Global Policy

Anti-Money Laundering and Anti-Terrorism Policy

FB 081_2021

Approving Function	Board of Directors	**Date** December 2021
Proposer Function	Chief Executive Officer and General Manager	

Index

1. Introduction and purpose of the Policy

FinecoBank S.p.A, as Parent Company - in accordance with the current laws and regulations and in line with the Group's management coordination system as defined in the Group Managerial Golden Rules, issues guidance in order to promote the Group's stability and to ensure a consistent and cohesive approach to the business strategy and overall operation.

This document complement the Group rules, it is directly applicable to the Parent and it is addressed to the Group Companies (Entities or Companies) proportionally, i.e. by taking into account the economic relevance, the operational and organisational size and complexity.

FinecoBank as Parent in order to guarantee uniform behaviours by the Group Companies in important areas such as the fight against money laundering and terrorism financing issues this Global Policy – "Anti-Money Laundering and Anti-Terrorism Policy" (hereafter also "Global Policy "or "Policy").

As defined in the Group Managerial Golden Rules, this document will be adopted in accordance with the regulatory requirements applicable locally; in case of any conflicts between this Policy and the applicable local law (or in case of stricter rules) the latter will prevail.

After the approval, Fineco as Parent Company, is sending the GP to the Entities for approval by the respective Corporate Bodies and is monitoring its correct and timely implementation, availing also of its internal functions identified from time to time. Following the distribution of the rule, the Competent Function of the Parent will monitor the adoption and implementation of the rule

With respect to the current document, the Board of Directors is the relevant body in charge of the approval of same.

Group's Companies are required to promptly start – following the relevant assessment and approval by the competent body – the necessary activities aiming at ensuring the appropriate applicability of the current policy.

If a Company considers that:

1. this Global Rule is not applicable, or
2. changes/exceptions to the provisions contained in this Global Rule are necessary in order to comply with local laws (if more restrictive) or due to organisational and operational constraints,

the Company must submit a request for a Non-Binding Opinion to the Parent Company's Compliance function, in accordance with the provisions of the current Group regulations (Management of Group Regulations).

This Policy:

1. Illustrates and justifies the decisions made by the Group in relation to money laundering and terrorism financing in terms of the organisational structures, procedures and internal controls, due diligence and data retention in accordance with the principle of proportionality and the effect of exposure to the risk of money laundering;

2. outlines the AML Programme defined by the Parent Company by providing for:

    - the AML Business Risk Assessment;
    - monitoring of regulatory developments in relation to provisions concerning customer due diligence;
    - screening of customers;
    - transaction monitoring post-execution;
    - procedures for the internal reporting and investigation of potentially suspicious transactions and, if necessary, external reports of these transactions to the relevant Authorities;

- documents retention;
- staff training;
- information management and reporting;
- procedures for monitoring the efficacy of the above controls, and
- preventing the financing of terrorism.

3. provides a regulatory framework to identify the potential risks of money laundering and terrorism financing (hereinafter collectively "money laundering risk"), by setting the minimum standards for the AML Programmes to which the Group Companies must refer.

2. Recipients

The Policy is addressed to all Group Companies and applies to all Employees.

The Group Companies must deal with potential regulatory, legal and reputational risks in the areas of money laundering and counter terrorism financing, both because there are customers located in countries with different levels of financial crime risk and different regulatory systems, and also because of the wide range of products and services they offer.

Employees must always pay attention to situations that present a potential risk of money laundering and terrorism financing, managing these risks in accordance with this Policy and the regulations to which it is connected/linked.

If an Employee suspects that a particular activity/behaviour can be associated to money laundering instances, he is required to report this immediately in accordance with the procedure outlined in this Policy, and the internal regulations set by the Parent Company. Otherwise, the Group Companies and/or Employees may incur administrative or criminal penalties. Failing to comply with this Policy or breaching of this Policy may result in disciplinary action – in addition to the measures provided for by law – including, in serious cases, termination of the contract of employment.

Offering assistance to money laundering or the funding of terrorism, failing to identify and/or report suspicious transactions or informing the person involved in a suspicious transaction that the same has been reported may have serious legal consequences, including imprisonment.

3. The reference regulatory framework

This Policy has been drafted in accordance with the current regulatory provisions in force in the EU and in Italy, of which the principal ones are outlined below:

- Directive (EU) 2015/849 or 4th AML/CFT Directive on the prevention of the use of the financial system for the purposes of money laundering or the financing of terrorism, as locally implemented in the States where the the Group's Companies operates;

- Regulation EC 2015/847 concerning information on payers and payees accompanying transfers of funds;

- Directive (EU) 2018/843 or the 5th AML/CFT Directive as locally implemented in the States where the the Group's Companies operates, which repealed Directive 2005/60/EC and 2006/70/EC and amended the 4th AML Directive.

- Directive (EU) 2018/1673 on combating money laundering by criminal law as locally implemented in the States where the the Group's Companies operates (D. Lgs nr 195/2021 in Italy);

- EBA Guidelines on customer due diligence and the AML risk factors dated 1 march 2021 as locally implemented in the States where the Group's Companies operates

In particular, for the Parent Company only, the following regulatory references have also been considered:

- Legislative Decree 231/2007 as amended by Legislative Decree 90 of 2017, which enacted the 4th AML/CFT Directive into Italian law.

- Legislative Decree 109/2007 on measures to prevent, combat and repress the financing of terrorism and activities of countries that threaten peace and international security, implementing Directive 2005/60/EC.

- Legislative Decree 125/2019 enacting the 5th AML/CFT Directive into Italian law

- Bank of Italy provision of 26 March 2019 containing implementing provisions on organisation, procedures and controls on AML

- Bank of Italy provision of 30 July 2019 containing implementing provisions concerning customer due diligence.

- Bank of Italy provision of 24 march 2020 with respect to "rules on record keeping and making documents, data and information available to contrast money laundering and terrorist financing".

4. Glossary and Acronyms

Key words	Definition
Customer Due Diligence or Know Your Customer (KYC)	Due diligence that the Group's Companies are required to carry out in order to identify its customers and to verify information which is relevant before entering into operations with them
Senior Management	For the purpose of the current Rule the general manager, its deputies and those performing equivalent functions as well as the managers and officers of the internal control function. For FinecoBank, this is the CEO, the general manager, the deputy general manager and the heads of the corporate control functions.
Top Manager	For the purpose of the current Rule, a director, the general manager or another employee delegated by the t body with management functions or by the general manager to handle relations with high risk customers; a top manager has suitable knowledge of the risk of money laundering or the financing of terrorism to which the recipient is exposed, and has sufficient autonomy to be able to take decisions that affect this level of risk. For FinecoBank this relates to employees identified in the Delegated Powers document approved by the Board of Directors.
Supervisory Authorities	Authorities responsible for the supervision and control of banking and financial intermediaries, responsible for issuing specific regulations on anti-money laundering and antiterrorism, and who must therefore be respected by the Fineco Group, where applicable. In Italy, these Authorities are those indicated in Title I, Chapter II of Legislative Decree 231/2007.
Intermediate Shareholder	A legal entity in an intermediate position in the chain of control between the Customer and the ultimate owner, who owns or controls at least 25% of the capital of the Customer.

Criminal Activity	As defined in the Art. 2 of the EU Directive 2018/1673, offences within the following categories are considered a criminal activity: • participation in an organised criminal group and racketeering • terrorism • trafficking in human beings and migrant smuggling • sexual exploitation • illicit trafficking in narcotic drugs and psychotropic substances, • illicit arms trafficking; • illicit trafficking in stolen goods and other goods; • corruption, • fraud, • counterfeiting of currency, • counterfeiting and piracy of products; • environmental crime, • murder, grievous bodily injury; • kidnapping, illegal restraint and hostage-taking; • robbery or theft; • smuggling; • tax crimes relating to direct and indirect taxes, as laid down in national law; • extortion; • forgery; • piracy; • insider trading and market manipulation • cybercrime
Shell Bank	Bank (or a financial intermediary performing functions similar to a bank) with no significant establishment in the country in which it is formed and licensed to exercise its business, and which does not belong to a financial group that is subject to effective, consolidated supervision.
Parent Company	FinecoBank S.p.A. (hereinafter also “FinecoBank” “Fineco” or the “Bank”)
Customer/Client	The person who enters into or conducts ongoing relations or carries out occasional operations with persons to whom these anti- (for the Parent, with or without holding a current account) money laundering and anti-terrorism provisions apply; in the case of ongoing relations or occasional operations with multiple parties, each of these parties will be considered a Customer
Corporate Customers	Customers other than natural persons (companies and legal institutions) who generally but not exclusively have a separate identity from that of their owners and controlling entities. For example, trusts do not always have a separate identity but this term also includes trusts.
Private Banking Customers[1]	Clients owing significant portfolio of assets, associated to a Financial Advisor – the Relationship Manager (i.e. the Financial Advisor) who on a continuous basis looks after the customised relationship with the clients being these latter recipient of customised financial and banking services.
Subsidiary	Entity directly or indirectly controlled by FinecoBank S.p.A. (hereinafter also "Subsidiary Entity", or "Subsidiary Company" or “LE”)
Additional Name Checks	Searches carried out by an external media provider in order to identify reputational and/or legal issues related to a Customer, such as adverse information, sanctions, PEP, etc. An example of an external media provider is World Check which is operated by Global World-Check

[1] Clients qualified as “Private “exclusively for commercial purposes, to whom favorable economic conditions are assigned without benefiting of customized banking services are not in the scope of this definition.

