have strategic deficiencies in their national AML/CFT regimes, as identified by the European Commission in the exercise of powers regulated by Articles 9 and 64 of the AML Directive;
- *"Personnel" means* employees and those who otherwise work on the basis of relationships that result in their inclusion in the organization of the obligor, including in a form other than an employment relationship;
- *"Politically exposed persons" (or PEPs):* natural persons who occupy or have ceased to occupy important public office for less than one year, their family members, and those known to have close ties with the aforementioned persons, as listed below:
  - Individuals who hold or have held important public office are those who hold or have held the office of:

  - President of the Republic, Prime Minister, Minister, Vice-Minister and Undersecretary, Regional President, Regional Councillor, Mayor of provincial capital or metropolitan city, Mayor of municipality with a population of not less than 15,000 and similar offices in foreign states;
  - congressman, senator, European parliamentarian, regional councilor and similar offices in foreign states;
  - Member of central governing bodies of political parties;
  - judge of the Constitutional Court, magistrate of the Court of Cassation or the Court of Auditors, state counselor and other members of the Council of Administrative Justice for the Sicilian Region and similar positions in foreign states;
  - Member of the governing bodies of central banks and independent authorities;
  - ambassador, chargé d'affaires or equivalent positions in foreign states, senior officer in the armed forces or similar positions in foreign states;
  - member of the administrative, management or control bodies of enterprises controlled, even indirectly, by the Italian state or a foreign state or participated, predominantly or wholly, by regions, provincial capitals and metropolitan cities and municipalities with a total population of not less than 15,000 inhabitants;
  - general manager of ASL and hospital corporation, university hospital corporation and other entities of the national health service;
  - director, deputy director and member of the management body or person performing equivalent functions in international organizations;
- are family members of politically exposed persons: the parents, spouse or person related in civil union or de facto cohabitation or similar institutions to the politically exposed person, children and their spouses and persons related to the children in civil union or de facto cohabitation or similar institutions;
- are individuals with whom politically exposed persons are known to have close ties:
  - individuals who, in accordance with the Anti-Money Laundering Decree, jointly with the politically exposed person hold beneficial ownership of legal entities, *trusts* and related legal institutions or have close business relations with the politically exposed person;
  - individuals who only formally hold totalitarian control of an entity known to be established, in fact, in the interest and for the benefit of a politically exposed person;
- *"Local Italian Politicians" (or PILs)*: individuals who, while not PEPs, operate in contexts closely related to local political life and who, therefore, present a higher potential risk of money laundering, identified by the bank in the following figures: provincial president, provincial alderman and municipal alderman, mayor of municipalities with a population of less than 15,000;
- *"Providers of services related to companies and trusts" means* any natural or legal person who

provides any of the following services to third parties in a professional capacity:

- Establish companies or other legal entities;
- occupy the function of an officer or director of a company, a member of an association, or a similar function with respect to other legal persons, or arrange for another person to occupy such a function;
- To provide a registered office, business, administrative or postal address and other related services to a company, association or any other legal entity;
- perform the function of a trustee in an express *trust* or related legal institution or provide for another person to fill that function;
- exercising the role of shareholder on behalf of another person or arranging for another person to perform this function, provided that the company is not a company listed on a regulated market and subject to disclosure requirements in accordance with European Union or equivalent international standards;

- " *Providers of services related to the use of virtual currency* ": any natural or legal person who provides third parties, on a professional basis, including *online*, with services functional to the use, exchange, storage of virtual currencies and their conversion from and/or into legal tender currencies or into digital representations of value, including those convertible into other virtual currencies as well as the services of issuing, offering, transferring and clearing and any other service functional to the acquisition, trading or intermediation in the exchange of the same currencies;
- " *Digital Wallet Service Providers* ": any natural or legal person who provides, to third parties, in a professional capacity, including *online*, private cryptographic key safeguard services on behalf of its clients in order to hold, store and transfer virtual currencies;
- *"Relationships similar to pass-through accounts" means* relationships however denominated held between banking and financial intermediaries on which the customer of the correspondent institution is given the authority to directly execute even part of the transactions pertaining to him;
- *"Continuous relationship" means* a relationship of duration, falling within the scope of the establishment activity carried out by the obligated persons, which does not end in a single transaction*;*
- *"Correspondent relationships" means* accounts maintained by banks for the settlement of interbank services (remittances of bills, bank and cashier's checks, deposit orders, rounds of funds, documented remittances, and other transactions) as well as relationships, however denominated, maintained between banking and financial intermediaries used for the settlement of transactions on behalf of customers of respondent institutions (e.g., securities deposit, investment services, foreign exchange transactions, document collection services, issuance or management of debit or credit cards);
- *"Money laundering": for* the purposes of Legislative Decree 231/2007, as amended, money laundering means:

- the conversion or transfer of property, carried out with knowledge that it is derived from criminal activity or participation in such activity, for the purpose of concealing or disguising the illicit origin of such property or assisting anyone involved in such activity to evade the legal consequences of their actions;
- Concealment or concealment of the true nature, origin, location, disposition, movement, ownership of property or rights to the same, carried out with knowledge that such property is derived from criminal activity or participation in such activity;
- The purchase, possession, or use of goods being aware, at the time of their receipt, that they are derived from criminal activity or participation in such activity;
- participation in any of the acts referred to in the preceding paragraphs, association to commit such an act, attempt to perpetrate such an act, aiding, instigating or advising anyone to commit such an act, or facilitating the commission of such an act.

Self-laundering also falls under this definition, where the launderer coincides with the person who committed the predicate offense;

- *"Money Laundering and Terrorist Financing Risk" means* the risk arising from the violation of legal, regulatory and self-regulatory provisions functional to the prevention of the use of the financial system for the purpose of money laundering, terrorist financing or financing of WMD development programs, or the risk of involvement in money laundering, terrorist financing or financing of WMD development programs;
- *"Risk Appetite Framework":* the framework that defines-consistent with the maximum risk that can be taken, the *business model,* and the strategic plan-the risk appetite, tolerance thresholds, risk limits, risk governance policies, and the reference processes needed to define and implement them;
- *"Economic resources" means* assets of any kind, whether tangible or intangible, and movable or immovable property, including accessories, appurtenances and fruits, which are not funds but which can be used to obtain funds, goods or services, owned, held or controlled, even partially, directly or indirectly, or through intermediaries, by designated persons, or by natural or legal persons acting on behalf of or at the direction of such persons;
- *"System of internal controls" means* the set of rules, functions, structures, resources of processes and procedures that aim to ensure, in accordance with sound and prudent management, the following purposes:
  - Verification of the implementation of corporate strategies and policies;
  - risk containment within the limits specified in the framework for determining the bank's risk appetite;
  - Safeguarding asset value and protecting against losses;
  - effectiveness and efficiency of business processes;
  - Reliability and security of business information and computer procedures;
  - Prevention of the risk of the bank being involved, even unintentionally, in illegal activities

(with particular reference to those related to money laundering, usury, and terrorist financing);

- compliance of operations with the law and supervisory regulations, internal policies, regulations and procedures;

- *"Designated persons" means* the natural persons, legal persons, groups and entities designated as recipients of the freeze on the basis of EU regulations, UN resolutions and national legislation;
- *"Operational Structures" means* the bank's territorial branches; they represent the first and essential level of corporate supervision for the purposes of preventing and combating money laundering and terrorist financing, which are concretely responsible for the administration and management of customer relations;
- *"Beneficial Owner."*
  - the natural person or persons on whose behalf the customer establishes an ongoing relationship or carries out a transaction (in short, "*sub* 1 beneficial owner");
  - in the case where the customer and/or the entity on whose behalf the customer establishes an ongoing relationship or carries out a transaction are entities other than a natural person, the natural person(s) who ultimately is attributable direct or indirect ownership of the entity or control over it or who are its beneficiaries (in short, "beneficial owner *sub* 2"). In particular, in the case of corporations or other private legal entities, even if based abroad, and express *trusts*, regardless of their place of establishment and the law applicable to them, the beneficial owner *sub* 2) is identified according to the criteria set forth in Articles 20 and 22, paragraph 5, of Legislative Decree 231/2007; the same criteria, apply, to the extent compatible, in the case of partnerships and other legal entities, public or private, even if without legal personality;
- *"Bearer security" means a* security that entitles the holder to exercise the right mentioned in it based on mere presentation and whose transfer is effected by delivery of the security;
- "FIU" *means* the Financial Intelligence Unit for Italy, established at the Bank of Italy;
- *"Virtual currency" means* the digital representation of value, not issued or guaranteed by a central bank or public authority, not necessarily linked to a legal tender, used as a medium of exchange for the purchase of goods and services or for investment purposes, and transferred, stored and traded electronically.

2. ROLES AND RESPONSIBILITIES OF BODIES, FUNCTIONS AND CORPORATE STRUCTURES

2.1. Body with strategic oversight function (OFSS)

The OFSS, i.e., the Board of Directors, approves and periodically reviews the strategic directions and policies for governing AML/CFT risks and is responsible for oversight and implementation in the *governance* and internal control environment. The OFSS must collectively possess adequate knowledge, skills, and experience to understand the AML/CFT risks related to the bank's activities and *business* model, including knowledge of the relevant legal/regulatory framework.

Within this framework, the Board of Directors:

- approves a specific anti-money laundering *policy*, which explains and justifies the choices that the bank and the Group intend to make on the various relevant profiles of organizational structures, procedures and internal control, as well as on customer due diligence and data retention in order to assess consistency with actual exposure to money laundering risk;
- Approves the guidelines of the organic and coordinated internal control system functional for the detection and management of money laundering risk and ensures its effectiveness over time;
- Decides on the establishment, arrangement, reconfiguration and/or abolition of the Group AML department, identifying its duties and responsibilities, as well as coordination arrangements with other control functions and AML structures of subsidiaries;
- Approves principles for managing relationships with customers classified as "high risk," specifying possible types of customers with whom the bank should not deal;
- deliberates, after hearing the Body with control function, on the appointment and/or revocation of the head of the anti-money laundering function of Banca Popolare di Sondrio and his deputy; the verification of the possession of the requirements of the head must be reported analytically in the minutes of appointment;
- deliberates, after consultation with the Body with control function, the appointment and/or revocation of the Group AML officer and his deputy; the verification of the officer's possession of the requirements must be analytically reported in the appointment minutes;
- ensures the allocation of tasks and responsibilities in a clear and appropriate manner, ensuring separation between operational structures and control functions;
- ensures a system of adequate, complete and timely information flows to the Corporate Bodies and between the control functions, as well as a system of documentation sharing that allows the Corporate Bodies direct access to the reports of the control functions on anti-money laundering matters, relevant communications exchanged with the Authorities and supervisory measures imposed or sanctions imposed;
- Ensures that the identity of the reporter of a suspicious transaction is protected;

- at least twice a year, reviews the reports of the activity carried out by the head of the Group AML department and the controls carried out by the relevant functions, as well as the document on money laundering risk assessment;
- assesses, at least once a year, the effective functioning of the Group AML service, taking into account, among other things, the conclusions of any internal and external reviews that may have been carried out, including on the adequacy of the human and technical resources assigned to the head of the Group AML service, engaging, where appropriate, the Personnel and Organizational Models service for the relevant reviews;
- ensures that any anomalies or deficiencies found as a result of the second-level controls are immediately brought to its attention and takes the resulting corrective measures, the effectiveness of which it assesses;
- assesses risks related to operations with third countries considered to be at "high risk" of money laundering, identifying safeguards to mitigate them, and monitors their effectiveness;
- appoints the representative responsible for anti-money laundering of both the Parent Company and the Group and ensures that they meet the conditions set forth in the *Bank of Italy Provisions on Organization, Procedures and Internal Controls for Anti-Money Laundering Purposes,* as well as the Ministry of Economy and Finance Decree No. 169 of November 23, 2020[3] . The relevant assessments must be minuted in an analytical manner;
- ensures that the individual appointed as the AML officer is promptly informed of decisions that may affect the bank's AML exposure.

The OFSS has direct and timely access to the reports of the Group AML manager and the Internal Audit department, the conclusions and observations of any external auditors in the AML/CFT area, as well as the communications or findings of the competent authorities and any measures or sanctions imposed by them.

2.2. Exponent responsible for anti-money laundering (of the bank and Group)

Without prejudice to the collective responsibility of the corporate bodies, the Board of Directors, while retaining responsibility for approving the bank's and the Group's overall AML/CTF strategy and overseeing its implementation, appoints one member from among its members as the AML officer. The appointment is executive in nature.

The position of anti-money laundering officer may be attributed to a director without delegated powers (so-called non-executive) who, as a result of this appointment, acquires the status of executive director and, as such, must comply with the suitability requirements for this role. It can also be attributed to the managing director; in any case, it is necessary to verify compliance with the requirements of the regulations and to consider possible situations of conflict of interest.

[3] "*Regulation on the requirements and criteria for eligibility to hold office of corporate officers of banks, financial intermediaries, confidiums, electronic money institutions, payment institutions and depositor guarantee schemes*."

The anti-money laundering officer may not delegate his duties to third parties.

Such a subject:

a) possesses adequate knowledge, skills, and experience concerning AML/CFT risks, policies, controls, and procedures, as well as the bank's *business* model and related area of operation;
b) has adequate time and resources to carry out its tasks effectively.

The Anti-Money Laundering Officer is the main point of contact between the Group Anti-Money Laundering Officer, the Board of Directors and the Managing Director in his capacity as the Body with management function. He or she also ensures that the same Bodies have the necessary information to fully understand the significance of the money laundering risks to which the bank is exposed, for the purpose of exercising their respective powers.