	Holdings Limited. The Internet (i.e Google as search engine) may also be used for further searches. See below “Standard Name Checks”.
Standard Name Checks	Searches on names of customers and Connected Parties whose names are contained on the relevant lists of sanctioned individuals, and also the internal Fineco lists.
Employees	For the purposes of this Rule and regardless of current labour law, Employees are considered to be all members of the strategic supervision, management and control bodies, employees, single-client agents (for example financial advisers licensed for distance selling), freelance or contract workers, any other individual with a contract of employment (including trainees) and temporary staff.
Regulated Entity	A credit or financial institution (including banks whose licence is not limited to offshore banking activities), intermediaries, insurance companies, management companies of collective investment funds and regulated funds which are subject to the regulations issued by a supervisory authority.
Financing of terrorism	The provision or collection of funds in any form, conducted directly or indirectly with the aim or in the awareness that these funds will be fully or partially used to carry out terrorist acts. Funds used to finance terrorism may come from lawful or illegal activities.
Signatory	Delegate or representative with the power to bind the company in an agreement or transaction.
Recognised Data Source	A source of data which the Bank or Group recognises as such to collect information and/or verify elements of a Customer’s identity.
Group	FinecoBank Group, consisting of FinecoBank S.p.A. and the Group Companies/Legal Entities (hereinafter also “Fineco Group” or FinecoBank Group))
Address of the principal place of business	The principal place of the ordinary business conducted by the Customer. This is normally the same as the company’s head office (general headquarters).
Occasional Transaction	An operation that is not related to an ongoing relationship with the Customer, whether it is carried out as a single transaction or whether it includes multiple transactions that appear to be connected (for ex.transactions related to the purchase of tax receivables from third parties not holding a current account, negotiated within the same master agreement).
Corporate Bodies	All of the supervisory, management and control bodies. At FinecoBank, these organs are considered to be the Board of Directors, the CEO and General Manager and the Board of Statutory Auditors.
Origin of Funds	The origin of the funds in a commercial relationship or occasional transaction. This includes both the activities that generated the funds used in the Commercial Relationship and also the methods by which the Customer’s funds were transferred.
Origin of Assets	The economic activity that generated the net worth of a natural person or corporate Customer. This may come from business activities, the sale of assets or goods, savings from paid employment, a loan etc.
High Risk Third Countries	Countries that do not belong to the European Economic Area and which have strategic deficiencies in their respective national rules for the prevention of money laundering and financing of terrorism, as identified by the European Commission in the exercise of the powers regulated by

	Articles 9 and 64 of the AML Directive;
Distance Transactions	Distance transactions are those carried out without the physical presence on the intermediary's premises of the Customer, the employees of the intermediary or other personnel commissioned by the intermediary (for example through telephone or online communications systems); when the Customer is a person other than a natural person, the Customer is considered present when they are the Executor.
Politically Exposed Person (PEP)	Any person who holds (or has held within the last 12 months) a prominent or important public position or who is closely connected, through a direct family relationship, with a person in such a position.
Red Flags	Types or indicators of risk used to identify behaviours that are generally linked to money laundering or the financing of terrorism.
Prohibited Business Relations	Banking relations which must not be initiated or which must be closed, by virtue of regulatory requirements or internal policies.
Remote Banking	A banking operation carried out through electronic means from a remote station (such as a telephone bank, Internet banking using PCs or mobile devices) in which the contract with the Customer is executed without face-to-face meetings.
Money laundering	Activities aimed at concealing the illegal origin of the proceeds of crime by creating the semblance of a legitimate origin, even if the activities that generated the capital to be laundered were carried out abroad. Under the applicable AML law a. the conversion or transfer of assets, carried out in the knowledge that they originate from a criminal activity or from participation in such activity, for the purpose of concealing or disguising the unlawful origin of the assets or assisting anyone involved in such activity to avoid the legal consequences of their actions; b. the concealing or disguising of the true nature, origin, location, availability, movement or ownership of the assets or the rights to them, carried out in the knowledge that they originate from criminal activity or from participation in such activity; c. the purchase, holding or use of assets, in the knowledge, at the time of their receipt, that the assets originate from criminal activity or from participation in such activity; d. participation in one of the actions referred to above, association for the purpose of committing said action, attempting to perpetrate it, assisting, instigating or advising someone to commit it or facilitating its execution;
High-risk Sector	Sector defined by the Bank as being exposed to corruption, bribery, fraud or other financial offences, to behaviours aimed at laundering illegally-gained proceeds, or funds destined to finance terrorism.
Fiduciary Company	The company set up to hold (as the registered owner) and to administer, as trustee, assets on behalf of another person or company.
Group Companies	Companies of the FinecoBank Group, which is the Parent Company FinecoBank and its Subsidiaries.
Group Controlled Entity	Entity directly or indirectly controlled by FinecoBank S.p.A.(also "Controlled Entity" or "Controlled Company" or briefly "LE" hereafter)
Connected Party	The persons within the chain of ownership and control who exercise day-to-day control, the authorised signatories, the legal representative and the Beneficial Owners.

Sanctioned Person	A person, company, or nation for whom there is a legal prohibition/limitation on undertaking commercial relations or carrying out transactions (European Union, OFAC-USA, or other authorities or international or local government agencies).
Beneficial Owner	The natural person or persons on behalf of whom the Customer establishes an ongoing relationship or carries out a transaction (in brief "beneficial owner type 1"); If the Customer or person on behalf of whom the Customer establishes an ongoing relationship or carries out a transaction is an entity other than a natural person: the natural person or persons to whom the direct or indirect ownership of the entity or the relative control can be attributed, or who are the beneficiaries of it (in brief “beneficial owner type 2”).
Funds transfer	Any operation performed using electronic means on behalf of an initiator through a Payment Services Provider with the purpose of making funds available to a beneficiary through a Payment Services Provider, regardless of whether the initiator and the beneficiary are the same person.
Identity checks	Check of the authenticity of documentary evidence presented by Customer or by a Recognised Data Source to validate information about identity.

Acronym	Definition
AFC	Anti-Financial Crime
AML	Anti-Money Laundering
CDD	Customer Due Diligence
CTF	Countering of Terrorist Financing
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
KYC	Know Your Customer
KYT	Know Your Transaction
OFAC	US Office of Foreign Assets Control of the US Department of the Treasury
PEP	Politically Exposed Person
SAR	Suspicious Activity Report
SDD	Simplified Due Diligence
SPV	Special Purpose Vehicles
STR	Suspicious Transaction Report
FIU	Financial Information Unit of the Bank of Italy

5. Role and responsibilities of the Parent Company's Corporate Bodies

5.1. Body with strategic supervisory functions

Fineco's Board of Directors, in its role as body in charge of strategic supervision, approves and periodically reviews the strategy and governance policies relating to the risk of money laundering; these policies are adapted to the entity and the type of risks the Bank's activities are actually exposed to, in accordance with the risk-based approach, on which the AML risk self-assessment exercise is based.

Specifically, Fineco's Board of Directors

- approves this Policy, and all its updates, which illustrates and justifies the decisions made by Bank in terms of organisational structures, procedures and internal controls, due diligence and data retention in accordance with the principle of proportionality and the effective exposure to the risk of money laundering;
- approves the establishment of the AML Function, identifying its tasks and responsibilities, the way it is coordinated, and its collaboration with the other control functions;
- approves the guidelines for the system of internal controls which is organic and coordinated, and is able to promptly detect and manage the risk of money laundering and ensure its efficacy over time;
- approves the principles for the management of relations with customers classified as "high risk";
- appoints or revokes the person responsible for reporting suspicious transactions and the AML Manager, with the support of the Nominations Committee, subject to the opinion of the Risks and Related Parties Committee (CRPC") after consulting the body with control functions;
- ensures that the duties and responsibilities relating to anti-money laundering have been clearly and appropriately allocated, ensuring that the operational departments are separate from the control departments and that they have sufficient qualified members of staff;
- ensures that there is an adequate, complete and prompt flow of information to the company bodies and the control functions;
- guarantees confidentiality in the context of the procedure for reporting suspicious transactions;
- at least once a year, examines the reports on the work done by the Head of the AML Function and the controls carried out by the relevant departments as well as the document on the results of the AML risk self-assessment;
- makes sure that any shortcomings or anomalies found as a result of the controls at various levels are duly brought to its attention, and takes appropriate corrective measures, evaluating their efficacy;
- evaluates the risk of operating with third countries which are associated with higher AML risks; assesses the AML risks, identifies controls to mitigate these risks and monitors their efficacy.

5.2. Body with Management functions

Fineco's Body with Management functions is the CEO and General Manager.

The Body with Management functions:

- implements the strategic guidelines and governance policies for AML risk, as approved by the body with strategic supervision function and is responsible for taking all the measures necessary to ensure the efficacy of the organisation and system of the AML controls. In preparing the work procedures, it takes into account the indications and guidelines emerging from the competent authorities and international bodies.

- defines and implements a system of internal controls which is able to promptly detect and manage the risk of money laundering and ensures its efficacy over time, in line with the results of the risk self-assessment exercise;

- ensures that the operational procedures and information systems allow the proper fulfilment of the customer due diligence obligations and the obligation to conserve documents and information.

- With regard to the reporting of suspicious transactions, the Management Body will define and implement a procedure which is adequate to the specific nature of this activity, to the size and complexity of the Bank in accordance with the principle of proportionality and the risk-based approach

The Body with Management functions also:

- duly fulfils the obligations to report to the Authorities as required by the AML regulations.
- defines the AML Policy which is submitted for approval by the body responsible for strategic supervision, and ensures that the Policy is implemented;
- defines and implements flows and information procedures in order to assure knowledge of the risk factors, for all the company departments involved, and for the bodies responsible for the control functions;
- defines and implements a procedure for managing relations with customers classified as “high risk” in accordance with the principles set by the strategic supervision body;
- draws up the programmes for the training and guidance of personnel on the obligations provided for in the AML regulations; this training must be continuous and systematic and must take into account changes in the law and regulations, and in the procedures put in place by the recipient;
- establishes which tools are appropriate to allow the verification of work done by personnel, in order to highlight any irregularities in behaviours, in the quality of communications sent to co-workers and to company departments, and in staff relations with customers;
- in cases of remote operations (for example through digital channels), it assures that specific information procedures are used in order to comply with AML regulations with particular reference to the automatic identification of irregular operations.

5.3. Body with Control functions

The Body with Control functions (the Board of Statutory Auditors) oversees compliance with the regulations and the completeness, functionality and adequacy of the AML control systems. In the exercise of its powers, it relies on the internal departments to carry out the necessary checks and uses the information received from the other Corporate Bodies, the AML Manager and, where present, from the other internal control functions.

In this regard, the Body with Control functions:

- evaluates the suitability of the procedures for customer due diligence, conservation of information and reporting of suspicious transactions;
- analyses the reasons for the deficiencies, anomalies and irregularities found, and ensures that the appropriate corrective measures are adopted;
- is consulted in the context of the procedures for appointing the head of the AML Function and the suspicious transactions reporting officer, and in defining the elements of the overall structure of the system for the management and control of AML risk.
- immediately informs the Bank of Italy of any events it becomes aware of in the exercise of its functions, which could constitute serious, repeated, systematic or multiple violations of the applicable provisions of law and of the related enacting provisions.

6. Role and responsibility of the Company Functions

6.1. The AML Function of the Parent Company and of the Subsidiaries

The AML Function is the function responsible for preventing and combating money-laundering operations.
The AML Function is independent, has enough suitably qualified staff to fulfil its tasks in terms of quality and quantity, reports directly to the strategic supervision, management and control bodies and has access to all activities as well as any information that is relevant for the carrying out of its duties.

The AML Function is responsible for:

a) identifying laws, regulations and guidelines at local level and for assessing their impact on internal processes and procedures and for monitoring changes to them in order to guarantee the related internal updates;
b) helping to define the system of internal controls and procedures aimed at the prevention and combating of the risks of money laundering;
c) conducting ongoing checks on the adequacy of the process of managing the risks of money laundering and suitability of the system of internal controls and procedures, and for proposing, with the involvement of the other company departments involved, any organisational and procedural changes which are necessary or appropriate in order to ensure an adequate level of control of risk;
d) conducting checks on the functionality of the reporting process in collaboration with the officer responsible for reporting suspicious transactions ("SAR/STR"), and for checking the congruency of the level I assessments on customer operations;
e) assisting with the definition of AML governance policies and of the risk management process, as well as the various phases of the process of managing this risk;
f) conducting, in collaboration with the other company departments involved, the annual self-assessment of money laundering risks, where this is required by the local regulations;
g) providing support, assistance and advice to the Company Bodies and to Top Management (also in the case of new products and services), as well as on issues relating to the opening or closing of customer accounts;
h) pre-assessing the AML risk connected to the offer of new products or services;
i) evaluating the reliability of the information system used for customer due diligence, the conservation of data and the reporting of suspicious transactions;
j) providing monthly submissions to the local authority (the FIU for the Parent Company) of aggregate data on the Bank's overall operations, where required by the local regulations;
k) providing monthly submissions to the local authorities (the FIU for the Parent Company) based on their instructions, the "Objective Communications" about operations at risk of money laundering, where required by the local regulations;
l) putting in place, in collaboration with the other company departments responsible for training, an adequate training plan in order to obtain an ongoing update of employees and contractors, and to raise their awareness of compliance with this Policy and with the regulatory requirements;
m) duly informing the Company Bodies of any significant violations or shortcomings detected in the exercise of their duties, or in general;
n) providing information to the Company Bodies and to Top Management.

the Parent Company's AML Function, and where required by local regulations, the function of the Subsidiaries, will prepare and send to the body with management functions and to the body with strategic supervision functions a document that sets out in detail the responsibilities, duties and operational procedures for the management of AML risk (the AML Manual). This document is regularly updated and is available and easily accessible to all staff.

The AML Function of the Parent Company and of the Subsidiaries pays particular attention to: the adequacy of the internal systems and procedures in relation to customer due diligence and registration requirements, as well as the systems for detecting, assessing and reporting suspicious transactions; the efficient registration of any other situation that requires disclosure, and the appropriate conservation of documentation and evidence as required by law.

At least once a year, the AML Function will present to the strategic supervision, management control bodies and to the CRPC (for the Parent Company, or equivalent bodies for the Subsidiaries) with a report on the

actions taken, any malfunctions found, and the related corrective actions to be taken as well as on staff training and the self-assessment exercise, where this is required by the local regulations.

The AML Function of the Parent Company is part of the Parent Company's Compliance Department.

6.2. The Head of the AML Function of the Parent Company and of the Subsidiaries

The Head of the AML Function and must have the appropriate requirements of independence, influence and professionalism; the Head of the AML Function reports directly to the Governance Bodies of the respective Group Companies.

The Head of the AML Function is not in charge of operational areas, nor is hierarchically dependent on persons responsible for these areas.

The Parent Company's Head of AML Function is responsible for:

- preparing an effective AML Programme (including the relevant Group Rules);
- providing advice, coordinating and supervising the implementation of the Group Companies' AML Programmes;
- examining the periodic information received from the Subsidiaries and acting jointly with the local AML Managers to take any necessary corrective or improvement actions.

The Head of the AML Function of the Subsidiary, with the support of the teams and staff operating in the local AML Function, is responsible for:

- implementing the AML Programme in line with the Parent Company's guidelines;
- carrying out AML and antiterrorism controls in accordance with the Global Rules;
- carrying out the business risk assessment exercise and the assessment of AML risk;
- identifying and analysing any irregularities or suspicious transactions identified and reported to the local authorities as required by the local regulations;
- monitoring local regulatory developments and proposing any necessary adaptations;
- preparing periodic reports for the Parent Company, containing at least the above information.

In relation to any adjustment or implementation by the Subsidiaries, the Head of the AML Function of the Parent Company relies on the AML and Anti-terrorism Unit, by setting the minimum AML standards for each Group Legal Entity.

6.3. Parent Company - Anti-Money Laundering and Anti-Terrorism Service Unit and the Money Laundering Reporting Officer (MLRO)

The operational role of the AML Function is mainly attributed to the Anti-Money Laundering and Anti-Terrorism Service Unit (the "AML Unit").
The activities and duties of the AML Unit are defined in the Bank's AML Manual and in the company processes.

Within the AML Function works the Unit dedicated to the reporting of suspicious transactions, headed by the MLRO, who is appointed by a resolution of the Board of Directors, after consulting the Board of Statutory Auditors with the support of the Nominations Committee subject to the opinion of the Risks and Related Parties Committee (CRPC"). The Bank puts in place internal processes and procedures to regulate the activities performed by the MLRO and the SAR/STR team, who assess potential suspicious transactions for subsequent forwarding to the FIU.

6.4. Parent Company – Other Functions

Subject to the obligation to adjust the AML organisational structures according to the principle of proportionality and the risk-based approach, the Bank allocates specific responsibilities (which are allocated to the unit indicated in brackets in the following list), in relation to the:

- Ongoing verification of the adequacy of the AML structure and its compliance with the regulations (Internal Audit)
- Implementation of the rules for identifying and verifying customer data and due diligence data (Back Office)
- Implementation of the second level controls safeguarding the AML&CFT risk (compliance Seconl Level Controls)
- Preparation and updating of the business processes that include the line checks (which is done by Business Development and Business Continuity in collaboration with the relevant Process Owner);
- definition of specific staff training programmes (HR);
- preparation and management of supporting IT tools (ICT).

The various business units who are responsible for each task will work with the AML Function and are responsible for providing it with any information about internal or external events that may have potential AML implications.

7. AML Business Risk Assessment

The Group Companies will assess the AML risk connected to the products or services they offer. The risk assessment will consider, at minimum, the AML risk presented by the customers, products and services, by the jurisdictions in which the Group Companies operate or offer their services and by the transactions or retail channels used to serve customers. The risk assessment must be adequate for the nature and size of the units and of the business and it is documented and communicated at least once a year to the Company Bodies, by the business units' AML Function.