When appointing the AML/CFT officer, the bank must identify and consider potential conflicts of interest, as well as take measures to prevent or mitigate them. In any case, the provisions of the "*Regulations on the Control of the Independence Requirements of Directors*" approved by the Board of Directors on January 19, 2024 shall apply, including with regard to measures to prevent and mitigate conflicts of interest.

With regard to the verification regarding the availability of time necessary for the effective performance of the assignment, the provisions of Ministerial Decree of November 23, 2020, No. 169 ("*Regulations on the requirements and criteria for eligibility for the performance of the assignment of corporate officers of banks, financial intermediaries, confidiums, electronic money institutions, payment institutions and depositor guarantee systems*") apply.

The exponent responsible for AML:

a) Monitors that AML policies, procedures and internal control measures are adequate and proportionate, taking into account the bank's characteristics and the ML/TF risks to which it is exposed;
b) assists the Board of Directors in evaluations concerning the organizational structure and resource allocation of the Group AML service, including the possible choice of assigning responsibility for this service to the same officer responsible for AML;
c) ensures that the Corporate Bodies are periodically informed about the activities carried out by the head of the Group AML service, as well as about the interlocutions held with the Authorities;
d) informs the Corporate Bodies of violations and critical issues concerning AML of which it has become aware and recommends appropriate action;
e) verifies that the head of the Group AML department has direct access to all information necessary for the performance of his or her duties, has sufficient human and technical resources and tools, and is informed of any AML-related deficiencies identified by other internal control functions and supervisory authorities;
f) ensures that issues and proposals for action represented by the Group AML Manager are evaluated by the Managing Director.

Similarly, the Board of Directors of each Italian component of the Group to which the "Provisions on Organization, Procedures and Internal Controls to Prevent the Use of Intermediaries for the Purposes of Money Laundering and the Financing of Terrorism" apply, appoints from among its members its own person in charge of AML, with similar procedures, requirements and duties as those mentioned above.

The Board of Directors of the Parent Company also appoints a member as the representative responsible for Group AML, who must meet the same eligibility requirements as the representative responsible for AML of the Parent Company and may coincide with the same. The duties of the exponent responsible for Group AML are set out in paragraph 3 below (*Banking Group AML/CFT Risk Management Model*).

2.3. Body with management function (OFG)

The OFG, in the person of the Managing Director:

- oversees the implementation of the strategic guidelines and policies for governing the risk of money laundering approved by the Board of Directors and is responsible for the adoption of all actions necessary to ensure the effectiveness of the organization and the system of anti-money laundering controls; to this end, it examines the proposals for organizational and procedural actions submitted by the head of the Group AML department and formalizes, giving reasons, any decision not to accept them;
- oversees the establishment of a functional system of internal controls for the prompt detection and management of AML/CTF risk and ensures its effectiveness over time, consistent with the evidence drawn from the AML/CTF risk self-assessment exercise;
- Ensures that operational procedures and information systems enable the proper fulfillment of customer due diligence and document and information retention requirements;
- in the area of suspicious transaction reporting, defines and takes care of the implementation of a procedure appropriate to the specifics of the bank's business, size and complexity, which guarantees reference certainty, homogeneity in behavior, generalized application to the entire structure, full use of all relevant information and the reconstructability of the evaluation process; it also adopts measures to ensure compliance with the confidentiality requirements of the reporting procedure as well as tools, including computer tools, for the detection of anomalous transactions;
- defines and oversees the implementation of the initiatives and procedures necessary to ensure the timely fulfillment of reporting obligations to the Authorities under the AML regulations;
- Validates the AML *policy* submitted to the Board of Directors for approval and ensures its implementation;
- defines information flows that ensure knowledge of risk factors to all involved company structures and supervisory bodies;
- defines and oversees the implementation of procedures for managing relationships with customers classified as "high risk," consistent with the principles set by the Strategic

Oversight Board;

- Establishes appropriate tools to enable the verification of the activities carried out by staff so as to detect any anomalies that emerge, namely, in behavior, the quality of communications addressed to contact persons and corporate structures as well as in staff relations with customers;
- ensures, in cases of outsourcing the operational tasks of the AML function, compliance with applicable regulations and receives periodic information on the performance of outsourced activities;
- ensures, in cases of remote operations, the adoption of specific IT procedures for compliance with anti-money laundering regulations, with particular reference to the automatic detection of anomalous transactions.

The Managing Director acts in cooperation with the Audit and Risk Committee and reports to the Board of Directors on initiatives and actions needed to ensure the completeness, adequacy, functionality and reliability of the system of internal controls and risk governance on an ongoing basis.

In cooperation with the Group Anti-Money Laundering Service and the Personnel and Organizational Models Service, it establishes programs to train and educate personnel on their obligations under AML regulations on a continuous and systematic basis.

2.4. Body with Control Functions (OFC)

The OFC, i.e., the Board of Statutory Auditors, monitors compliance with regulations and the completeness, functionality, and adequacy of anti-money laundering control systems. In this regard, the Board of Statutory Auditors:

- makes use of internal facilities to carry out the necessary checks and verifications;
- uses information flows from other corporate bodies, the head of the Group AML department and other corporate control functions;
- assesses the suitability of procedures for customer due diligence, retention, documents, data and information, and suspicious transaction reporting;
- analyzes the reasons for the deficiencies, anomalies and irregularities found and promotes the adoption of appropriate corrective measures.

He is also heard on decisions to appoint the head of the Group AML department, the deputy head of the Group AML department, the head of STRs and the deputy head of SOS, and in defining the elements of the overall architecture of the AML/CFT risk management and control system.

Pursuant to Article 46 of the Anti-Money Laundering Decree, members of the Body with Control Function shall report without delay to the Bank of Italy all facts of which they become aware in the performance of their duties that may constitute serious or repeated or systematic or multiple violations of applicable legal provisions and their implementing provisions.

2.5. Supervisory body

The Supervisory Board (SB) established pursuant to Legislative Decree 231/01 continuously monitors compliance with the processes set forth in the adopted Organization, Management and Control Model.

In the event that a predicate offense is nevertheless committed, it analyzes its causes in order to identify the most suitable corrective measures. To carry out these activities, the Supervisory Board receives appropriate information flows from the various structures and/or functions of the company and has unrestricted access to all data and information relevant to the performance of its duties.

Finally, the Supervisory Board forwards any suspicious transaction reports it detects independently in the course of its duties to the SOS manager.

2.6. Internal Audit Service

In the area of preventing and combating money laundering and terrorist financing, the Internal Audit Department is responsible for verifying the adequacy of the company's organizational structure with respect to the relevant regulations, as well as supervising the functionality of the overall system of internal controls.

The Internal Audit Department periodically reviews the adequacy and effectiveness of the functions performed by the Group AML Department.

The service verifies through systematic checks, including inspections:

- compliance with the duty of due diligence, both at the stage of establishing the relationship and as the relationship develops over time;
- The effective acquisition and orderly storage of documents, data and information;
- The degree of effective involvement of staff as well as the heads of central and peripheral structures, in the implementation of the communication and reporting obligation.

Interventions, both inspectional and remote, are subject to planning according to a *risk-based* logic in order to allow the intensity of audits to be greater for operational structures deemed more exposed to the risk of money laundering and terrorist financing, and for all operational structures to be subject to assessment over a reasonable period of time.

It also carries out *follow up* actions to verify the adoption of the corrective actions envisaged for any anomalies found, and reports, at least annually or as part of its periodic *reporting*, to the corporate bodies information on the activities carried out and their outcomes, subject to compliance with the confidentiality obligations provided for in the anti-money laundering decree.

Finally, the head of the Parent Company's Internal Audit department oversees the activities of the Internal Audit functions present in the subsidiaries to ensure homogeneity in controls and adequate attention to the different types of risks, including those attributable to non-compliance with the legislative provisions on preventing and combating money laundering and terrorist financing.

2.7. Group Anti-Money Laundering Service

The Group AML service is internally divided into:

- AML office of BPS;
- Group AML office.

The Group AML service:

1) at least twice a year, prepare a Group-wide ML/TF risk assessment. In this regard, the Parent Company must take into account, in its ML/TF risk management system, both the individual risks of the various Group entities and their possible interrelationships that could significantly affect risk exposure at the Group level. Particular attention should be paid in this context to the risks faced by Group companies established in third countries, particularly if they are at high ML/TF risk;
2) establishes AML/CTF policies and procedures, as well as the controls and systems to be applied under Article 8(4) of Directive (EU) 2015/849;
3) establishes AML/CFT *standards* at the Group level and ensures that local policies and procedures at the individual entity level comply with the AML/CFT laws and regulations applicable individually to each Group entity and are also in line with the *standards* established at the Group level;
4) establishes Group-wide policies, procedures and measures regarding, in particular, data protection and information sharing within the Group for AML/CFT purposes, in accordance with national legal provisions;
5) ensures that Group entities have adequate suspicious transaction reporting procedures in place and share information properly, including notification that a suspicious transaction report has been submitted (subject to limitations under national regulations);
6) prepares and transmits to the Managing Director, the Board of Statutory Auditors, the *Chief Risk Officer* and the Head of Internal Audit specific Group indicators, useful for highlighting and monitoring the trend of the main AML/CFT risk indicators, prepared on the basis of data provided by the individual components of the Group.

The Group AML department reports-directly or through the representative responsible for AML-to the Board of Directors, the Managing Director, the Board of Statutory Auditors, and has access to all the bank's activities, as well as any information relevant to the performance of its duties.

Personnel called to work with the Group AML service, even if they are placed in operational areas, report directly to the head of the service for matters pertaining to their duties.

Annex 1 (Internal Information Flows) details the cases in which the Group AML department reports to the Corporate Bodies directly or through the representative responsible for AML. In any case, the Group AML department may report directly in case of significant violations and deficiencies.

2.8. Group head of anti-money laundering service

The head of the Group Anti-Money Laundering Service is appointed by the Board of Directors - after consultation with the Board of Statutory Auditors, on the recommendation of the Audit and Risk Committee and with input from the Appointments Committee.

The same shall, likewise pursuant to Article 20 of Ministry of Economy and Finance Decree No. 169 of November 23, 2020:

1) Be in possession of appropriate independence, competence, professionalism and reputational requirements, honesty and integrity;
2) must be provided with adequate time and resources in order to carry out their duties effectively;
3) must have sufficient decision-making power to operate effectively for ML/TF risk management and prevention purposes, in accordance with the principle of proportionality and applicable legislation;
4) must possess adequate knowledge, skills and experience concerning AML/CTF risks, policies, controls and procedures, and the Group-wide *business* model.

The same falls within the group of heads of corporate control functions, so he is placed in an appropriate hierarchical - functional position, does not have direct responsibility for operational structures and is not hierarchically dependent on individuals responsible for said areas. He reports to the Corporate Bodies of the Parent Company, either directly or through the representative responsible for anti-money laundering, in accordance with Annex 1 and reports hierarchically to the Managing Director.

In the event of absence or impediment, the duties of the head of the Group AML department shall be performed by a delegate, appointed by the Board of Directors of the Parent Company, as provided in Section 2.1. The appointed delegate must possess adequate skills and experience to assume the duties of the manager in the above cases.

At least twice a year, the head of the Group Anti-Money Laundering Service prepares and transmits - directly or through the person responsible for anti-money laundering in accordance with Annex 1 - to the Board of Directors, the Managing Director and the Board of Statutory Auditors a report, including a Group report, on the initiatives taken, the anomalies ascertained and the relevant corrective actions to be taken, as well as on staff training activities. The report also incorporates the results of the group self-assessment exercise, in the manner indicated in Section 5.

The report of the head of the Group AML department must include at least the following points, based on the data reported by the AML officers of individual banking group companies:

a. consolidated Group-wide statistics concerning, in particular, risk exposure and suspicious transaction reports;
b. monitoring of inherent risks that have occurred in one or more Group companies and an analysis of the impact of residual risks;
c. supervisory reviews, internal or external audits, including serious deficiencies identified

in the Group's AML/CFT policies and procedures, as well as actions or recommendations for corrective measures;

d. Information on supervision and supervision of subsidiaries and branches located in high-risk countries, if any.

With regard to information flows to and from the individual AML structures of the individual Group components and to and from the corporate bodies, these are detailed in Appendices 1 and 2 ("Internal Information Flows" and "Intra-Group Information Flows").

The bank shall transmit to the Bank of Italy, within twenty days of the relevant resolution, the decision to appoint or dismiss the head of the Group AML department.

2.9. Office AML of BPS

The AML office of BPS (Banca Popolare di Sondrio) falls within the second level of the internal control system, reports through the head of the Group AML department to the Bodies with strategic supervision, management and control functions, and has access to all the bank's activities, as well as to any information relevant to the performance of its duties.

The office appears to be qualitatively and quantitatively resourced for the tasks to be performed.

Personnel performing tasks attributable to the AML office of BPS are adequate in number, technical and professional skills, and up-to-date, including through training programs on an ongoing basis.