The AML risk assessment is used to adjust both the customer due diligence and the procedures used to monitor operations for each category of customer risk. After completing the risk assessment, the Group Companies will ensure that they have adequate resources, internal regulations, procedures and controls to mitigate the identified risks as far as possible, including the assessment of the emerging risks so that these are timely included in the overall AML&CFT risk assessment of the Bank and the Group.
To identify the customer risk profile, the Group Companies, where appropriate, will draw information from all available sources and documents, including the official reports published by European and Italian authorities (the Supranational Risk Assessment Report of the European Commission, the National Risk Analysis by the Financial Security Committee) and other documents from other regulators and other local authorities.

The AML&CTF risk assessment ("AML Business Risk Assessment") is a process updated every three months to incorporate possible changes that might occur on the organisational AML framework. The AML Risk Assessment must be approved by the Board of Director and pre.validated by the CRPC (for the parent only) and is transmitted to the Competent Authority where this is required by the local laws.

7.1. Customer risk assessment and classification

Customers must be assessed individually in order to identify and classify the level of risk of money laundering, terrorism financing to determine whether it would be appropriate to enter into relations with the Customer. The assessment of Customer risk and the classification of the Customer in terms of the risk of money laundering essentially follows a risk-based approach, so that the checks (such as due diligence measures and the monitoring of transactions) and the use of resources can be concentrated on the riskier customers. In identifying the risk factors pertaining to a Customer, the Parent Company will also consider the Beneficial Owner and, if relevant, the Executor, as indicated in the following sections.

RISK-BASED APPROACH

In order to assess the risk of money laundering and financing of terrorism, the Group Companies will consider the characteristics of the Customer, their conduct, the professional activity carried out, his reputation and the specific nature of the operation or ongoing relationship to be established.

In particular, the following risk factors will be considered:

- Country risk, which is the geographical area of residence or establishment of the Customer or the Beneficial Owner e connected person, the geographical area where the work activities or work relationships take place;
- Sector risk and the main activity performed by the Customer and by the Beneficial Owner;
- The risk of the requested product and service;
- Entity risk, for customers other than natural persons;
- PEP risk;
- Distribution channel risk
- Reputational risk (e.g. negative information).

The Group Companies, in proportion to their size and type of business, will have procedures designed to ensure that all new customers and, where relevant, the directors, beneficial owners and other related parties (the legal representative and authorised delegate) undergo screening using a database containing:

- lists of the Sanctions in accordance with the requirements of the internal regulations on Financial Sanctions;
- the PEP lists provided by an influential commercial organisation such as World Check;
- any other internal lists that may be issued from time to time by the Parent Company and/or by the Subsidiaries;
- a list of negative information provided by an influential commercial organisation such as World Check

The Group Companies will assess the AML risk for each Customer based on the elements obtained through the due diligence – also using a relevant questionnaire – and the checks carried out; they will allocate the risk profile according to three categories (“low”; “medium”; “high”) as described in more detail below.

The risk profile can be seen by the operators involved, and searches can be made using different search parameters.

The Group Companies will utilise at least the following factors, to determine the methodology to classify the Customer risk profile:

COUNTRY RISK

Country risk is the risk of committing Criminal Activities for countries from which the customers, beneficial owners and executors originate or where they operate, in other words the risk that those customers will be involved in some kind of criminal activities due to their place of origin or place of activity: money laundering, terrorism financing, corruption, fraud or a combination of these.

The regulations on Financial Sanctions identify countries, which are sanctioned, while the classification of country risk in the categories of low, medium or high risk is indicated in the GOR – Customer Due Diligence Requirements for AML. The classification takes into account the political stability of the country, its AML controls and prevention systems and its vulnerability to financial crime.

For the purposes of classifying Customer risk, the following criteria are relevant (for the Customer itself, for the Beneficial Owner and, where relevant, the Executor):

- for natural persons: the country in which they are resident, domiciled or regularly operate (commercial relationship), their nationality or geographical area of origin (also of the funds), the countries in which they have significant connections. In particular, where the Customer has significant relationships/connections with a high-risk geographical area, the Group Companies will consider whether there is a valid economic or legal reason to justify the type of ongoing relationship or operation that is requested, or whether the Customer’s financial requirements could be better met in the country where they have the significant relationship/connections or the country where the Customer is based;
- for legal entities:

- the country in which they have commercial relationship and/or are registered and/or where they have a base and carry on commercial relationships;
- the country of which the Beneficial Owner and executors has nationality,
  - the country in which the Beneficial Owner and executor are resident or domiciled and the countries with whom they have significant relationship/connections, where other economic activities carried out by same.

SECTOR RISK

The sector risk is the risk of carrying on Criminal Activities relating to the sector, type of profession or economic activity in which the Customer, the Beneficial Owner or, where relevant, the Executor, operate. Certain economic sectors have a high level of money laundering risk (on a non-exclusive basis, these are sectors characterised by a high degree of use of cash, such as gold trading, currency exchanges, betting or gaming, casinos or money transfer businesses, or trading in antiques, auction houses and art galleries; the trading of scrap metal) or they may be sectors with a particular exposure to the risk of corruption (sectors of the economy which receive public funds, including EU funds, such as weapons and dual use goods; waste collection and disposal; production of renewable energy); Certain sectors have a greater propensity to corruption (for example construction, telecommunications, etc.), if they depend on works contracts or public licences; other sectors may have a low risk of financial crime, but in countries with a high level of corruption this risk may rise considerably due to the high level of dependence on licences or public works contracts.
Where an entity may be involved in more than one activity or sector, the primary sector, or the one in which it conducts most of its business, will prevail.
The sectors classified and assessed by the Parent Company as being high risk are indicated in the GOR- Customer Due Diligence Requirements for AML.

PRODUCT AND SERVICE RISK

Some products and services are inherently more vulnerable to financial crime, possibly because the nature of the product allows the rapid transmission of funds between different parties. Other risks associated to products, services or operations depend on the level of transparency or opacity of the product (i.e.products or services allowing the client to stay anonymous or promoting the concealment of the identity (i.e.bearer shares, fiduciary deposits etc..), on the complexity of the same (i.e..a transaction/operation involving several parties or countries).

The GOR- Customer Due Diligence Requirements for AML provides a list of the products and services classified as high risk.

ENTITY RISK

Some entities present a higher risk of financial crime due to the lack of transparency about their ownership, or due to corporate or trust structures, which can be classified as vehicles for financial interposition.
The Global Operational Regulation - Customer Due Diligence Requirements for AML. identifies the types of Customer, entity or legal person considered to be at high risk by the Group Companies.

RISK OF POLITICALLY EXPOSED PERSONS AND PUBLIC OFFICE

Politically exposed persons (PEP) are considered to be at a higher risk of money laundering as they are more exposed to potential risks of corruption. The qualification as PEP is significant for a Customer of the Bank, for the Beneficial Owner or for the Executor.
When the Customer, the Beneficial Owner or the Executor are classified as a PEP, the Group Companies will ensure that the commencement or continuation of the ongoing relationship, or the execution of the occasional transaction, is authorised by a Top Manager who will assess the PEP's exposure to the risk of money laundering and the level of controls in place to mitigate this risk.

In line with the reference local regulations, the Parent Company will identify as a PEP any individual who occupies a public office or who resigned less than one year ago from public office as indicated on the article 1, paragraph dd) of the AML Decree, as well as their family members or anyone who is known to have close links with them. For the Group Entities, local regulatory references are applicable.

More information is provided in the GOR Requirements for Customer Due Diligence for AML.

DISTRIBUTION CHANNEL RISK

The distribution channel risk refers to the manners in which the Client obtains the products or services requested (remotely, in person, through a Financial Advisor or (PFA"). A special attention must be placed upon the remote operations in consideration to the absence of the direct contact with the client or the executor.

REPUTATIONAL RISK

Customers and/or Beneficial Owners and Executors may represent a higher risk if they are the subject of negative information that could damage the reputation of the Group in the event that a Customer relationship were to be started with them. It is not possible to list every type of negative information that could be a reputational risk, and it is necessary to exercise good judgement. Particularly important are charges or convictions for Criminal Activities, specifically, the existence of criminal proceedings if the information is known to the Group Companies and is not covered by secrecy obligations that would prevent its use, proceedings for crime against the Treasury, proceedings for administrative liability, fines inflicted for the violation of anti-money laundering laws, against the Customer or the Beneficial Owner.

A reputational risk exists when the Customer, the Beneficial Owner or Executor are the subject of significant negative information. The degree of reputational risk must be assessed on the basis of a combination of our exposure to the risk (including the volume of business we will have with the Customer, the level of confidentiality of the operation, etc.) and the probable reaction of our customers, the regulators and the other stakeholders (including potential media coverage).
To ensure that the Group's reputation is not damaged, any negative information must be assessed to determine the potential laundering of money or reputational risk inherent in the decision to establish or continue a relationship. Even if the negative information can have various levels of gravity, each new case must be assessed to determine first of all whether a Customer relationship is legally admissible, and if the case needs to be brought to the attention of a higher level of approval. If it is determined that the relationship is legally admissible, the negative information must be assessed as indicated in the GOR - Customer Due Diligence Requirements for AML.

Further information about the relevance or irrelevance of information about a new or existing Customer is provided in the GOR - Customer Due Diligence Requirements for AML.

If during the assessment doubts arise about the importance of negative information, that information must be reported to the local Head of AML Function who may request further investigation in order to propose to Top Management the opening/maintenance of the account or its refusal/termination, following the assessment. Where authorisation is given to open or maintain the account, the local Head of AML Function and/or the Top Manager may impose additional Customer Due Diligence criteria (such as increased monitoring of transactions), as they consider necessary.

8. Customer Due Diligence

Knowing the identity of Customers, of the Beneficial Owner and of the Executor is essential to prevent Group Companies from being used by money launderers and anyone who intends to finance terrorism. Therefore, Group Companies will not enter into business relations with a Customer before they have reasonable assurance about their identity, the identity of the Beneficial Owner and of the Executor. The Group Companies do not undertake anonymous relations nor do they establish relations where it is not possible to identify the Beneficial Owner.

The Customer due diligence programme implemented by the Group Companies is aimed at:

- obtaining the identity of the Customer, the Beneficial Owner and the Executor;
- verifying the identity of the Customer, of any Executor and of any Beneficial Owner based on the documents, data or information obtained from a reliable independent source;
- obtaining and evaluating information based on the purpose and nature of the ongoing relationship and, where there is a high risk of money laundering and terrorism financing, also of the occasional transaction; identifying the type of Customer entity (for example, a regulated entity, listed company, private company, public entity, sovereign fund, trust/foundation, SPV or fund etc.)
- obtaining and evaluating information about the relations between the Customer and the Executor and between the Customer and the Beneficial Owner;
- establishing which products and services have been requested by the customer;
- regularly checking on the relations with the Customer throughout the duration of the relationship.

Further information to be obtained according to the risk-based approach may, for example, relate to:

- the origin of the funds used in the relationship;
- business relations and relations with other recipients;
- the financial situation.

The customers provide, under their own responsibility, all the necessary and updated information in order to allow the Group Companies to fulfil the customer due diligence obligations.
A consideration of these factors will determine whether the Customer in question meets the requirements for the Group Companies to establish a relationship with it.
KYC measures must be applied in the following circumstances:

- when an ongoing relationship is established;
- when an occasional transaction is executed, or where such a transaction arises and involves the transmission or movement of means of payment for amounts equal to or higher than € 15,000 regardless of whether it is a single transaction or multiple split transactions, or where it involves the transfer of funds of more than € 1,000;
- where there is the suspicion that an operation is linked to money laundering or the financing of terrorism regardless of any derogation, exception or minimum threshold that may apply;
- when there are doubts as to the accuracy or adequacy of the identification data previously obtained for identification purposes (for example where the correspondence did not reach the address given, or where there are inconsistencies between the documents submitted by the Customer or otherwise obtained by the operator)

If any suspicious elements do arise, during a due diligence process for an existing or new Customer, which determine a suspicious report, the person must not be informed of any of these elements in any way, as doing so could lead to prosecution under criminal law.

When the Group Companies are unable to meet the customer due diligence obligations, they will not establish an ongoing relationship or they will not carry out the operation requested by the Customer. If it becomes impossible for an existing ongoing relationship to continue, the Group Companies will start a unilateral procedure to terminate the account for high-risk parties, or they will place a block on operations on ongoing relations for low and medium risk parties.

The Group Companies will also consider whether or not to report a suspicious transaction to the relevant local authority (the FIU for the Parent Company).

8.1. Types of due diligence and allocation and management of Customer's risk profile

Based on the information obtained during the due diligence (for example by completing the AML questionnaire), taking into account the data already known about the Customer (for example news of crimes, pending criminal proceedings, etc.), the Beneficial Owner and the Executor, the Group Companies will allocate a risk profile to the Customer using automated IT procedures, at the time of onboarding (before the ongoing account is opened), if these procedures are available, in proportion to the type and size of the

Customer's business. The automated IT procedure, where existing, also assures that the Customer's risk profile remains updated, based on the operations they carry out, and any updates to the subjective profile.

8.1.1. Simplified due diligence – Low Risk

SDD – Simplified Due Diligence can apply (where permitted by the relevant local laws) where the risks of money laundering/terrorism financing associated with a Customer are low and the Customer is classified as low risk.
The risk of money laundering and terrorism financing, for certain entities, is low thanks to the level of market regulation or supervision or public attention, in a jurisdiction which is considered to have adequate laws and regulations in this area. The assessment of Customer risk is low in cases where it is possible to identify one of the "Factors of low risk" provided for in AML regulations, included in Annex 3 of the GOR - Customer Due Diligence Requirements for AML.

The simplified due diligence measures that apply to customers with a low risk of money laundering consist of reducing the scope or frequency of the requirements provided for by AML regulations, having regard to:

- the time required to complete the activities to identify the Customer, Executor or Beneficial Owner.
- a reduction in the frequency of the updating of the due diligence data.

The Parent Company does not reduce the information required in cases of low risk Customers or in simplified due diligence.

8.1.2. Enhanced due diligence – High Risk

Group Companies are required to apply EDD - Enhanced Due Diligence when the risks of money laundering/terrorism financing are high, in order to manage and mitigate the risks appropriately.

Enhanced due diligence measures consist of obtaining more information about the Customer, the Beneficial Owner and, where relevant, the Executor; a more accurate description of the nature and purpose of the relationship; intensifying the frequency of checks, and greater depth of analysis in terms of the ongoing checks on the relationship.

The measures taken by the Group Companies depending on the type of high risk Customer will consist of:

a) obtaining more information about:
   i. the identity of the Customer, the Beneficial Owner or ownership and control structure of the Customer. This will also include obtaining and evaluating information about the reputation of the Customer, the Beneficial Owner and the Executor;
   ii. the ongoing relationship, to fully understand its nature and scope. This will include obtaining information about:
   - the number, scope and frequency of the expected transactions in order to identify any discrepancies that may lead to suspicions;
   - the reasons why the Customer is requesting a certain product or service, especially if their financial requirements could be better satisfied in another way or another country;
   - the destination of the funds;
   - the nature of the activity performed by the Customer, the Beneficial Owner and the Executor;

b) obtaining a better quality of information. This will include checking the origin of assets and funds of the Customer, used in the ongoing accounts.

c) requesting information updates from the Client more frequently, completing more frequent checks on the ongoing relationship with the Customer, in order to duly identify any changes in the information on file which could impact the outcome of the assessment of the relationship in terms of maintenance or termination of the relationship, and which may lead to the decision to send a a SAR/STR to the competent local FIU (the "UIF" for the Parent Company);

d) requesting authorisation from the Top Manager to start or continue the ongoing relationship.

The Group Companies apply enhanced due diligence obligations taking into account specific regulatory requirements (including the high factors identified by the Bank of Italy and included in Annex 4 of the GOR - Customer Due Diligence Requirements for AML), or where there are reinforced controls that are necessary following independent assessments of the Customer's AML risk. All high-risk customers must be assessed in order to determine whether a more customised monitoring of their activities is necessary, in which case the nature and frequency of such monitoring will also be determined. The type and scope of monitoring will depend on the specific risk factors identified and, in any case, it may not be less frequent than 12 months.

In summary EDD applies to all high-risk Customers, as in the following cases:
:

- the Customer or the Beneficial Owner is a PEP;
- the Customer is a joint account holder with a PEP or is an authorised signatory on the account of a PEP or has provided a power of attorney to a PEP
- the Beneficial Ownership of a Customer is in the form of bearer shares
- the Customer is an AML Private Customer i.e a client with high net worth, to whom highly personalised and complex services are provided";
- the Customer, the Beneficial Owner and the Executor, where relevant, are based in countries identified as high-risk
- the Customer carries out operations for unusually high amounts or when there are doubts as to the purpose for which they are ordered.
- the Customer, the Beneficial Owner and the Executor, where relevant, have been reported to the local authorities for suspected money laundering (in which case the risk profile will remain unchanged for the five years after the report is made, with a proposal for downgrading made to Top Management if, during the five years thereafter, no new risk factors have arisen and no requests for further investigation by the local authorities (the "UIF" for the Parent Company or investigating authorities) have been received;
- the Customer is classified as "high risk client" based on the characteristics of the relationship and the transactions being in place, client information on file, and the number of active accounts and services received individually or jointly)
- the Customer and the Beneficial Owner or Executor, where relevant, are involved in criminal prosecutions or are involved in press reports concerning criminal convictions against them (in which case their risk profile will remain unchanged for the five years following the court order or negative press report; after that period, if during the five years following these events there are no new risk factors and if there are no requests for further investigation by the FIU or the investigating authorities, a proposal for downgrading may be made to Top Management).

In all cases listed above, the owner of the assessment of a high-risk client may determine the appropriate manners to obtain more information and documentation, to carry out more frequent checks and to carry out a more in-depth monitoring of transactions. This involves:

- verifying the identity of the Customer and the Beneficial Owner or the ownership and control of the Customer based on more than one reliable independent source, using the data sources referred to in Annex 2 of the GOR - Customer Due Diligence Requirements for AML;
- verifying the origin of the assets of the Customer and the origin of the funds used in the relationship;
- Identifying and verifying the identity of the other shareholders who are not Beneficial Owners of the Customer. In the case of high risk customers, the names of anyone who owns or controls 10% or more of the shares or voting rights, must also be obtained;
- the reasons why the Customer is requesting a certain product or service, especially if their financial requirements could be better satisfied in another way or another country;
- the destination of the funds;
- more frequent updates of information received.

For the Parent Company, the preparation of the risk profile is based on algorithms and IT procedures (Gianos KYC and GPR) which are suitably configured to assure that the correct risk profile is given to the Customer based on the information obtained and as updated from time to time.
The Parent Company may raise the Customer's risk profile that has been automatically set by the application, if this is considered necessary. Any lowering of the Customer's risk profile must be limited to exceptional cases, justified in detail in writing, and authorised by Top Management.