BPS's AML office verifies on an ongoing basis that the company's procedures are consistent with the objective of preventing and countering the violation of AML/CFT regulations. Specifically:

- Identifies applicable standards and assesses their impact on internal processes and procedures;
- Collaborates in defining the system of internal controls and procedures aimed at preventing and countering money laundering risks;
- verifies on an ongoing basis the adequacy of the risk management process and the suitability of the system of internal controls and procedures, and proposes organizational and procedural changes to ensure adequate risk management;
- conducts, through its manager, in liaison with other relevant business functions, the annual self-assessment exercise of the money laundering risks to which the bank is exposed, as outlined in Paragraph 5, to be forwarded to the head of the Group AML department;
- submits annually, through the service manager, to the Board of Directors a plan of activities, including both the second-level controls to be carried out and any organizational and/or technical/IT interventions necessary to strengthen the safeguards in the areas of customer due diligence, suspicious transaction reporting, and retention of data, information, and documents;
- recommends to the Body with management function the corrective measures to be taken to remedy any weaknesses detected, including by the Competent Authority and Internal Audit;

- conducts checks on the functionality of the reporting process and the appropriateness of the assessments made by the first level on customer operations;
- collaborates in the establishment of policies to govern money laundering risk and the various steps involved in the process of managing this risk;
- Provides support and assistance to corporate bodies and senior management;
- assesses on a preventive basis the money laundering risk associated with offering new products and services, making significant changes to products or services already offered, entering a new market, or initiating new activities, and recommends measures to mitigate and manage possible risks;
- verifies the reliability of the information system for fulfilling customer due diligence obligations, storing and making available documents, data and information, and reporting suspicious transactions;
- submits aggregate data concerning overall operations to the FIU on a monthly basis, according to the "Provisions for sending aggregate data" published by the FIU on August 25, 2020;
- Transmits to the FIU, based on the instructions issued by the FIU, objective communications concerning money laundering risk transactions;
- defines, in agreement with the person in charge of suspicious transaction reports, procedures for handling internal reports (from the so-called "first level") concerning particularly high-risk situations to be treated with due urgency;
- takes care, in cooperation with the relevant corporate functions, of the preparation of an appropriate training plan, aimed at achieving refresher training on an ongoing basis for employees and collaborators and indicators of the effectiveness of the training activities carried out;
- promptly informs, through the head of the service, the corporate bodies of significant violations or deficiencies found in the performance of relevant duties;
- periodically informs the Corporate Bodies - either directly or through the person responsible for AML in accordance with Annex 1 - about the progress of the corrective actions taken against deficiencies found in control activities and about the possible inadequacy of the human and technical resources assigned to the AML function and the need to strengthen them;
- Prepares direct information flows to corporate bodies, the anti-money laundering officer and senior management;
- performs enhanced customer due diligence in connection with special circumstances-objective, environmental or subjective-where the risk of money laundering is particularly high;
- makes notifications of infringements under Article 49 of Legislative Decree 231/2007 to the Ministry of Economy and Finance.

The AML department of BPS prepares a document that defines in detail responsibilities, tasks and operating procedures in the management of money laundering risk (so-called "AML manual"). It, after being validated by the head of the Group AML department, is forwarded by the latter to the Managing Director and the Board of Directors.

In assessing the adequacy of internal procedures for preventing and countering money laundering risk, the AML office of BPS, also in conjunction with the Internal Audit Department, may conduct on-site audits to verify their effectiveness and functionality.

Further details on the attributions of the AML office of BPS can be found in the appropriate "Regulations of the AML office of BPS."

2.10. Office manager AML of BPS.

The head of BPS's AML office is appointed by the Board of Directors after consultation with the Board of Statutory Auditors, on the recommendation of the Audit and Risk Committee and with the input of the Appointments Committee, and is found to possess adequate requirements of independence, authority and professionalism.

Before appointment, it should be verified that the same is in possession of:

a) adequate reputational profile, honesty and integrity necessary to perform their function;
b) appropriate skills and experience in AML/CFT, including knowledge of the applicable legal framework and in the implementation of policies, controls, and procedures in this area and in the identification, assessment, and management of ML/FT risks;
c) Sufficient knowledge and understanding of the ML/FT risks associated with the bank's *business* model to enable it to effectively fulfill its function;
d) Adequate experience in identifying and managing ML/TF risks;
e) adequate time and hierarchical position to perform their functions effectively, independently and autonomously.

If the same is entrusted with other assignments, the department head must assess potential conflicts of interest and propose specific measures to prevent or manage them to the Managing Director. In addition, if there are other assignments, the head of the AML office must be able to devote sufficient time to the performance of his or her duties.

The head of the AML office of BPS:

- for the purpose of identifying and considering risks, supports the service manager in developing a ML/TF risk assessment framework for analysis at the individual relationship and business area level, in line with Bank of Italy regulations and EBA Risk Factor Guidelines;
- supports the service manager in the development of AML/CTF policies and procedures to be implemented by the bank and keeps them up-to-date, including in relation to changes in laws or regulations;

- communicates, either directly or through the person responsible for AML in accordance with Annex 1, the findings of the risk assessment on an individual or business area basis to the Board of Directors;
- assesses ML/FT risks pertinent to the introduction of new products or services or major changes to existing products or services, the development of a new market, or the start-up of new activities;
- Proposes ways to address any changes in legal or regulatory requirements or ML/CTF risks that are necessary to address any gaps or deficiencies identified through the monitoring activity;
- must be consulted by senior management prior to the decision to accept new high-risk clients or on the maintenance of such relationships, especially in cases where senior management approval is expressly required under Directive (EU) 2015/849 and the AML Decree;
- Supervises the effective implementation of controls by *business* lines and internal units (so-called first level);
- submits-directly or through the person responsible for AML-to the Board of Directors corrective measures to be taken to remedy weaknesses, including those found by the competent authorities, external auditors and the Internal Audit function;
- periodically informs - either directly or through the representative responsible for AML - the Managing Director about the progress of the measures adopted or recommended and, where appropriate, the possible inadequacy of the human and technical resources assigned to the AML office of BPS and the consequent need to strengthen them.

The head of BPS's AML office may assign and delegate his or her duties to other employees working under his or her direction and supervision, but remains ultimately responsible for the effective performance of those duties.

Where the head of BPS's AML office works for two or more Group entities and/or is entrusted with other functions, he or she must be put in a position to perform his or her duties effectively.

2.11. Group AML Office

The Group AML office reports hierarchically to the head of the Group AML department and is qualitatively and quantitatively resourced to the tasks to be performed.

The heads of the AML function, or similar structures, of each subsidiary may communicate directly with the head of the Group AML office.

Group AML office:

- constitutes a coordinating unit for all Group companies to implement Group policy and adopt adequate and appropriate systems and procedures for effective ML/TF prevention, consistent with the Group structure and the size and characteristics of each intermediary;
- Sets up internal control mechanisms on AML/CFT at the Group level;
- collaborates, through its manager, with the AML functions or similar structures of each

Group entity.

With regard to information flows to and from the individual AML functions of the individual Group components and to and from the corporate bodies, these are detailed in Appendices 1 and 2 ("Internal Information Flows" and "Intra-Group Information Flows").

2.12. Group AML Office Manager

The head of the Group AML office is appointed by the head of the Group AML department, subject to the endorsement of the Managing Director, and is found to possess appropriate independence, authority and professionalism.

Before appointment, it should be verified that the same is in possession of:

(a) an adequate reputational profile, honesty and integrity necessary to perform their function;

b) appropriate AML/CFT skills and experience, including knowledge of the applicable legal framework and in the implementation of policies, controls and procedures in this area and in the identification, assessment and management of ML/FT risks;

c) sufficient knowledge and understanding of the ML/FT risks associated with the Group's *business* model to enable it to effectively fulfill its function;

d) adequate experience in identifying and managing ML/TF risks;

e) adequate time and hierarchical position to perform their duties effectively, independently and autonomously.

If the same is entrusted with other assignments, the department head must assess potential conflicts of interest and propose specific measures to the Managing Director to prevent or manage them. In addition, if there are other assignments, the head of the Group AML office must be able to devote sufficient time to the performance of his or her duties.

The head of the Group AML office:

- oversees the money laundering risk assessment exercise conducted by Group components;
- cooperates fully with the AML officer of each Group entity;
- coordinates the *business* area-level assessment of ML/TF risks locally from the various Group companies and organizes the aggregation of related findings to understand the nature, intensity, and location of ML/TF risks faced by the Group as a whole;
- Coordinates the activities of the various AML officers of Group entities to ensure that they operate consistently;
- Develops and submits to the Bodies of the Parent Company anti-money laundering procedures, methodologies and group standards, and ensures that the policies and procedures of the group components are in line with these *standards*, as well as in compliance with the relevant laws and regulations applicable to them;
- Establishes periodic information flows from all Group companies to share information

necessary for the performance of their duties;

- Monitors the compliance of subsidiaries and branches located in third countries with EU AML/CFT requirements, particularly where the requirements for the prevention of ML/TF are less stringent than those in Directive (EU) 2015/849.

2.13. Head of suspicious transaction reporting of Banca Popolare di Sondrio

Pursuant to Article 36 of the Anti-Money Laundering Decree, the person in charge of suspicious transaction reports (or SOS) is the legal representative of the recipient or a proxy of the recipient; the proxy may also be given to the head of the Group AML department. The delegation of authority is decided by the Board of Directors, after consultation with the Board of Statutory Auditors.

The person in charge of the SOS possesses adequate requirements of independence, authority and professionalism and carries out his or her activities with autonomous judgment and in compliance with the confidentiality obligations provided for in the AML decree, including with respect to exponents and other corporate functions. The role of the SOS manager is adequately formalized and made known within the structure and to the territorial network. The appointment and revocation of the same manager shall be promptly communicated to the FIU in the manner specified by the FIU.

The SOS manager has no direct responsibilities in operational areas and is not hierarchically subordinate to individuals in those areas. He or she must verify that any human resources entrusted with the tasks of analyzing transactions and computer "*alerts*" possess the necessary skills, knowledge, and suitability and are adequately educated about the bank's obligations of confidentiality of information and protection of the reporter.

The SOS manager is familiar with the structure and selection criteria of operation monitoring systems and internal procedures for handling "*alerts*" and periodically checks their proper functioning.

He may receive reports from employees in the network, business units and offices, or from the Bank's Bodies, ensuring that they are evaluated in a timely manner. To this end, the head of SOS establishes a process for managing the prioritization of internal reports received, in proportion to their risk.

The person responsible for suspicious transaction reports:

- promptly assesses, in the light of all available elements, suspicious transactions reported by the head of the branch or other operational point or organizational unit or structure responsible for the concrete management of customer relations (so-called first level);
- promptly assesses, in light of all available evidence, suspicious transactions of which it has otherwise become aware in the course of its business;
- Transmits to the FIU the reports deemed well-founded, omitting the names of those involved in the transaction reporting procedure;
- maintains evidence of the assessments made as part of the procedure, even if the report is

not sent to the FIU, in compliance with confidentiality obligations;

- acquires any useful information from the structure carrying out the first level of analysis of anomalous transactions and from the Group AML department;
- has free access to information flows directed to corporate bodies and structures and/or functions, significant for preventing and combating money laundering and terrorist financing (e.g., requests received from judicial authorities or investigative bodies);
- in evaluations also uses information about any SOS already performed on the same customer by other Italian group companies;
- also considers any additional elements inferable from freely accessible information sources (e.g., search engines, journalistic sources, etc.);
- plays an interlocutory role with the FIU and the investigative bodies and responds promptly to any requests for further investigation from them.

The person in charge of the SOS communicates, in an appropriate organizational manner to ensure compliance with the confidentiality requirements of the AML Decree, the outcome of his or her assessment to the first-level responsible person who originated the report.

In compliance with the confidentiality obligations under the Anti-Money Laundering Decree on the identity of individuals who take part in the transaction reporting procedure, the head of SOS provides-including through the use of appropriate information bases-information on the names of customers subject to suspicious transaction reporting to the heads of the relevant structures for assigning or updating the risk profile of those customers.

Further guidance on the role of the suspicious transaction reporting officer and the reporting process is detailed in the bank's special "Regulations for Suspicious Transaction Reporting."

2.14. Risk Control Service

With reference to the control of money laundering and terrorist financing risks, the Risk Control department cooperates with the Group Anti-Money Laundering department and its manager:

- for the definition of AML/CFT risk assessment methodologies, fostering synergies with the tools and methods specific to *operational risk management*;
- to integrate the noncompliance risk assessment and management model into the *Risk Appetite Framework*;
- in the analysis of risks associated with new products and services to be launched for marketing, including entry into new businesses and new markets, both on request and through a structured *clearing* process, collaborating in the identification of potential risks to the bank and customers and providing quantitative assessments where applicable.

2.15. Operating facilities

The company's operational structures represent the first and essential level of corporate oversight for the purposes of preventing and combating the phenomena of money laundering and terrorist

financing, since they are the operational units that are concretely responsible for the administration and management of customer relationships. In particular:

- transpose the operational instructions on AML/CFT, provided by external and internal regulations;
- carry out customer due diligence obligations, both at the stage of establishing ongoing relationships and on occasional customers, also carrying out constant monitoring throughout the duration of the relationships, including through the use of computer tools specifically designated for this purpose;
- acquire and ensure the orderly storage of the documents, data and information prescribed for the fulfillment of customer due diligence obligations, consistent with the provisions of internal regulations, and also ensure that they are kept up-to-date;
- based on the evidence provided through the specifically deputized tools, make periodic assessments of the risk profile attributed to customers;
- assess the operations carried out by customers, including-but not exclusively-through the supporting IT tools set up for this purpose, activating the suspicious transaction reporting process where appropriate;
- review the periodic evidence from time to time provided by the relevant central departments or offices aimed at ensuring compliance with the obligations prescribed by the regulations on customer due diligence;
- ensure the utmost cooperation with the competent Authorities, within the scope of investigations, in-depth investigations, inspections regarding money laundering and financing of terrorism carried out at them, coordinating with the competent structures and/or functions of the company.

2.16. Branch anti-money laundering contacts

At each of the bank's branches, a branch contact person is identified - by the head of the branch - who is specially trained in the subject matter, and who, while reporting hierarchically to the head of the branch, coordinates, where necessary, with the AML office of BPS to:

- constitute the contact person within the branch to the BPS AML office, both for requests for advice from the branch and for requests received from the central service;
- ensuring the circulation of information within the operational structure, avoiding redundancy in requests for information or assistance, receiving and responding to queries within the dependency, and involving the AML office of BPS if support is needed;
- Support the dependency manager in the ongoing assessment of customer operations and the detection of any suspicious transactions.

As such, the branch AML contact person does not assume the responsibilities normatively assigned to the branch manager.

3. MONEY LAUNDERING AND TERRORIST FINANCING RISK MANAGEMENT MODEL OF THE BANKING GROUP

The Banca Popolare di Sondrio Banking Group adopts a unified approach to AML/CFT, with guidelines, rules, processes, controls and IT tools that are as homogeneous as possible. To this end, Banking Group companies are required to transpose this Document, adapting it to their own corporate context and, in the case of foreign subsidiaries, to the specifics of local regulations, submitting it for approval by the Body with strategic supervisory functions. Subsidiaries of the Banking Group shall inform the bank of the outcomes of the transposition process in the manner set forth in the "Management Regulations for Corporate Regulations" dated June 30, 2023.

Strategic decisions at the Banking Group level on AML/CFT risk management and related controls are referred to the Corporate Bodies of the Parent Company. The latter ensures that the Corporate Bodies of the other Group companies implement the Group's AML/CFT strategies and policies in their own businesses and ensures that the Bodies and internal structures of each component, including their respective control functions, have the necessary information to be able to carry out their tasks.

The Parent Company appoints a member of the Board of Directors as the representative responsible for AML at the Group level. The appointment is executive in nature. The exponent responsible for AML at the Group level is the main point of contact between the head of the Group AML department and the Bodies with strategic supervision and management functions of the Parent Company, and ensures that the latter have the necessary information to fully understand the relevance of the money laundering risks to which the Group is exposed, for the purpose of exercising their respective powers. The Group Anti-Money Laundering Officer ensures that the Group Anti-Money Laundering Officer performs his or her duties effectively.

The person responsible for AML at the Group level may coincide with the person responsible for AML at the Parent Company.

The Corporate Bodies of the Banking Group's subsidiaries must be aware of the choices made by the Corporate Bodies of the Parent Company and are responsible, each according to their competencies, for the implementation of AML/CFT risk management strategies and policies in line with their own business reality. With this in mind, the Parent Company involves and makes participates, through the Managing Director and the head of the Group's AML department, the Corporate Bodies of the investees about the choices adopted regarding policies, processes and procedures for managing the risk of money laundering and terrorist financing.

The Parent Company defines and approves at the Banking Group level:

- A Group methodology for assessing the risk of money laundering and terrorist financing;
- the general *standards on* due diligence requirements, the retention and making available of documents, data and information, and the detection and reporting of suspicious transactions;
- formalized procedures for coordination and sharing of relevant information on the subject within the Banking Group, including for the purpose of identifying suspicious transactions,

and a direct reporting line between the heads of the AML functions of the components, including foreign components (consistent with the legal regimes of third countries), of the Group and the head of the Group AML department;

- Group-wide AML control procedures.

The Parent Company identifies suitable organizational solutions to ensure compliance with the applicable provisions in relation to the various areas of operations, periodically assesses the effectiveness and functionality of the Group's AML policies and procedures, and ensures that AML risk management takes into account all the assessment and measurement elements held by the individual components.

The Parent Company ensures that Group entities promptly implement corrective measures necessary to overcome deficiencies in AML safeguards detected by the Bank of Italy, the FIU or, in relation to foreign components, the competent authorities.

Within the Banking Group, the specific tasks assigned to the Group AML department are carried out according to two distinct models, declined to take into account the operational and territorial articulation of the Banking Group itself. In particular:

1) for Banca della Nuova Terra Spa, whose operations are marked by a high level of integration with the parent company, it is planned to *outsource* AML/CFT risk control activities to the Group's AML department, with the simultaneous appointment of an internal contact person (RAE) at the subsidiary;
2) for Banca Popolare di Sondrio Spa, Factorit Spa, and Banca Popolare di Sondrio (SUISSE), the establishment of autonomous AML structures and the appointment of a manager for each is established.

In the first case, AML and terrorist financing risk control activities are carried out by the AML office of BPS and the related activities provided are regulated by specific outsourcing contracts. Provision is also made for the appointment of an internal anti-money laundering contact person (RAE) who, operating in close functional coordination with the Group AML office, oversees processes related to AML/CFT regulations within the individual subsidiary.

The outsourced AML structure--based on the guiding principles and *standards of* behavior established by the Group AML department that Banca della Nuova Terra must follow for the management of the main compliances in question--is:

- Identifies and updates the system of first- and second-level controls;
- defines the requirements for tools to support the processes of customer due diligence and profiling and intervenes in the process of assessing customers with a high risk profile;
- Carries out supervision of the storage archive of information, documents and data for compliance with AML obligations;
- Prepares periodic summary reports, or specific *reports* in the case of particularly serious events, to be forwarded to corporate bodies and top management.

The internal contact person appointed at the subsidiary is responsible for verifying the proper performance of the service by the outsourced AML structure and adopts the necessary

organizational precautions to ensure the maintenance of the powers of direction and control by the corporate bodies. Specifically:

- Monitors, through periodic audits, compliance with contractual obligations and the proper performance of the service by the outsourced function;
- Verification that the service provided enables the effective fulfillment of AML obligations;
- reports regularly to corporate bodies on the performance of outsourced tasks to ensure that any necessary corrective measures are taken in a timely manner.

In contrast, for the subsidiaries of the banking group to which the second model applies-Factorit Spa and Banca Popolare di Sondrio (SUISSE)-an autonomous AML structure is established and the relevant person in charge is appointed (who may also be given authority for suspicious transaction reporting) who:

- operates in coordination with the head of the Group AML office and informs him/her of the outcomes of the control activities carried out and any significant occurrences;
- ensures that the head of the Group AML office, consistent with applicable national regulations, has access to all data and information needed to assess ML/FT risks;
- liaises with the relevant supervisory authorities, coordinating with the Group AML office.

With regard to the reporting of suspicious transactions, the organizational model at the Banking Group level provides for the appointment by the Board of Directors of each subsidiary subject to the relevant regulatory obligations, having consulted with the Board of Statutory Auditors, of a corporate manager for the reporting of suspicious transactions. In order to ensure the existence of suitable coordination mechanisms to safeguard the homogeneity and consistency of the analysis logics employed, the SOS manager appointed at the Parent Company, for the purposes of in-depth analysis of anomalous transactions and relationships from a Banking Group perspective, interfaces with the SOS managers at the subsidiaries, in order to share data and information relating to common customers in respect of whom a reporting *process* has been initiated, without prejudice to the regulatory limits present in foreign jurisdictions, as explained in greater detail in paragraph 3.1. In any case, the confidentiality of the identity of the individuals participating in the reporting process is guaranteed.

In general, to carry out its duties, the Group AML office has access to all activities and any information relevant to the performance of its tasks.

The head of the Group's AML office has an information base that enables a homogeneous assessment of the customers shared by the Group's Italian companies. With regard to the Swiss subsidiary, due to the restrictions on the exchange of information that remain in the Swiss legal system, the data subject to sharing relate to BPS (SUISSE) customer entities subject to suspicious transaction reporting and those deemed to be at high risk, as explained in more detail in section 3.1.

Specifically, the following information is shared among all companies based in Italy:

- Master data of common customers;
- Risk profiles of common customers;

- Suspicious transaction reports filed against common customers, along with the reasons for them.

The Board of Directors of the Parent Company verifies:

- That each Group company assesses its respective money laundering and terrorist financing risks in a coordinated manner and based on the Parent Company's guidelines, while taking into account their respective specificities;
- That in the case of supervisory activities carried out on a Group company, the corrective measures taken by that company to remedy any deficiencies found are implemented in a timely and effective manner.

3.1. ML/FT risk management in relation to foreign subsidiary Banca Popolare di Sondrio (SUISSE)

Commission Delegated Regulation (EU) 2019/758 of Jan. 31, 2019, supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical standards for minimum action and the type of additional measures to be taken by credit and financial institutions to mitigate the risk of money laundering and terrorist financing in certain third countries provides for additional measures - including minimum action - to be taken by credit and financial institutions to effectively address the risks in question in cases where the legal system of a third country does not allow for the implementation of group policies and procedures as referred to in Article 45(1) and (3) of Directive (EU) 2015/849 (c.d. IV AML Directive), at the level of majority-owned branches or subsidiaries that are part of the Group and are established in a third country.

In addition, where the third country's legal system prohibits or limits the implementation of policies and procedures necessary to appropriately identify and assess the money laundering and terrorist financing risk associated with a business relationship or occasional transaction by restricting access to relevant customer and beneficial ownership information, or by limiting the sharing and use of such information for customer due diligence purposes credit and financial institutions must, among other things, at a minimum, "*disclose to the competent supervisory authority of the home Member State without delay how the application of third country law prohibits or restricts the implementation of policies and procedures necessary to detect and assess money laundering and financing risk associated with a customer.*" Specifically, as also stipulated in the Bank of Italy's "Provisions on organization, procedures and internal controls aimed at preventing the use of intermediaries for the purpose of money laundering and terrorist financing" of March 26, 2019, "*The Parent Company shall establish a common information base that allows all companies belonging to the group to assess customers in a uniform manner.*" If this is not possible, "*The Parent Company shall notify the Bank of Italy in the terms and manner provided for in the European Commission's regulation pursuant to Article 45(7) of the AML Directive and shall take further measures specified therein.*"

As pointed out to the Bank of Italy by the Parent Company of the Banca Popolare di Sondrio Banking Group, in a specific communication, the contents of which were approved at the December 20, 2019 board meeting, the Swiss regulatory provisions on constraints and

restrictions limit the possibility of sharing and processing, within the Group, data on the subsidiary's customers and their risk profile, as well as information on suspicious transaction reports. Similar restrictions apply to the local regulations in force at Banca Popolare di Sondrio SUISSE's branch located in the Principality of Monaco.

Subsequently, on June 26, 2020 - in response to the Bank of Italy's communication of April 19, 2020 regarding Banca Popolare di Sondrio. Communication pursuant to Delegated Regulation (EU) 2019/758: request for clarifications - the Board of Directors of the Parent Company, on June 20, 2020, provided that - in addition to the indicators and data flows and information of an aggregate nature that the Swiss subsidiary already provides - "*upon the detection of situations with a high risk of money laundering and terrorist financing, likely to create legal and reputational issues at the Group level, the subsidiary shall make available to the Parent Company's control functions the information available at the Parent Company, including information concerning certain business relationships. The assessment of individual cases and coordination for the provision of the aforementioned information are ensured, as a rule - except in cases of urgency - by bimonthly confrontations that will take place at the subsidiary, between the head of the subsidiary's Legal & Compliance department and the head of the Group's AML department.*"

In light of the foregoing, below are the methods and procedures by which the Parent Company implements AML/CFT risk control with respect to the subsidiary Banca Popolare di Sondrio (SUISSE) SA, including the branch in the Principality of Monaco, as defined by the Board of Directors.

It should be noted, in this regard, that a *compliance officer* is appointed at the Monaco branch, responsible for AML, who functionally reports to the head of the *Legal & Compliance* office of the Swiss parent company.

Specifically, through:

a. The provision - by the subsidiary - of aggregate information flows;
b. The preparation - by the subsidiary - of periodic reports;
c. bimonthly coordination and sharing meetings at BPS (SUISSE) among the Heads of "AML" facilities;
d. interactions between the head of the *Legal & Compliance* BPS (SUISSE) office and the head of the Group AML department for issues that are of an urgent nature or upon the occurrence of events that exceed certain attention thresholds;
e. Sending by the Parent Company of the so-called Country List.

a. Aggregate information flows

BPS (SUISSE), on a monthly basis, sends a set of indicators to the Parent Company, described below.

INDICATOR	CONTENT

Customer distribution by risk range[4]	The flow provided reports to the end date of the reporting period: - The distribution of customers, divided between individuals and legal entities; - Distribution of reports by risk band; - Manual changes in the risk band (decreases/increases); - Distribution of subjects by risk factors; - Distribution of relationships with risk factors, with evidence of how many opened during the reporting period; - Number of incomplete/missing adequate verification information; - Number of events for updating due diligence.
Operations with countries at risk[5]	The flow provided reports to the end date of the reporting period: - Distribution of subjects by country risk with country evidence and subsequent breakdown; - Distribution of fund transfers by country risk with country evidence in terms of amounts and number of transactions.
Distribution and trends of matching situations of names with those surveyed in external lists	The flow provided includes: - number of reports highlighted to the *Legal & Compliance* department at the opening stage by the information technology solution (CREA)[6] , for verification of any correspondence; - Number of reports, at the opening stage, with coincidence of names actually ascertained; - number of concordances detected in the *AML-Bestvision* procedure[7] during the reporting period; - Number of relationships in place at the end of the reporting period; - Number of concordances in AML procedure confirmed in the reporting period; - number of transactions "put on hold" by the *Fircosoft* procedure[8] *;* - Number of transactions verified by the *Fircosoft* application during the reporting period; - Confirmed types of subjects.
Indicators of abnormal or unexpected behavior (so-called "plausibilizations")	The flow provided reports to the end date of the reporting period: - Distribution of the unexpected by type of behavior; - Distribution of the unexpected by assessment time; - Distribution of unexpected unassessed from both Level I and Level II.
Distribution of suspicious transaction reports (SOS)	The flow provided reports the number of suspicious transaction reports sent to the Money Laundering Reporting Office (MROS) as of the end date of the reporting period, with a distribution:

[4] At BPS (SUISSE) the categorization of customer risk profiles is different from that of the Parent Company. Specifically: Band A (PEP); Band B (policyholder and/or proxy and/or beneficial owner with domicile and profession at risk); Band C (domicile of the policyholder and/or proxy and/or beneficial owner in a country at risk); Band C1 (domicile of the control holder in a country at risk); Band C2 (place of business of the contracting party and/or beneficial owner in a high-risk or non-cooperative country according to the FATF); Band C3 (ordinary relationship (belonging to Band E) that, on a semi-annual basis, for a volume of 25% or more, totaling more than 30.000 CHF, receives or sends from or to other-risk or non-cooperative countries according to the FATF); Band D (profession/business activity at risk of the owner and/or attorney and/or beneficial owner); Band D1 (relationships with assets exceeding 5 million CHF; Band E (all other relationships not covered by the higher risk categories); Band F (relationships requiring special monitoring); Band G (complex structures).