The Subsidiaries will adopt automated or manual procedures to process the Customer's risk profile, depending on the size and type of business.

8.1.3. Standard due diligence – Medium Risk

Standard Due Diligence generally applies to customers with medium risk, when there are no indications to carry out SDD or EDD.

8.1.4. Due diligence – ongoing monitoring

The information obtained during the due diligence process (for the Parent Company in the form of an AML questionnaire completed by the Customer, the Beneficial Owner and the Executor) must be updated periodically, at least:

- once a year for "high" risk Customers;
- every three years for "medium" risk Customers;
- every five years for "low" risk Customers.

Where the documents obtained for due diligence (for the Parent Company this is the AML questionnaire, the additional PEP questionnaire for politically exposed persons, the supplementary questionnaire for links with high risks countries or the ID card) have expired, the Group Companies will automatically block the Customer's operations. For high risk Customers, after authorisation by the body with delegated powers for the Parent Company or the body with equivalent functions in the Subsidiaries, the accounts will also be terminated and they will consider whether or not to send a SAR/STR to the local authority (the UIF for the Parent Company).

The following events will always result in a review of the Customer due diligence,

- the scheduled review based on the high risk rating has fallen due;
- there is a need to examine unusual operations (for the Parent Company this is taken from the system used to monitor Unexpected transactions, FBI Fineco, event driven cases, request for investigation by the FIU);
- there is a doubt that the information the Bank has on file has changed in terms of corporate structure, residence of the customer, or a change in the type of the Customer's economic activity;
- substantial negative information has been obtained;
- it is requested by the AML Function.

The review of the Customer's KYC information must include:

- verification that the account with the Customer is still active;
- confirmation that the Customer's risk rating is accurate. If the risk rating has changed, the KYC must be reviewed in accordance with the type of Customer (natural person or entity);
- verification that the KYC documentation has been archived and is suitably updated, in accordance with the type of Customer;
- check that any Connected Parties are the same, and identify any new parties. If they have changed, due diligence must be carried out in accordance with the type of Customer entity (if necessary);
- for all names, adequate name checks must be carried out, as described in this Policy and the relative GOR.

The periodic KYC review does not necessarily mean that the Customer's **whole** documentation has to be redone, if it is still valid as it was at the time of onboarding (for example the ID card may be valid but the AML questionnaire has expired).

If a Customer who has an ongoing relationship requires the opening of an additional account[2], he will be asked to update the data they previously gave (for example the AML questionnaire for the Parent Company) during the due diligence, or to confirm the validity of the information.
When the periodic review falls due, the KYC information that was previously obtained may not be used.

[2] a long-term relationship which forms part of the activities of a bank performed by the obligated parties, which is not completed in a single transaction;

In relation to the opening of new accounts, it should be clarified that:

- for all relations classified as “ongoing” the Parent Company requires that when the account opening request is made, the Customer updates the AML questionnaire; in the case of a PEP the supplementary PEP questionnaire must also be updated or obtained
- In the case of:

    - PEP customers and legal entities considered to be high risk: when the request to open an ongoing account is made, the enhanced due diligence must be carried out, and the authorisation to open the account must be obtained from a Top Manager of the Parent Company (equivalent authorities in case of subsidiaries)
    - natural persons who have a HIGH risk profile (not PEP): a distinction must be made depending on the type of ongoing account:

        - for relations involving the provision of credit (credit card, mortgage or personal loan, bank guaranty), enhanced due diligence must be carried out, and authorisation to open the account must be obtained from a Top Manager;
        - for relations that do not involve the provision of credit, or which do not present additional risks or require additional AML assessments other than those already done when the account was opened (Advice Plus accounts, Credit Lombard), the enhanced due diligence and authorisation to open the account from a Top Manager is not necessary.

8.2. Customer identification and verification

The identification and verification of the Customer’s identity (and that of the Beneficial Owner and Executor) must take place before the account is opened or before the occasional transaction is executed. If there is more than one person to be identified (in the case of joint account holders or multiple Executors), the ID cards may be obtained at different times, provided that they are obtained before the joint account becomes effective or before powers of delegation of representation are given.
For customers with low money-laundering risk, who are subject to simplified due diligence, the Bank may delay the acquisition of a copy of the ID card needed to complete the due diligence process for up to 30 days.

The identification consists of obtaining the ID provided by the Customer, upon production of an ID card or equivalent legally accepted recognition document, for which a hard copy or digital copy will be obtained. The joint account holders and Executor will be identified in the same way. For the Executor, information about the existence and extent of their powers of representation will also be obtained.

If the Customer is not a natural person and therefore is operating through natural persons with the power of representation, identification will be required for:

- the Customer, by obtaining the identification details and information about the type, legal form, purposes and activities of the business, and, if applicable, details from the companies' register entry and registers kept by the relevant regulatory authorities. For non-profit organisations, information will also be obtained about the category of target beneficiary (for example victims of natural disasters or wars). In the case of trusts, the recipients will obtain a copy of the last version of the deed of formation, in order to collect and continuously monitor the information about the actual purposes of the trust, the identity of its beneficiaries and the trustee, the mode of execution of the trust and any other characteristics;
- the Executor, who is identified in the same way as for a natural person[3], and for whom information about the power of representation will also be obtained.

Depending on the distribution model (online or distance selling through a network of financial advisers licensed for distance selling) adopted by the Parent Company, specific identification procedures have been defined, in particular:

- for sales in Italy:
    - distance

[3] It must be noted that the identification of the executors of natural person and corporate clients always occur in person.

    - *facial* through the financial advisers' network
- for sales in the UK (free provision of services):
    - distance

Annex 2 of the GOR - Customer Due Diligence Requirements for AML contains a list of documents and reliable sources to identify and verify the identity of a Customer, a Beneficial Owner and an Executor.

8.3. Identifying and verifying the Beneficial Owner

The Parent Company will obtain information about the Beneficial Owners based on the declaration made by the Customer, and will also obtain a copy of a currently valid ID card and/or verifying the identification data obtained from the client based on independent, influential sources.

Clarity of information about the effective ownership is a key element of the AML Programme. Without this information, it is not possible to adequately manage issues concerning sanctions, politically exposed persons and reputational risk, nor is it possible to accurately profile the Customer in terms of AML risk nor to properly configure the transaction monitoring systems. It is thus essential, before establishing a relationship with the Customer and opening the account, that the Beneficial Owners are identified and that this information is accurately researched and recorded.

If the Customer is a company with **share capital:**
a) direct ownership means the ownership of more than 25 per cent of the Customer's capital, held by a natural person;
b) indirect ownership means the ownership of more than 25 per cent of the Customer's capital, held through subsidiary companies, fiduciary companies or through an intermediary.

in cases where the ownership structure does not allow for the identification of the natural person or persons who have direct or indirect ownership of the company, the Beneficial Owner will be the natural person(s) to whom the control of that entity can ultimately be attributed, by virtue of:
a) the control of the majority of votes that may be exercised at the ordinary shareholders' meeting;
b) the control of votes sufficient to exercise a dominant influence at the ordinary shareholders' meeting;
c) the existence of particular contractual constraints that allow for a dominant influence to be exercised.

For high risk customers, in addition to the identification of the Beneficial Owner, it is necessary to identify (not verify) the names of shareholders who hold or control 10% or more of the Customer company.

For Entities such as **foundations** and **Trusts,** Beneficial Owner means:

- the settlor;
- the trustee;
- the protector (if existing);
- the beneficiaries or, where the natural persons benefiting from the legal agreement or entity still have to be identified, the category of people in whose interests the legal arrangement or entity was formed or operates;
- any other individual exercising effective control over the trust through direct or indirect possession or any other means.

If the Customer is a private legal person[4], the following persons will all be identified as Beneficial Owners:
a) the founding members, when alive;
b) the beneficiaries, when identified or readily identifiable;
c) the holders of the powers of legal representation, management and administration.

Ultimately, if the adoption of the above criteria does not allow one or more Beneficial Owners to be unequivocally identified, the Beneficial Owner will be the natural person or persons who have the powers of legal representation, administration or direction of the Customer/ company.

The Designated Parties subject to the AML requirements will keep track of any checks made to identify the Beneficial Owner.

[4]as referred to in the **Decree of the President of the Republic no. 361 of 10 February 2000 (local Italian law)**

Clarifications about the procedures applied to identify the Beneficial Owner are contained in the GOR - Customer Due Diligence Requirements for AML.

8.4. Identification and verification for distance transactions

The Group Companies pay particular attention to remote identification considering the absence of direct contact with the Customer. As far as the remote identification is concerned, the Group Companies:

- Obtain the Customer's identification details and will carry out a check on a copy – obtained electronically or in a similar way – of a valid ID document in accordance with the current laws;
- Require additional enhanced checks (for example, for the Parent Company: a webcam, a bank transfer made by the Customer through a banking and financial intermediary based in Italy or in an EU country, validation based on reliable new technologies based upon robust security safeguard (for example biometric recognition such as *videoselfies*[5]), supported by robust security checks, etc.)