[5] The definition of "risk countries" for Swiss regulations is partially different from that of the Parent Company: the "sanctioned" countries are those decreed by the UN, the EU and the State Secretariat for Economic Affairs (SECO).

[6] *CREA*, an IT solution expressly dedicated to the automatic verification, through direct interfacing with the *WorldCheck* and *Compliance Daily Control* lists, of the names *of* potential customers and other possible participants in the relationship.

[7] *AML-Bestvision*, an IT solution dedicated to assessing "higher risk" transactions and monitoring tax compliance.

[8] *Fircosoft/Stelink*, IT solution for monitoring transactions having payer and/or payee included in *WorldCheck* lists.

	- By category; - by type; - by origin; - By number of secondary subjects involved; - By number of operations; - By range of amount; - By forwarding time (with evidence of the average value); - By storage type.

b. Periodic reports

INFORMATION FLOW	SENDER	RECIPIENT	FREQUENCY
Report on *compliance* risk assessment and the activities carried out by the *Legal & Compliance* department	*Legal & Compliance* office of the subsidiary	- Group Anti-Money Laundering Service	Semiannually (data as of June 30) and annually (data as of December 31), subject to approval by the subsidiary's board of directors
Action plan accompanied by the measures that will be prepared during the year	*Legal & Compliance* office of the subsidiary	- Group Anti-Money Laundering Service	Annual, prior to approval by the board of directors of the subsidiary
Action plan update and progress of activities	*Legal & Compliance* office of the subsidiary	- Group Anti-Money Laundering Service	Annual, prior to approval by the board of directors of the subsidiary

c. Bi-monthly coordination meetings

With a view to proactively combating money laundering and the financing of terrorism, on a bimonthly basis - except in cases of urgency, for situations deemed to be high-risk, requiring immediate sharing with the parent company, - specific meetings are held between the head of the *Legal & Compliance* office of the BPS (SUISSE), the Group AML manager and the head of the Group AML office. During these meetings, usually held at the head office in Lugano, the master data of the names subject to suspicious transaction reports sent to the competent authorities by the Swiss parent company and the Munich branch are, among other things, shared. In addition, the parent company provides special list containing the names of individuals reported by it for suspicious operations in the last two months prior to the meeting. At the next meeting, the subsidiary will provide evidence regarding the existence of common customers with those subject to SOS by the Parent Company, indicating, if applicable, the measures taken to mitigate any risk situations. The Group's Anti-Money Laundering service will provide a registry check of all the names contained in the list provided by the subsidiary; in the event of any correspondences, the service itself will carry out the necessary checks and in-depth investigations in order to manage any emerging risks of money laundering and terrorist financing. On a continuous monthly basis, the Group's AML service will renew the above-mentioned checks on the entire list

of names communicated from time to time and subject to reporting for suspicious or higher risk transactions.

d. Additional coordination meetings and attention thresholds ("*triggers*")

In the event that the head of the *Legal & Compliance department* and/or the head of the Group's Anti-Money Laundering department perceive the need for alignment on certain issues that could have negative impacts on the risk of money laundering and terrorist financing - or even only from a reputational point of view - the same will take action, even in the shortest possible time - so that the examination of what is necessary takes place in the shortest possible time, if deemed necessary also through specific meetings at the Lugano branch of the subsidiary.

In case of absence or inability, the Group AML officer may make direct contact with the contact person of the BPS (SUISSE) Compliance Office and, as a last resort, with the chairman of the general management.

The events and related attention thresholds ("*triggers*"), upon the occurrence of which the Group AML department must conduct additional checks and investigations against the subsidiary, are as follows:

TRIGGER	THRESHOLD	ADDITIONAL MEASURES
Incidence of PEP clients in total clientele	≥ 0,10%	Request to the local *Legal & Compliance* office of BPS (SUISSE) to provide clarification in writing regarding the reasons for exceeding the threshold, the type of customers affected and the corresponding measures taken to mitigate ML/TF risks
Incidence of customers classified as high risk out of total customers	≥ 2,5%	Request to the local *Legal & Compliance* office of BPS (SUISSE) to provide clarification in writing regarding the reasons for exceeding the threshold, the type of customers affected and the corresponding measures taken to mitigate ML/TF risks
Incidence of no. of transactions to countries subject to AVR; Incidence of the amount of transactions to countries at AVR	≥ 0,60% ≥ 1,30%	Request to the local *Legal & Compliance* department of BPS (SUISSE) to provide clarification in writing regarding the reasons for exceeding the threshold, the type of customers affected and the corresponding measures taken to mitigate ML/TF risks
Presence of findings by the external auditing firm or the local supervisory authority	a event	Constant monitoring of consequent actions, in compliance with the deadlines set for compliance

If he/she sees the need for further investigation, the Group AML officer may request further information from the *Legal & Compliance* office of BPS (SUISSE) - possibly even on site - involving, where deemed appropriate, also the Corporate Bodies of the subsidiary and, in the most serious cases, also the Board of Directors of the Parent Company and the representative responsible for AML of BPS and the Group.

During on-site visits, the Group AML officer must also request information and documentation related to suspicious transaction reports submitted by the subsidiary to the local (Swiss and/or Monegasque) authority.

e. Transmission Country Table

The Group AML Office provides all Banking Group subsidiaries, including BPS (SUISSE), with the Country Table prepared according to the criteria outlined in Section 4.2, at the time of each update. As far as the Group's Italian companies are concerned, the risk profile assigned to each country is relevant (along with other factors) for the purposes of assigning the risk profile to individual customers, as well as in the context of the depth and extent of the due diligence measures applicable to individual transactions from/to third countries.

With regard to the subsidiary BPS (SUISSE), the Country Table is used for the purpose of providing the Parent Company with consistent data regarding transactions from/to non-EU countries (other than Switzerland and the Principality of Monaco), as part of the development of monthly and quarterly risk indicators. It is also used in the AML/CFT risk self-assessment activity carried out twice a year (on June 30 and December 31) and reported to the Parent Company for Group self-assessment.

4. EXPOSURE AND RISK MANAGEMENT AML/CTF AND IN INTERNATIONAL FINANCIAL EMBARGOES AND SANCTIONS

Banca Popolare di Sondrio offers itself on the market as a universal bank, combining its tradition as a company strongly rooted in the territory with its great attention to the development of international relations.

Taking into account the nature, size and complexity of the business carried out as well as the type and range of services provided, the bank is exposed to a risk of money laundering and terrorist financing monitored by the Group's AML department, including through the self-assessment exercise, in order to maintain an organizational structure, operational and control procedures as well as information systems suitable for ensuring compliance with legal and regulatory provisions on countering the aforementioned risks.

For details regarding the self-assessment exercise, please refer to the appropriate section 5 of this Document ("AML/CFT Risk Self-Assessment and Annual Report"). BPS's AML office-through this periodic exercise-identifies the current and potential risks to which the bank is exposed ("inherent risk") and the level of adequacy of its organizational structure ("vulnerability analysis").

The combination of the judgments of inherent risk and vulnerability of internal controls determines the allocation of residual risk based on the matrix provided by the Bank of Italy in the "Provisions on organization, procedures and internal controls aimed at preventing the use of financial intermediaries for money laundering and terrorist financing."

Based on the level of residual risk determined, and taking into account the vulnerability analysis, the bank identifies corrective or adjustment initiatives to be taken to prevent and mitigate residual risks. These measures are implemented by the Body with management function through the Group AML department, which is also responsible for monitoring the progress of the planned adaptation actions.

As part of this, the AML office of BPS updates the outcomes of the last self-assessment exercise conducted every six months, adjusting the vulnerability analysis in light of the implementation of the planned upgrades.

In determining the vulnerability analysis, the bank assesses the organizational set-up, operating and control procedures as well as the information systems adopted to ensure compliance with AML laws and regulations. In making this assessment, the bank also takes into account the indications and assessments from the company's control functions (e.g., Internal Audit) as well as takes into account any findings by the Bank of Italy in carrying out its own controls.

Detailed below are the choices that the bank has made on the various relevant profiles (organizational structure and operating/control procedures, due diligence, data retention, suspicious transactions) to ensure an overall internal control system for the prevention of money laundering and terrorist financing risks, capable of guaranteeing compliance with legal and regulatory provisions on anti-money laundering.

4.1. Organizational procedures and internal control measures

In application of the risk-based approach, the bank has equipped itself with an organizational structure, operating and control procedures, and information systems suitable for ensuring compliance with laws and regulations on AML/CFT, in view of the nature, size, and complexity of its business and the type and range of services provided.

To this end, the body with strategic oversight function:

- conducts a comprehensive assessment, periodically updated, of its exposure to money laundering and terrorist financing risk, including at the Banking Group level;
- gives the Group AML department the responsibility for ensuring the adequacy, functionality and reliability of AML/CFT safeguards within the Banking Group;
- Approves any delegation of responsibilities for suspicious transaction reporting, including with regard to the deputy of the delegate;
- assigns the Internal Audit Department the task of verifying the degree of adequacy of the AML/CFT organizational structure and compliance with regulations.

In this context, in order to mitigate the risk of money laundering, the involvement of the Corporate Bodies and the proper fulfillment of the obligations that fall on them is essential. For this reason, too, the composition of the Corporate Bodies must be such as to ensure the presence of adequate knowledge, skills and experience for the purpose of understanding the money laundering risks related to the bank's activity and *business* model.

4.2. Assessment of money laundering and terrorist financing risk factors and customer profiling

The bank shall apply customer due diligence measures proportionate to the extent of the AML/CFT risks detected.

In order to graduate the depth and extent of customer due diligence requirements, the bank adopts appropriate procedures aimed at profiling each customer according to the risk of money laundering and terrorist financing, in application of the broader principle of proportionality referred to in the regulatory provisions, the aim of which is to maximize the effectiveness of corporate safeguards and rationalize the use of resources.

The criteria used to determine the risk attributable to each client take into consideration a number of factors, including the subjective characteristics of the client, the executor and the beneficial owner, the nature of the relationships established with it, the type of transactions, supplemented by elements inferable from the subject's overall operations (such as the client's behavior, the reasonableness of the transaction, the geographical area, the distribution channel, etc.). In assigning the profile, the criteria set forth in the AML Decree, the Bank of Italy's "Provisions on Due Diligence," and the EBA Guidelines on Risk Factors are considered.

The IT principals at the bank's disposal allow it to determine, based on the processing of data and information acquired during the master census, the establishment of ongoing relationships, the execution of occasional transactions and the monitoring of operations, a score representative of

the level of risk of money laundering or terrorist financing and to classify customers into four classes: Insignificant, Low, Medium, High.

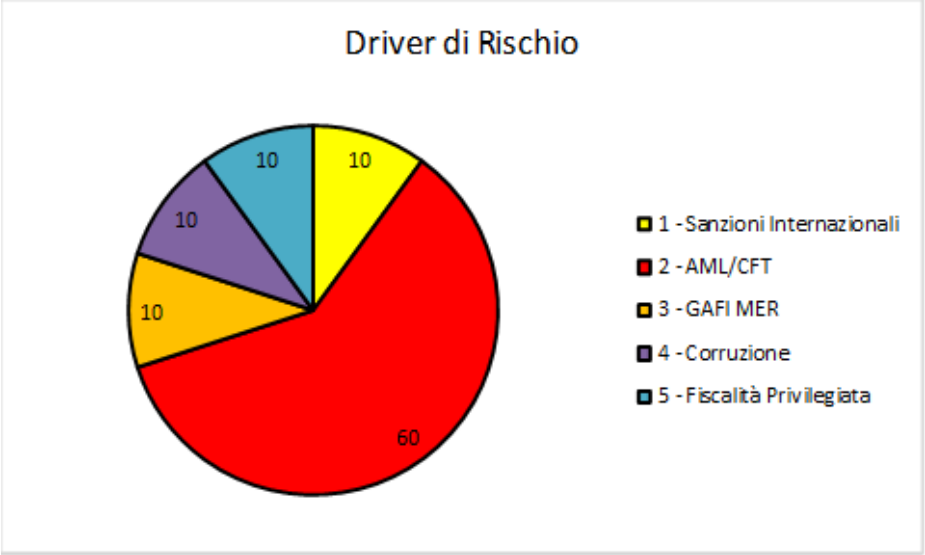
Risk factors related to:

- client (business, area of operation, reputation, behavior, ties to high-risk individuals or entities);
- countries and geographic areas (country classification; risk associated with Italian provinces classified as having high crime rates);
- products, services and operations (level of opacity, complexity, value, third-party intervention, high use of cash);
- Distribution channels (in-person or remote, use of agents/mediators).

Specifically with regard to risk factors inherent in the country or geographical area, the bank assesses:

1) the presence of financial sanctions, embargoes or measures related to the financing of terrorism or the proliferation of weapons of mass destruction, adopted by the UN, the European Union, the US Treasury Department (so-called "OFAC sanctions"), SECO (State Secretariat for Economic Affairs-Switzerland) and the United Kingdom (UK);
2) possible inclusion in lists of countries considered to be at "high risk" of money laundering and terrorist financing, drawn up by authoritative sources ("black list" of the FATF; European Commission's list of "high risk" third countries);
3) The robustness of the AML safeguards in place, as reflected in the mutual evaluation reports adopted by the FATF (so-called MER - *Mutual Evaluation Reports* - and related *follow-up* reports);
4) the level of corruption and permeability to other criminal activities, as resulting from assessments by authoritative and independent international organizations, such as *Transparency International* and the *Basel Institute on Governance*;
5) the level of tax transparency, as reflected in the reports endorsed by the OECD *Global Forum on* Tax Transparency and Exchange of Information and assessments of the commitment to automatic exchange of information based on the so-called "*Common Reporting Standard* (or CRS)"; for this purpose, the possible inclusion in the EU list of non-cooperative jurisdictions for tax purposes is also relevant.

The different geographical factors highlighted above take on the relative weight detectable from the graph below:



Based on these risk factors, countries are classified into three categories (A, B, C), subject to enhanced, ordinary and simplified due diligence measures, respectively. The list of countries, with their assigned risk level, is constantly updated by the AML office of BPS and disseminated within the company and is also transmitted through the Group AML office to the subsidiaries for appropriate adjustments.

Information on the risk profile of money laundering and terrorist financing is made available to the operational structures in charge of the management and administration, in concrete terms, of customer relationships.

Lowering a client's risk level is allowed only by the AML office of BPS under exceptional circumstances and detailed reasons in writing.

At the Group level, each Italian company assumes, for the same customer, the highest risk profile among those assigned by the Group's Italian components.

4.3. Update profiles and information acquired for customer due diligence

The bank monitors and periodically updates the scores and rules assigned to the risk profiling system, checking the appropriateness of the assigned risk class upon the occurrence of events or circumstances likely to change the customer's risk profile.

The timing and frequency of updating the data and information acquired vary according to the risk profile assigned; however, the update is carried out when it appears that the information previously acquired and used for adequate verification is no longer current. Specifically, it is carried out:

1) on the occasion of the opening of any new relationship in the head of existing customers, regardless of the risk profile;
2) When changes, reported by the bank's automatic procedures, have occurred with respect to:

a. expiration of identity documents and powers of representation;
b. Changes in beneficial ownership in the case of customers other than natural persons;
c. quality acquisition that can change the risk profile, detected by specific internal *screening* procedures, such as PEP or GDP qualification.

The following table shows the minimum frequency of updating data on due diligence in relation to the risk profiles attributed to customers.

REFERENCE	RISK CLASS	MINIMUM UPDATE FREQUENCY
I	Irrelevant	A event-when the information is no longer current
B	Low	A event-when the information is no longer current
M	Medium	Every 24 months
A	High	Every 12 months

4.4. Customer due diligence procedures

The bank shall conduct customer and beneficial owner due diligence with respect to relationships and transactions inherent in the conduct of its institutional business:

1) On the establishment of an ongoing relationship;
2) on the occasion of the execution of an occasional transaction of an amount of €15,000 or more, regardless of whether it is carried out by a single transaction or by several transactions that appear to be linked to carry out a split transaction;
3) If the bank acts as a conduit or is a party to the transfer of cash or bearer securities, whether in euros or foreign currency, for a total amount of €15,000 or more;
4) In all cases where:
   - there is suspicion of money laundering or terrorist financing, regardless of any applicable exemption, waiver or threshold;
   - there are doubts about the completeness, reliability or truthfulness of previously acquired information or documentation.

To ensure the proper conduct of customer due diligence, the bank shall proceed:

a) to the identification of customers, possible executors, and beneficial owners;
b) to verifying the identity of the customer, the executor, if any, and the beneficial owner on the basis of documents, data or information obtained from a reliable and independent source;
c) to the acquisition and evaluation of information on the purpose and nature of the ongoing relationship and, in the case of high risk of money laundering and terrorist financing, the occasional transaction;
d) to ongoing monitoring of continuing relationships, to update knowledge of the customer

and the stated purpose of the relationship, to assess any unexpected, abnormal or inconsistent transactions with the customer's previously known economic and financial profile, or news of significant events;

e) to updating the data and information collected, with frequency dependent on the risk profile previously associated with clients.

The bank requires from the customer, and the customer is required by regulation to provide under his or her own responsibility, all necessary and up-to-date information to enable the fulfillment of due diligence obligations.

Customer due diligence measures are proportional to the magnitude of money laundering and terrorist financing risks, taking into account specific factors with reference to the customer, the customer's conduct, the transaction, and the continuing relationship.

Customer due diligence obligations are fulfilled with respect to both new customers prior to establishing a continuing relationship or executing an occasional transaction and existing customers at the time of fulfilling the obligations prescribed by Council Directive 2011/16/EU of February 15, 2011 on administrative cooperation in the field of taxation and the relevant national implementing legislation . When the bank is unable to comply with the customer due diligence requirements, it shall not establish the continuing relationship, i.e., it shall not execute the transaction and, if the continuing relationship is already in place, it shall refrain from continuing the relationship. In such a case, the bank also considers whether to send a suspicious transaction report in the manner defined by the "Suspicious Transaction Reporting Regulations."

The concrete procedures for identifying and verifying the data of the customer, executor and beneficial owner, for acquiring and evaluating information on the purpose and intended nature of the continuing relationship and occasional transactions, and for ongoing monitoring during the course of the continuing relationship are regulated in the AML Decree, the Bank of Italy's "Provisions on Customer Due Diligence," the AML Handbook, and the bank's additional internal regulations, circulars and manuals on the subject.

4.4.1. Enhanced due diligence requirements

The bank applies enhanced customer due diligence measures when there is a high risk of money laundering and terrorist financing resulting from specific regulatory provisions or from its own assessment.

The bank considers the following high risk factors related to customer, performer, beneficial owner, products/services, distribution channels, or geography:

a) continuing relationships established under abnormal circumstances, such as reticence of the client or executor in providing the requested information or unreasonableness of the transaction;
b) customers and/or beneficial owner residing or based in high-risk geographies;
c) Negative reputational indexes related to the client, the beneficial owner and the executor;
d) structures that qualify as vehicles of wealth interposition;

e) companies that have issued bearer shares or are held by trustees (so-called *nominee shareholders*);
f) type of economic activity characterized by high use of cash (gold buyers, money changers, companies operating in the gaming/betting sector, both physical and *online*, agents and/or *money transfer* companies);
g) type of economic activity attributable to sectors particularly exposed to corruption risks;
h) Activities of nonprofit organizations (NPOs);
i) customer or beneficial owner identifiable as "Local Italian Politicians" (PIL);
j) abnormal or excessively complex ownership structure in relation to the nature of the business conducted;
k) services with a high degree of customization, offered to customers with significant assets;
l) products or transactions that could promote anonymity or encourage concealment of the identity of the customer or beneficial owner. Relevant, for example, are anonymous prepaid cards issued by foreign intermediaries, bearer shares, transactions attributable to services related to the conversion of legal tender into virtual currency and vice versa;
m) frequent and unjustified cash transactions characterized by the use of large denomination euro banknotes, or the presence of damaged or counterfeit notes;
n) transactions involving the transfer of cash or valuables from abroad with a total amount equal to or exceeding the equivalent of 10,000 euros. In such cases, the bank shall request from the customer a copy of the cash transfer declaration provided for in Article 3 of Legislative Decree No. 195 of November 19, 2008, and elaborate on any refusal or unwillingness on the part of the customer to provide the documentation;
o) payments received from third parties with no obvious connection to the client or the client's business;
p) next-generation products and business practices, including the use of innovative distribution mechanisms or technologies for new or pre-existing products;
q) the circumstance of having ceased for more than one year to hold one of the public offices stipulated in Article 1, paragraph 2 (dd) (1) of the AML Decree;
r) transactions related to oil, weapons, precious metals, tobacco products, cultural artifacts and other movable property of archaeological, historical, cultural and religious importance or rare scientific value, as well as ivory and protected species .

The bank always applies enhanced customer due diligence measures in those cases that are legislatively required, namely:

1) Occasional relationships and operations involving high-risk third countries identified by the European Commission;
2) cross-border correspondent relationships, involving the execution of payments, with a correspondent banking or financial intermediary located in a third country;

3) ongoing relationships or occasional transactions with customers and their beneficial owners who have the status of politically exposed persons (PEPs), except in cases where they act in their capacity as bodies of public administrations. In such cases, the bank shall adopt adequate verification measures commensurate with the risk actually detected , also taking into account the provisions of Article 23(2)(a)(2) of the AML Decree;
4) customers who carry out transactions characterized by unusually large amounts or with respect to which there are doubts about the purpose for which they are, in practice, intended.

Next, the approval process provided for opening/maintaining relationships with customers always considered high risk is given:

TYPE OF RELATIONSHIP	AUTHORIZATION
1. Occasional relationships and transactions involving high-risk third countries identified by the European Commission	Group Anti-Money Laundering Service Manager
2. Cross-border correspondent relationships, involving the execution of payments, with a correspondent banking or financial intermediary located in a third country	Managing Director, subject to the positive opinion of the head of the Group AML service; in the event that the Managing Director decides to depart from any negative opinion of the AML manager, he/she must justify such decision in writing, proposing appropriate measures aimed at mitigating the ML/FT risks highlighted by the head of the Group AML service
3. Continuous dealings or occasional transactions with clients and their beneficial owners who qualify as politically exposed persons (PEPs), except when they are acting in their capacity as organs of public administrations	Senior management delegated for this purpose, subject to the positive opinion of the head of the Group AML department; in the event that the senior management decides to deviate from any negative opinion of the AML manager, he/she must justify this decision in writing, proposing appropriate measures aimed at mitigating the ML/FT risks highlighted by the head of the Group AML department
4. customers who carry out transactions characterized by unusually large amounts or with respect to which there are doubts about the purpose for which they are, in practice, intended	Branch/unit manager

In addition, in the presence of one or more of the high risk factors listed above--and if the operations deviate from those normally expected, or are attributable to abnormal behavior patterns--the bank applies enhanced due diligence measures on relationships held by:

5) *trust* or related legal institution;
6) trust companies not registered in the register provided for under Article 106 of the Consolidated Banking Act;
7) agents and/or financial intermediaries engaged in *money transfer* activities;
8) Companies operating in the gaming/betting industry, both physical and *online*;
9) non-profit organizations (NPOs);
10) customers who have already been the subject of a suspicious transaction report in the previous three years and entities related to them;
11) persons in respect of whom the bank has received notice of investigations or proceedings by the judicial authority or investigative bodies for money laundering offenses in the previous three years and persons related to them;

12) PEPs-related entities;
13) customers resident or based in third countries assessed by the bank as high risk, according to the criteria outlined in Section 4.2, or transactions involving those countries;
14) customers who, for objective reasons or additional assessments made by the relevant subsidiary or other Group company, should be subjected to enhanced measures.

The enhanced due diligence measures, which are in addition to the specific authorization *processes* provided for the cases under points 1), 2), 3) and 4) highlighted in the table above, take the form of acquiring more information about the customer and the beneficial owner, if any, and a more accurate assessment of the nature and purpose of the relationship; a higher quality of the information requested; and an intensification of the frequency and depth of the analyses carried out as part of the ongoing monitoring of the relationship and transactions. Specifically, these measures consist of:

i) in the acquisition of more information regarding the ownership and control structure of the customer. Specifically, the documentation used to identify the beneficial owner must be dated no earlier than the previous two years;
ii) In acquiring more information about the continuing relationship to fully understand its nature and purpose, particularly on:
    - the reasons why the customer asks for a particular product or service, especially if his or her financial needs could be better met in another way or in another country;
    - The source and destination of the funds;
    - The nature of the business conducted by the client and the beneficial owner;
iii) In better quality of information to be acquired, such as:
    - Verification of the origin of the client's assets and funds, employed in the continuing relationship;
    - in the case of frequent and unjustified cash transactions, especially if carried out with large denomination banknotes, the bank shall make in-depth inquiries with the customer about the reasons behind such operations;
iv) in more frequent-at least annually-checks on ongoing relationships in order to detect any suspicions of money laundering and terrorist financing in a timely manner;
v) in the case of financial intermediaries exercising the activity of *money transfer*, in the need to obtain the authorization of the head of the Group Anti-Money Laundering Service (or his delegate) for the opening or continuation of ongoing relationships;
vi) in the case of trusts and companies participated by trusts, in the need to obtain responsible authorization from the Group AML department (or its delegate) for the opening or continuation of continuing relationships;
vii) in the case of cross-border correspondent relationships with banking or financial intermediaries from a third country, the bank shall apply, at the initiation of the relationship, the enhanced due diligence measures set forth in Article 25 paragraph 2 of the AML Decree, Section IV, Part Four of the Bank of Italy's Due Diligence Provisions, and

the Risk Factor Guidelines published by the EBA (Guideline No. 8).

4.4.2. Simplified measures of due diligence

The bank may apply simplified customer due diligence measures in terms of the extent and frequency of the required compliance if there is a low risk of money laundering and terrorist financing.

The bank considers the following categories of customers or products/services as low-risk factors and, therefore, applies simplified due diligence measures:

1) companies admitted to listing on a regulated market and subject to disclosure requirements that impose an obligation to ensure adequate transparency of beneficial ownership, i.e., those listed on regulated markets in EU and non-EU countries recognized by Consob pursuant to Article 70 of the TUF;
2) public administrations, i.e., institutions or bodies performing public functions, in accordance with European Union law;
3) reports in the name of executive and bankruptcy proceedings;
4) clientele resident or based in EU countries and third countries with effective AML/CFT prevention systems, characterized by a low level of corruption or permeability to other forms of crime, an adequate level of tax transparency and commitment to automatic exchange of information in tax matters, based on authoritative and independent sources;
5) banking and financial intermediaries specified in Article 3 Paragraph 2 of the Anti-Money Laundering Decree - with the exception of those in (i), (o), (s) and (v);
6) Community banking and financial intermediaries;
7) banking and financial intermediaries based in a third country with an effective AML/CFT regime, except in cases of cross-border correspondent relationships;
8) appropriately defined financial products or services restricted to certain types of customers, aimed at fostering financial inclusion; this includes the "basic current account" and financing through salary or pension assignment and delegation of payment.