These remote identification mechanisms are based on technologies supplied by external, recognised operators (Experian Prove-ID for the UK market and Infocert for the Italian market). They are subject to a pre-assessment by the local AML Function, in accordance with the EBA requirements (Opinions on the use of Innovative Solutions by Credit and Financial Institutions in the Customer Due Diligence Process). For the Parent Company, the outcome of these assessments is recorded in data sheets which are periodically updated by the AML Function.

8.5. Purpose/nature of economic activity and source of assets

The Group Companies will assess information about the purpose and nature of the account. The depth and scope of these checks is related to the risk profile. The Group Companies will in any case obtain and assess information about:

- the aims relative to establishing the relationship;
- the relations between the Customer and the Executor;
- the relations between the Customer and the Beneficial Owner of the account;
- the working and economic activities they carry out, and, in general, the business relations with the Customer.

Further information to be obtained according to the risk-based approach may, for example, relate to:

- the origin of the funds used in the relationship;
- business relations and relations with other recipients;
- the economic situation (for example sources of income) and assets (including for example the following : financial statements, VAT and tax returns, documents or declarations from the employer, financial intermediaries or other parties);
- the employment, financial and asset situation of the Beneficial Owner and, where this is known or can be easily obtained, the situation of family members and cohabiting partners.

8.6. Power of Representation

Apart from relations with regulated Entities, the Group Companies must obtain evidence that the representative of the Customer with whom the Group Company is communicating has sufficient authority to bind the Customer in the relationship in question, and their identity must be verified. This authority may be implicit in the case of single Administrator or equivalent representative.

8.7. Name Checks

Name checks are carried out when an account is opened and on an ongoing basis. The checks must be done on the names of the identified parties, in order to be able to identify any issues that may arise in terms of assessing the Customer risk and to identify any Entities that may be subjected to sanctions.

8.8. Approval of relationship

A new customer relationship can be established if (1) all the information about the Customer, the Beneficial Owner and the Executor have been correctly obtained, (2) no impediments to the opening of the account have arisen.

According to the four-eyes principle, high risk customers not only have to be evaluated by the AML Function but they must also obtain authorisation from a local Top Manager. The declassification of PEP customers, after a year from the end of the PEP role does not require a specific authorisation from the Top Manager of the Group Company, unless there is a high risk of money laundering and then the Group Companies may determine that it is still appropriate to apply EDD, in which cases the decision to keep the relationship with the customer as such will be subject to the approval from the Top Management of the Group Company..

8.9. Prohibited business relations

The Group Companies do not enter into business relations with Shell Banks, nor will they carry out or allow transactions into anonymous accounts.
The Group Companies must also take adequate steps to ensure that they do not open or maintain correspondent banking relations with banks that allow relations with Shell Banks.
The Group Companies will not establish or maintain business relations with legal persons when the identity of the Beneficial Owner(s) needs to be ascertained on the basis of this Policy but where it cannot, in fact, be established.
The Group Companies will not enter into or maintain relations nor will they process transactions linked to natural persons or legal entities who are included on the List of Financial Sanctions of the European Union or on the Specially Designated Nationals and Blocked Persons List ('SDN list') of the Office of Foreign Assets Control (OFAC), on the UK and UN Sanction lists.

In addition, Group Companies do not enter into relations with:

- currency exchange and currency transfer services (non-banking entities and entities not listed on registers kept by the regulatory authority, which offer their customers money transfer or exchange systems, the cashing of cheques, or the issue/cashing of travellers cheques);
- digital/virtual providers and money exchange platforms and providers of virtual portfolios except the case of designated persons subject to the AML requirements and registered in specific registers issued and maintained by the regulatory authorities of the countries where they operate;.
- natural or legal persons who are known to be actively involved in criminal activity, corruption or terrorism
- persons operating in a red light business/narcotic drugs/weapons sectors.

8.10. Checks during business relations

The Group Companies require ongoing checks to be made with regard to Customer operations. Apart from identifying potential unusual aspects in individual transactions by the departments responsible for collecting and executing the operations (PFA and Parent Company internal departments), customer transactions must be periodically analysed to check that they are compatible with the knowledge that the Bank has of its Customer, their commercial activities and their risk profile.
In the first case, if the unusual aspects of the transaction or of the customer behaviour have been identified and may indicate that money laundering activities are taking place, the department that identified the issue must make a SAR/STR.

8.11. Sharing of Customer information within the Group

Although most of the legal systems of non-EU countries do not prevent the groups from implementing AML/CFT policies and Group procedures which are stricter than the national legislations, there may be cases in which the implementation of the law of a third country does not allow the application of some or all of the

regulations set by the Parent Company, for example because the sharing of specific customer information within the Group conflicts with the local laws on data protection or banking secrecy.
Where a Group owns all or most of an entity that operates in a non-EU country does prevent the sharing of information about customers within the Group, it is necessary to check whether the consent of the customers and, where applicable, the Beneficial Owners of the customers, can be utilised in order to legally overcome prohibitions or restrictions.
Where this is not possible the Subsidiary must take the following additional steps:

- inform the Parent Company, through the NBO process, of the legal requisites that are preventing the sharing of information;
- assist the NBO with a legal opinion that specifically illustrates the prohibition.

If the local laws applicable to the Group Company are stricter than those applicable to the Parent Company, the Subsidiary will follow the stricter rules that apply at local level.

8.12. Escalation

If the local Head of the AML Function, having been informed by the local AML Unit, establishes that an account, operation or payment may infringe the prohibitions provided for in this document, he/she must inform the business unit involved that the activity is prohibited. This decision will be considered final and binding.
If a relationship, transaction or payment, even if permitted by law and by the internal AML restrictions, represents an operational and/or reputational risk that is significant, the decision to open a particular account or execute a payment or transaction falls to the local Top Management.
The decisions taken must be final, and may involve rejecting the operation, approving it under certain conditions or setting specific restrictions.
If the decision of the local Top Management is different from the proposal made by the local AML Unit, the head of the local AML Function may escalate the case to the local Top Manager of the higher grade.
The escalation must:

- take place in writing;
- contain the reasons as to why it was made; and
- be accompanied by full supporting documentation.

.

9. Record keeping (documentation, information and operations) and making data and information available to authorities

The Group Companies will implement and maintain procedures to ensure that the following documents are kept for the period of time determined by the applicable laws (10 years from the execution of an occasional transaction or from the termination of a continuous business relations in the case of the Parent Company).

- a copy of or references to the documents used for the customer due diligence; and
- documents and records to support the account and the operations, consisting of the originals and/or copies used for legal proceedings in accordance with current national laws.

The documents must allow at least the reconstruction of the following details:

a) with respect to continuous relationships, the place where the relationship was established the date on which the account was opened or the mandate was given and closed;
b) with respect to occasional transactions subject to CDD and to the transaction on accounts: the date of the transaction, the amount and sign of the transaction, the rational of the transaction and the mean of payment used;
c) with respect to occasional transactions not subject to CDD, the recipients of these provisions keep additional records to what listed above on point b) data and information needed to univocally identify the client and the executor and where known, the sector of the economic activity and the data and the appropriate information required to univocally identify the beneficial owner.
d) identification data, including, where available, data obtained through electronic identification tools and the relevant fiduciary services as per the EU Regulation Nr 910/2014 or through secured electronic identification procedures authorised or recognised by the AGID the Customer, the Beneficial Owner and the Executor, and information about the purpose and nature of the account or service;
e) the access, where executed, to the BO registers

To guarantee that the documents and information can be used by the competent national authorities in any investigation, or when investigating cases of possible money laundering or terrorism financing, the procedures of the Company, where requested by the relevant local laws, must ensure that the information is archived in the respective computerised accounting procedures and that the documents are kept in digitised record keeping systems ensuring:

a) complete and prompt access to documents, data and information by competent authorities,
b) prompt acquisition by the recipients of these requirements, of documents, data and information with the relevant date;
c) integrity of the documents, data and information with no possibility to change them after being acquired
d) adoption of appropriate measures aiming at preventing any loss of the documents, data and information
e) transparency, completeness and clarity of the documents, data and information together with maintaining the historical accuracy of the same.

The Group Companies comply with the obligations listed above with respect to continuous business[6] relationships and transactions undertaken within the institutional activity of the Entity[7], unless such activities or operations are included in the list of exemptions described below in the par. 8.13.2 (applicable to the Parent only).

The acquisition of documents, data and information in the digitised record keeping systems must be promptly completed and, in any cases, not after 30 days from the establishments of the continuous business relationship, execution of the transaction, amendment and closure of the same.

[6] For FinecoBank: current acounts, security accounts, mortgages, personal loans, credit cards,banking guaranty.
[7] The activity for which the Bank has been registered and authorised by the competent authirity.

9.1. Making data available: the new single digitised archive (for Parent only)

In order to make available to Bank of Italy and UIF data and information in line with the standards defined in the Dispositions for the Record keeping and making documents, data and information to contrast money laundering and terrorism financing (Provision of Bank of Italy of 24 march 2020), the Bank avails of standardised archives compliant with the standards defined in the Attachment Nr 2 of the Bank of Italy Provisions. This choice allows the Bank to continue to use the Single Digitised Archive (AUI), the feeding procedures and checks in place, updated, where necessary, to ensure compliance with the regulatory requirements set out in the Bank of Italy Provisions.