Simplified due diligence measures consist of:

i) in the ability to carry out verification of the data on the beneficial owner by acquiring a confirmation statement signed by the customer, under his or her own responsibility;
ii) in the absence of set deadlines for updating the data collected for due diligence, except in cases of opening new relationships, or when events occur that may increase the ML/TF risk profile of the customer.

In each case, the bank verifies the continued existence of the conditions for applying the simplified procedure.

Simplified due diligence measures cannot be applied when:

- there are doubts, uncertainties or inconsistencies in relation to the identifying data and information acquired in the identification of the customer, executor or beneficial owner;

- the conditions for the application of the simplified measures, based on the risk indices stipulated in the AML Decree and the provisions issued by the Supervisory Authorities, are eliminated;
- monitoring activities on the client's overall operations and information acquired during the course of the relationship lead to the exclusion of a low-risk case;
- there is a suspicion of money laundering or terrorist financing.

4.4.3. Adequate verification in cases of remote operation

The bank takes care in case of remote operation, by which is meant the operation carried out by the customer without his physical presence (e.g., through computer communication systems).

Specifically, the bank, in cases of remote operation:

1) acquires the identifying data of the client and the executor and matches them against a copy, obtained by *fax*, mail or electronically, of a valid identification document;
2) Carries out further feedback on the acquired data in one of the following ways:
   - transfer made by the customer through another intermediary based in Italy or in an EU country;
   - request for verification and confirmation of data at another intermediary based in a SEPA ("*Single Euro Payments Area*") country, via SEDA ("*SEPA Electronic Database Alignment*") electronic messaging;
   - Request to send countersigned documentation.

4.4.4. Third-party performance of due diligence obligations

The bank may use third parties to carry out customer due diligence obligations, without prejudice to full responsibility for compliance with such obligations, in the manner and within the limits established by the AML Decree and the provisions of the Supervisory Authorities.

Under no circumstances may the bank use third parties based in high-risk third countries.

4.4.5. Constant monitoring throughout the continuing relationship

The bank conducts ongoing monitoring during the course of the continuing relationship to keep the customer's profile up-to-date and identify elements of inconsistency that may constitute anomalies relevant to the adoption of enhanced measures of due diligence, suspicious transaction reporting, and abstention from executing the transaction or continuing the relationship.

Ongoing control is exercised through the examination of the customer's overall operations, having regard to both the ongoing relationships and any specific transactions arranged, as well as through the acquisition of information when verifying or updating information for the

identification of the customer, the beneficial owner, and the ascertainment and assessment of the nature and purpose of the relationship or transaction.

To this end, the bank adopts *ex-ante* and *ex-post* control procedures with the aim of identifying, blocking and highlighting suspicious money laundering and terrorist financing transactions and on the subject of restrictions on the use of cash and bearer securities.

Controls are carried out on two levels:

- first-level controls, carried out by the operating departments/units that directly manage the relationship with the customer;
- second-level controls, carried out by the AML office of BPS, according to criteria and procedures governed by a special control manual.

4.5. Obligations to abstain

If the bank finds it objectively impossible to carry out customer due diligence, it refrains from establishing the relationship or does not carry out the transactions and, for existing relationships, terminates them. It also considers whether to file a suspicious transaction report with the FIU.

In any case, the bank shall refrain from establishing relationships or executing transactions and terminate the continuing relationship in the following cases:

1) correspondent accounts traceable directly or indirectly to *shell* banks (or *shell banks*);
2) legal persons to which trusts, trusts, corporations (or controlled through bearer shares) established in high-risk third countries as identified by the European Commission in the exercise of the powers governed by Articles 9 and 64 of the AML Directive are directly or indirectly a party.

The bank also:

3) Does not open anonymous reports or reports with fictitious/numerical headers;
4) does not offer pass-through accounts (so-called "*payable through accounts*");
5) refrains from offering products and/or services or performing transactions that might promote anonymity;
6) refrains from entering into ongoing relationships or performing occasional remote transactions that are not assisted by appropriate recognition mechanisms and procedures.

In implementation of the provisions of the *Guidelines on Policies and Controls for the Effective Management of the Risks of Money Laundering and Terrorist Financing in Providing Access to Financial Services,* published by the *European Banking Authority* (EBA/GL/2023/04), and based on the consequent amendments made to Legislative Decree 231/2007 by Law no. 136[9] , obligated entities shall ensure that the procedures adopted pursuant to Article 16 of the AML Decree ("Risk Mitigation Procedures") do not preemptively and across the board exclude certain

[9] "*Conversion into law, with amendments, of Decree-Law No. 104 of August 10, 2023, on urgent provisions for the protection of users, economic and financial activities and strategic investments.*"

categories of entities from offering products and services solely because of their potential high exposure to the risk of money laundering or terrorist financing (so-called "*derisking*").

In light of the above, the bank does not have any dealings with and does not engage in occasional transactions with companies that engage in activities such as service providers related to the use of virtual currencies (or cryptocurrencies), unless they can demonstrate that they have adopted effective safeguards and adequate procedures to ensure the traceability of transactions in order to exclude the anonymity of transactions.

4.6. Controls on counterterrorism and international embargoes and on fund transfers

In view of the growing importance assumed by the fight against international terrorism, weapons of mass destruction development programs, and trade in *dual-use* ("*dual use*") products and technologies, the bank adopts internal control procedures capable of identifying those customers or those transactions that present a high risk of involvement in activities, of a commercial or financial nature, put in place by customers in violation of restrictive measures adopted by the international community against certain countries, natural and legal persons, entities, organizations.

These controls, complementary to those carried out as part of ordinary due diligence procedures, can be divided into:

1) name checks: these are applied to the names of counterparties in the movements of funds, with the aim of ascertaining that clients do not operate with persons subject to sanctions issued by international bodies involving the obligation to freeze funds and economic resources, or the application of restrictive measures of a different nature (so-called "designated persons"). In this context, lists of persons and entities subject to restrictive measures applied by the European Union, the UN, OFAC, SECO (State Secretariat for Economic Affairs, Switzerland) and the United Kingdom (UK) are considered;
2) country controls: apply to transactions to and from countries considered at risk because they are: a) designated by international bodies (FATF, European Union) as exposed to high risk of money laundering and terrorist financing; b) assessed by international bodies (OECD, European Union) as having privileged taxation or as being uncooperative in the exchange of information on tax matters; c) recipients of international embargoes, due to poor countering of terrorist activity or violation of basic human rights;
3) transactional controls on operations: apply on the funds transfer operations carried out by customers and any underlying goods or services, to verify that embargo measures or similar restrictions of a commercial (e.g., prohibitions or restrictions on *import/export* of goods, raw materials, and technology) or financial (e.g., prohibitions or restrictions on financial services, investments, capital transactions) nature are not violated.

As a result of the controls carried out, where high-risk situations are identified, enhanced measures are activated aimed at acquiring additional data and information, including through the production of appropriate documentation, and at monitoring with particular intensity the

evolution of the relationships headed by the subject, without prejudice to the obligation to report suspicious transactions when the conditions exist.

In the specific circumstances indicated by the national and EU embargo regulations, the fulfillments of freezing of funds and economic resources due to the persons or entities affected by the restrictive measures are also fulfilled, and with them the prohibition of making capital or economic resources available to them. The procedures of notification, communication or request for authorization to the competent Authorities that may be provided for by the sanctions measures are also activated.

Finally, in compliance with the provisions of Regulation (EU) 2015/847 of the European Parliament and of the Council of May 20, 2015 on information accompanying transfers of funds, the bank adopts procedures that can identify the originator and beneficiary information that must be contained in transfers of funds.

4.7. Retention and making available of documents, data and information

The bank shall keep documents, data and information useful to prevent, detect or ascertain any money laundering or terrorist financing activities and to enable the conduct of the analyses carried out by the competent Authorities through computerized storage systems that ensure:

- Full and timely accessibility to documents, data and information by the Authorities;
- The timely acquisition of documents, data and information, including the date thereof;
- The integrity of documents, data and information and the non-alterability of the same after their acquisition;
- The adoption of appropriate measures aimed at preventing any loss of documents, data and information;
- The transparency, completeness, clarity of documents, data and information and the maintenance of their historicity.

To this end, the bank shall ensure the preservation of documents, data and information acquired for ten years after the termination of the continuous relationship or the execution of the occasional transaction.

4.7.1. Types of documents, data and information to be retained

Pursuant to Article 31(2) of the Anti-Money Laundering Decree, the bank shall keep copies of the documents acquired during customer, executor and beneficial owner due diligence.

The bank also keeps the following information:

1) with reference to continuing relationships: the operating point of relationship establishment, the date of establishment, and the date of termination;
2) with regard to occasional transactions to be subject to adequate verification and transactions relying on continuing relationships: the date of execution, the amount, the monetary sign, the reason for the transaction and the means of payment used;

3) with respect to occasional transactions for which due diligence is not required, the bank shall retain, in addition to the provisions of item 2) above, the data and information capable of uniquely identifying the customer and the executor, as well as, where known, the sector of economic activity and the data and information capable of uniquely identifying the beneficial owner.

The acquisition of documents, data and information must be completed no later than the 30th day after the establishment of the continuing relationship, the execution of the transaction, the change and the closing of the continuing relationship.

Retention requirements refer to ongoing relationships and transactions that are part of the bank's institutional business.

4.7.2. Data and information to be made available to the Authorities

The bank shall make available to the Bank of Italy and the FIU, in accordance with the *standards* set forth in the Bank of Italy's March 24, 2020 "Provisions for Keeping and Making Available Documents, Data and Information for Combating Money Laundering and Terrorist Financing," the data and information set forth in Article 5 of the provisions.

4.7.3. Ways of storing and making available documents, data and information

For the preservation of documents, data and information, the bank uses computerized preservation systems consisting of its accounting and management systems.

To ensure the reconstructability of customer operations and to facilitate the conduct of control activities, including inspections, of the Bank of Italy and the FIU, the bank ensures the provision of data and information to the Authorities through a specific standardized archive[10] , which complies with Annex 2 of the Bank of Italy's "Provisions for the storage and provision of documents, data and information for combating money laundering and terrorist financing" dated March 24, 2020.

4.7.4. Exemptions

Contrary to what was mentioned in the previous paragraph, the bank does not apply the provisions regarding the provision of data and information to the Authorities through a specific standardized file in relation to ongoing relationships or transactions entered into with:

1) the following banking and financial intermediaries referred to in Article 3(2) of the AML Decree, established in Italy or in another member state;
   - banks;
   - Italian Postal Service S.p.A;
   - Electronic money institutions as defined in Article 1, paragraph 2, letter h-bis), TUB

[10] So-called "former AUI" (formerly the Single Computer Archive), updated according to the new instructions mentioned above.

(IMEL);

- payment institutions as defined in Article 1, paragraph 2 (h-sexies), TUB (so-called IPs);
- securities brokerage firms, as defined by Article 1, paragraph 1(e), TUF (SIM);
- Asset management companies, as defined in Article 1, paragraph 1 (o), TUF (SGR);
- investment companies with variable capital, as defined in Article 1, paragraph 1 (i), TUF (SICAVs);
- investment companies with fixed capital, securities and real estate, as defined in Article 1, paragraph 1, letter i-bis), TUF (SICAF);
- Brokers registered in the register provided for in Article 106 TUB;
- Cassa Depositi e Prestiti S.p.A;
- Insurance companies, which operate in the classes referred to in Article 2, Paragraph 1, CAP;
- Micro-credit providers, pursuant to Article 111 TUB;
- confidi and other entities referred to in Article 112 TUB;
- Established branches of banking and financial intermediaries (referred to in the previous paragraph), having their registered office and head office in another member state or in a third state;
- banking and financial intermediaries (referred to in the previous point) with registered office and central administration in another member state, established without a branch in the territory of the Italian Republic;

2) the persons referred to in Article 3(8) of the Anti-Money Laundering Decree[11] ;
3) The provincial state treasury and the Bank of Italy.

4.8. Suspicious transaction reporting

The bank sends a suspicious transaction report to the FIU, reasonably prior to carrying out the transaction, when it knows, suspects, or has reasonable grounds to suspect the existence or attempted existence of money laundering or terrorist financing transactions or that the funds of the transaction are derived from criminal activity. The suspicion is inferred from the characteristics, size, and nature of the transactions, also taking into account the economic capacity and activity of the person to whom it is reported.

The frequent and unjustified use of cash transactions and the withdrawal or deposit of cash in amounts inconsistent with the client's risk profile constitute suspicious elements.

The management of the process that may lead to the reporting of a suspicious transaction is assigned to the suspicious transaction reporting officer who:

[11] Central securities depositories, companies managing regulated markets for financial instruments, entities managing facilities for trading financial instruments and interbank funds, companies managing settlement services for transactions in financial instruments, companies managing clearing and guarantee systems for transactions in financial instruments.

- Evaluates, in light of all available evidence, the suspicious transactions detected;
- Transmits to the FIU those reports that are deemed well-founded;
- File reports deemed unfounded;
- maintains evidence of the assessments made under the procedure, even if the report is not sent to the FIU.

The bank guarantees all appropriate measures to ensure the confidentiality of the identity of persons reporting a suspicious transaction. In particular, the name of the reporter may never be disclosed, unless the judicial authority deems it essential for the purpose of ascertaining the crimes for which proceedings are being conducted. In any case, the provisions of Article 38 of the Anti-Money Laundering Decree ("Protection of the reporter") shall apply.

It is also prohibited for the persons required to report a suspicious transaction and anyone who has knowledge of it to give notice to the customer concerned or to third parties that a report has been made, that additional information requested by the FIU has been sent, or that there is and/or may be an investigation into the matter. In relation to the processing of personal data related to the reporting and communication activities referred to in this paragraph, the rights referred to in Articles 15 to 18 and 20 to 22 of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 are exercised within the limits provided by Article 2-undecies of Legislative Decree No. 196 of June 30, 2003, as amended.

The reporting of suspicious transactions, made in good faith by the bank, its employees or directors, does not constitute a violation of any reporting restrictions imposed by contract with the customer or by legislative, regulatory or administrative provisions; moreover, it does not entail liability of any kind, even in cases where the reporting party has no knowledge of the underlying criminal activity and regardless of whether the illegal activity was actually carried out.

4.9. Staff Training

Effective implementation of AML/CFT regulations presupposes adequate knowledge of the obligations and responsibilities that can result from failure to comply with the relevant regulations. Hence the need for appropriate ongoing training and education measures for all personnel, with programs that take into account developments in national and international regulations and internal self-regulation (regulations, manuals, procedures, circulars, etc.).

To this end, the bank organizes staff education and training programs and ensures the dissemination of a corporate culture of compliance.

The Managing Director establishes annually, in cooperation with the Group Anti-Money Laundering Service and the Personnel and Organizational Models Service, programs to train and educate personnel on the obligations under the anti-money laundering regulations on a continuous and systematic basis.

Specifically, such training programs:

- ensure increased preparation for employees and collaborators who are in direct contact with customers or otherwise involved in the process of reporting suspicious transactions as well as

those belonging to the Group Anti-Money Laundering service, who are required to be continuously updated on the evolution of money laundering risks and typical patterns of criminal financial transactions;

- ensure that staff are continuously updated on regulatory developments and the risks of money laundering and terrorist financing;
- are carried out periodically and systematically and are submitted annually to the body with management function for approval.

The bank ensures that procedures for internal reporting of violations under Article 48 of the Anti-Money Laundering Decree (so-called "*whistleblowing*") are brought to the attention of all personnel. This task is currently assigned to the Head of Compliance and DPO.

4.10. Information flows

With specific reference to information flows to the FIU, the bank transmits:

- aggregate data concerning its operations, in order to enable the performance of analyses aimed at bringing to light any money laundering or terrorist financing phenomena within certain territorial areas, in accordance with the methods and timing defined by the Authority itself in the "Provisions for sending aggregate data" dated August 25, 2020 (so-called S.AR.A. flows);
- within thirty days from the date of entry into force of EU regulations or decrees issued by the Ministry of Economy and Finance, on the freezing of funds and economic resources held by natural or legal persons, groups or entities engaging in conduct aimed at terrorist acts or the financing of weapons of mass destruction or the threat to international peace and security, the measures applied, indicating the persons involved, the amount and nature of the funds or economic resources;
- promptly, transactions, relationships and any other available information traceable to the designated entities or those in the process of designation in community regulations or decrees issued by the Ministry of Economy and Finance.

With reference to internal reporting within the bank and the Banking Group, the bank has defined the flows that corporate structures must exchange in order to ensure the necessary alignment in the area of AML/CFT risk control, detailed in Annex 1 ("Internal Information Flows") and Annex 2 ("Intra-Group Flows").

The Group AML department has access to all activities of the bank and any information relevant to the performance of its duties, including through direct interview with staff. For this purpose:

- the bank's other structures and/or functions must communicate to it, in a timely and complete manner, any facts relevant to the supervision of the risks in question;
- may request and receive from other structures and/or functions any additional information relevant to the performance of its duties.

4.11. Reporting obligations of the Board of Statutory Auditors and systems for reporting violations

The Board of Statutory Auditors monitors compliance with the regulations on money laundering and terrorist financing. In this regard, it shall report without delay to the Bank of Italy all facts of which it becomes aware in the performance of its duties that may constitute serious or repeated or systematic or multiple violations of the provisions set forth in the law and implementing provisions.

If, in the course of his or her duties, he or she becomes aware of potentially suspicious transactions, he or she shall notify the reporting delegate and the Group AML department.

The bank also has specific procedures for employees and collaborators to report internally potential or actual violations of the provisions dictated for the prevention of money laundering and terrorist financing (*whistleblowing*).

5. SELF-ASSESSMENT OF MONEY LAUNDERING AND TERRORIST FINANCING RISKS AND ANNUAL REPORT

The bank, in accordance with the criteria and methodologies set forth in the Provisions on Organization, Procedures and Controls issued by the Bank of Italy and the "Guidelines on Policies and Procedures Related to Compliance Management and the Role and Responsibilities of the Anti-Money Laundering Officer" issued by the EBA, conducts a self-assessment of the money laundering (ML) and terrorist financing (FT) risk to which it is exposed.

Self-evaluation is conducted based on a methodology that includes the following macro-activities and aspects:

a) Identification of inherent risk (on a four-value judgment scale): current and potential risks to which the bank is exposed are identified, also taking into account elements provided by external information sources. In particular, factors such as customer type, products and services offered, bank operations, distribution channels and geographical area are considered at this stage;

b) vulnerability analysis (on a judgment scale of four values): in this phase the adequacy of the organizational structure, prevention and monitoring principals are analyzed with respect to the risks previously identified in order to identify any vulnerabilities; the attribution of the vulnerability level is accompanied by an overall judgment on the effectiveness of the principals in place as well as a brief illustration of any weaknesses identified, with an explanation of the reasons for the score;

c) determination of residual risk (on a four-value judgment scale): the bank assesses, depending on and in relation to the line of *business, the level of* residual risk to which it is exposed because of the level of inherent risk and the robustness of the mitigation safeguards, making use of the residual risk determination matrix developed by the Bank of Italy;

d) remedial action: the bank, once the residual risk is determined, defines appropriate remedial action and remedies to be taken against any existing critical issues, as well as the adoption of appropriate AML risk prevention and mitigation measures.

With regard to the Banking Group, the head of the Group AML department coordinates the exercise carried out by each of the Group companies and conducts a Group self-assessment exercise, the results of which are evaluated by the Board of Directors, after consideration by the Audit and Risk Committee, the Board of Statutory Auditors, the Internal Audit department and the Risk Control department.

The self-assessment exercise, referring to both the Parent Company and the Banking Group as a whole, together with the Parent Company's annual report, is updated annually by the Group's AML department and submitted to the Bank of Italy by April 30 of the year following the year in which the assessment was made. It is also promptly updated when significant new risks emerge or significant changes occur in existing risks, operations, or organizational or corporate structure.

In addition, the findings of this activity contribute to the definition of the *Risk Appetite Framework of the* Bank and the Banking Group.

The annual report should include the following information:

1) As part of the risk assessment of ML/FT:
    a. a summary of the main findings of the risk assessment at the business area level; whether an update to this effect was carried out in the previous year; and whether supervisory authorities have requested updates in this regard;
    b. description of any related changes to customer profiling criteria, highlighting whether they are in line with the ML/FT risk assessment at the level of the company's business;
    c. Classification of customers by risk and indication of the number of customers, broken down by risk band, in relation to which the review and update of due diligence has not yet been completed;
    d. Statistical data concerning:
        i. Number of anomalous transactions identified;
        ii. Number of abnormal transactions analyzed;
        iii. Number of suspicious transaction reports forwarded to the FIU, broken down by country in which the transactions took place;
        iv. Number of reports closed due to AML/CFT-related anomalies;
        v. Number of requests for information received from FIU, the Judicial Authority, and investigative and law enforcement agencies;
2) Relative to resources:
    a. Description of the organizational structure of the Group AML service;
    b. Description of the human and technical resources assigned to the Group AML service;
    c. where present, list of outsourced processes in AML/CFT and description of supervision performed;
    d. Description of completed AML/CFT training activities and training plan for the following year;
3) On policies and procedures:
    a. summary of the most important measures and procedures taken during the year, including recommendations, problems, deficiencies or irregularities identified;
    b. control actions taken to assess the implementation of AML/CFT policies, controls, and procedures by employees, agents, distributors, etc., as well as the adequacy of control tools employed by the bank for AML/CFT purposes;
    c. Group AML service activity plan for the coming year;
    d. findings of internal and external reviews in AML/CFT and any progress made against them;

e. supervisory activities carried out by the Competent Authorities, violations identified and any penalties imposed, together with the actions taken to remedy the violations identified, with their status.

Using the same methodologies, the head of the Group AML department prepares an interim (semi-annual) summary report, including the self-assessment of ML/FT risks, the outcomes of which are evaluated by the Board of Directors, after review by the Audit and Risk Committee, the Board of Statutory Auditors, the Internal Audit department and the Risk Control department.

Following is the outline of the annual report according to Bank of Italy guidelines:

1	Description and location of the AML function in the corporate (or group) organization, including changes during the year, assigned human and technical resources, and outsourced processes
2	Activities of the anti-money laundering function during the reporting period, any dysfunctions found and related corrective actions in the areas:
	a. of due diligence and customer profiling. In this regard, specific details should be provided about: any delays in completing due diligence, including failure to identify the beneficial owner; the distribution of customers (in absolute terms and as a percentage of existing customers) across risk classes
	b. Of data retention
	c. Of the suspicious transaction detection and reporting process (indicating the number of reports sent to the FIU in the year and those assessed and filed)
	d. Of the identification and enforcement of international financial sanctions against terrorism and the proliferation of weapons of mass destruction
3	Money laundering risk self-assessment exercise
4	Adaptation initiatives defined in light of the findings of the AML risk self-assessment exercise and their status
5	Training activities carried out in the reporting period and planned for the following year
6	Intermediary-specific issues, if any, and other relevant news
7	Activity plan of the anti-money laundering function for the following year
8	Number of client relationships closed due to AML-related anomalies
9	Any dysfunctions established by other internal control functions and corrective measures implemented
10	Communications exchanged with the supervisory authority, including sanctions imposed and corrective actions requested by the supervisory authority
11	Number of requests for information received from the FIU, judicial authority and investigative and law enforcement agencies

Annex 1 - INTERNAL INFORMATION FLOWS.

INFORMATION FLOW	SENDER	WAYS.	RECIPIENT	PERIODICITY.
1. Annual report and self-assessment	Group Anti-Money Laundering Service	• Through the person responsible for anti-money laundering.	• Board of Directors • Audit and Risk Committee • Audit Board • Internal Audit Service • Chief Risk Officer	Annual
2. Semiannual report on operations and interim self-assessment	Group Anti-Money Laundering Service	• Through the person responsible for anti-money laundering.	• Board of Directors • Audit and Risk Committee • Audit Board • Internal Audit Service • Chief Risk Officer	Semiannual
3. Reports of significant violations or deficiencies found in the performance of relevant duties and on violations pursuant to Art. 46, para. 1, lett. b) and Art. 51, para. 1 of Legislative Decree 231/2007, for subsequent reporting to the Supervisory Authority or the MEF	Group Anti-Money Laundering Service	• Directly	• Board of Directors • Audit and Risk Committee • Audit Board • Supervisory body	A event
4. Group quarterly indicators	Group Anti-Money Laundering Service	• Directly	• Managing director • Exponent responsible for anti-money laundering. • Audit and Risk Committee • Audit Board • Chief Risk Officer • Head of Internal Audit • Risk Committee	Quarterly
5. Disclosure of specific requests from supervisory authorities	Group Anti-Money Laundering Service	• Through the person responsible for anti-money laundering.	• Board of Directors • Audit and Risk Committee • Audit Board	A event
6. Assessing risks associated with introducing new products and services, significantly modifying products or services already offered, entering a new market, or starting new activities	Group Anti-Money Laundering Service	• Directly	• Managing director	A event
7. Minutes of second-level audits where irregularities or failures in AML/CFT risk control safeguards were found, including at the Banking Group level	Group Anti-Money Laundering Service	• Directly	• Managing director • Exponent responsible for anti-money laundering. • Audit Board • Audit and Risk Committee • Head of Internal Audit • *Chief Risk Officer*	A event
8. Minutes of audits where irregularities or failures in AML/CFT	internal audit service	n.a.	• Managing director • Exponent responsible for anti-money laundering.	A event

INFORMATION FLOW	SENDER	WAYS.	RECIPIENT	PERIODICITY.
risk control safeguards were found, including at the Banking Group level			• Audit Board • Group anti-money laundering service manager; • Group AML office manager; • BPS AML office manager	

Annex 2 - INFRA GROUP INFORMATION FLOWS

INFORMATION FLOW	SENDER	RECIPIENT	PERIODICITY.
1. Annual report and self-assessment	AML structure of the subsidiary	• Group Anti-Money Laundering Service • Exponent responsible for anti-money laundering of BPS and Group	Annual
2. Semiannual report on operations and interim self-assessment	AML structure of the subsidiary	• Group Anti-Money Laundering Service • Exponent responsible for anti-money laundering of BPS and Group	Semiannual
3. Risk indicators established by the group AML department	AML structure of the subsidiary	• Group Anti-Money Laundering Service • Exponent responsible for anti-money laundering of BPS and Group	Monthly
4. Reporting significant anomalies, violations, or deficiencies found	AML structure of the subsidiary	• Group Anti-Money Laundering Service • Exponent responsible for anti-money laundering of BPS and Group	A event
5. Minutes of audits in which irregularities or non-compliance in the AML/CFT risk control safeguards of subsidiaries were found	Internal audit	• Managing director • Exponent responsible for anti-money laundering of BPS and Group • Audit Board • Group Anti-Money Laundering Service	A event