9.2. Exemptions (for Parent only)

In line with the regulatory provisions mentioned above, the Bank avails of the options to dis-apply rules related to the making data and operations available to the authorities, where the latter are related to continuous business relationships or occasional transactions put in place with:

1. banking and financial intermediaries located in Italy or in another EU Member State;
2. electronic money institutions[8];
3. payment institutions[9];
4. financial intermediaries[10];
5. asset management companies[11];
6. investment companies with variable share capital[12];
7. investment companies with fixed share capital[13];
8. other intermediaries listed in the register defined under art. 106 TUB;
9. "Cassa Depositi e Prestiti";
10. Insurance companies operating in activities set out under art. 2,1,CAP;
11. Entities providing micro lending;[14]
12. "confidi" and other entities listed in art. 112 of TUB;
13. Money market collective investment undertakings and othe collective investment undertakings established in EU countries;
14. EU banking authorities and central banks, including Bank of Italy;
15. Other financing and monetary authorities in EU.

9.3. Reporting "Comunicazioni Oggettive" (Parent Only)

The AML Function is in charge of sending the "Comunicazioni Oggettive" report to the local FIU, according to the provisions issued by the same in compliance with the regulations applicable to the Parent.

9.4. Reporting suspicious transactions

A suspicious operation is defined as any activity which, by its nature, is designed to have a link to money laundering or the terrorism financing, specifically: complex operations of a particularly large or unusually high amount, and any unusual transaction model which does not have a clear economic purpose or a clearly legitimate aim.

[8] as defined in the art.1,2, letter h-bis TUB (IMEL).
[9] as defined in the art.1,2, letter h-sexies TUB (IP).
[10] as defined in the art.1,1, letter e, TUF (SIM).
[11] as defined in the art.1,1, letter o, TUF (SGR).
[12] as defined in the art.1,1, letter i, TUF (SICAV).
[13] as defined in the art.1,1, letter i-bis, TUF (SICAV).
[14] As per art. 111 TUB.

9.4.1. Identification and reporting of suspicious transactions

The Bank actively works with the competent authorities in order to identify “suspicious transactions”. The suspicion must be deduced from the characteristics, scope and nature of the operation or any other known circumstances, also taking into account the financial capacity and activity performed by the person in question, based on the elements available to the parties required to make the report, which they obtained during their activities.
An element of suspicion would also be the frequent or unjustified use of cash transactions.
In order to ensure that the obligation to actively collaborate with the authorities is achieved, the Group Entities has implemented procedures that provide for:

- timely internal reporting of potentially suspicious activities to the MLRO or his deputy;
- the assessment and investigation of potentially suspicious activities, and the documenting of the results of these investigations;
- timely reporting to the authorities in the presence of, with suspicion of or where there are reasonable grounds to believe there may be actual or attempted money laundering activities; and
- timely replies to requests for information from the Authorities.

In particular, these procedures, the aim of which is to specifically define the process for reporting suspicious transactions and the related obligations:

a) provide for detailed organisational guidelines that regulate the process of reporting suspicious transactions, and guarantee their traceability from the time when the suspicion arises until the decision is made as to whether or not to make a report;
b) contain specific instructions as to how to assure timeliness and secrecy in the reporting process, both within the Group Entities and externally, minimising any intermediate steps between the reporting person or business unit and the person or business unit that is responsible for assessing the report;
c) provide for adequate measures designed to stop the operations from being executed where this is possible considering the actual operation in question, and provided that non-execution of the operation would not impede the investigations of the Authorities;
d) provide for an obligation to set up an archive in which the internal reporting forms are kept, complete with observations made by the people involved in the procedure and any attached documentation, a copy of the reports, any covering letters and any other communications sent to the relevant Authorities together with any further communications or requests received from them;
e) guarantee the confidentiality of the identity of the people who make the report.

Employees are adequately informed about the internal reporting process, through the publication of the operating procedures and also in specific training courses.

The Group Entities use methods and tools which can identify any suspicious behaviours, and will also refer to the anomaly indicators or red flags issued from time to time by the Regulatory Authority operating in the countries where the Group Entities operate

10. Training Obligations

As part of its training programme, the Parent Company provides ongoing mandatory training. For new hires, this takes place within three months from the date of employment. The training is obligatory for personnel and financial advisers, and concerns the prevention of money laundering and the financing of terrorism.

In consideration of the activities it performs, the Group Companies' HR Function, with the assistance of the local AML Function, will identify specific training courses, which may be addressed to different target of employees/advisers.

The first level of training involves the circulation of the Policy and the company regulations adopted in implementation of that Policy to all personnel and advisers of the Parent Company. These documents illustrate all the AML and terrorism financing prevention obligations, together with the related sanctions. It concentrates on the behaviours to be adopted by each employee or adviser, considering their work activities.

The training course includes a test which is intended to assess whether the employees and advisers have actually understood the topics covered.

If an employee or adviser does not complete the required training within a certain period, this must be reported to higher levels and adequate penalties will be imposed, including the impossibility of dealing with customers or handling operations, where necessary.

11. Information Systems

The Group Companies have suitable tools and procedures to:

- allow the proper conservation and processing of information on customer due diligence and on transaction records
- help to identify missing data to complete the information records referred to above, by producing adequate evidence, system warnings or operational blocks
- guarantee the physical and logical safety of the archives (to assist in the evaluation of suspicious transactions, by producing anomaly indicators for the purposes of reporting to the Authorities if necessary;
- where applicable, allow automated cohesion checks between the stored information, congruency checks and periodic data controls
- automatically verify that no business relations or individual transactions are carried out with people who are included on the list of suspected terrorists circulated by national or international Authorities
- allow checks to be made on all customer databases in response to external requests from the legislator, from the law enforcement bodies, or to respond to internal investigations;
- share information (about suspicious activities identified by the Bank) within the Group for AML management purposes, in line with what is permitted by the applicable laws.

12. Parent Company - Limitations on the use of cash and bearer shares

Legislative Decree 231/2007 provides for important limitations on the use of cash and bearer shares:

- the transfer of cash and bearer shares in euro or in foreign currency, undertaken for any reason between different natural persons or legal entities, is prohibited if the value of the transfer is equal to or above € 2,000; this threshold is also exceeded even if the transfer is made in multiple payments lower than the threshold, which appear to have been artificially split;
- a transfer above the limit of € 2,000 may only be made through banks, Poste italiane S.p.a., e-money firms or payment providers in the form of an instruction accepted in writing by those intermediaries, and with delivery of the cash sum to them;
- the cheque books and postal order forms are issued by the banks and by Poste Italiane S.p.A. with a non-transferability clause; the customer may make a written request for the issue of cheque books and postal orders in unrestricted form;
- bank cheques and postal orders for € 1,000 or more must contain details of the name or company name of the beneficiary, and the non-transferability clause;
- bank cheques and postal orders issued on the order of the drawer can only be endorsed for collection at a bank or through Poste Italiane S.p.A;
- cashier's cheques, bills and postal orders must contain details of the name or company name of the beneficiary, and the non-transferability clause.

If these requirements are violated, a fine of between € 3,000 and € 50,000 will be imposed.

- The Customer may make a written request for the issue of cashier's cheques, bills and postal orders of amounts of less than € 1,000, without the non-transferability clause. A revenue stamp of € 1.50 is required from the requester for each postal order or bank cheque requested in unrestricted form, or for each cashier's cheque or postal order or bill issued in unrestricted form.
- Only named deposit books, bank or postal books can be issued;
- The transfer of bearer books (of bank or postal deposits) is prohibited; if existing, they must be closed by the bearer by 31 December 2018; if these requirements are violated, a fine of between € 250 and € 500 will be imposed.
- The opening, in any form, of accounts or savings books anonymously or with a fictitious name, is prohibited; any violation of this prohibition results in a fine of between 20% and 40% of the balance.
- Finally, the use in any form of accounts or savings books, anonymous or with a fictitious name, opened in foreign countries, is prohibited; a fine of between 10% and 40% of the balance will be imposed for any violation.

12.1. Obligation to report violations to the Ministry for the Economy and Finance

The Bank is required to inform the Ministry for the Economy and Finance of any violations of the rules on the limitation of the use of cash and bearer shares which it may receive in relation to its service duties, and within the limits of its powers and activities; this communication must be made within 30 days from the date on which news of the violation was received. The same communication must be made by the members of the Board of Statutory Auditors, the supervisory committee and the management control committee where they find any violation of these provisions in the exercise of their control and supervisory functions. For violations relating to bank cheques, cashiers' cheques, bearer passbooks and similar items, the communication must be made by the bank who accepted the payment (the drawer) and by the bank who made the payment (drawee) except where the person required to make the communication is certain that the report has already been made by the other obligated party. If the violation relates to a transfer that is already the subject of a suspicious transaction report, there is no need to make the above communication.

13. Customer Due Diligence obligations carried out by third parties

Where Group Companies rely on third parties ("Delegated Parties") to carry out CDD it is required that:

a. the Group Company defines in specific agreements the obligations that must be satisfied, the manner in which the duties must be carried out and the timing framework;
b. the Group Company obtains a relevant attestation from the Delegated Party stating that the latter has undertaken CDD in compliance with the regulations applicable to the Group Company;
c. the attestation as per the above, refers unequivocally to the Delegated Party and it is provided to the same who will use it. The attestation will contain clear confirmations regarding the correct undertaking from the Delegated Party of the CDD measures applied, the checks carried out and the match between the client in respect of which the checks have been completed by the Delegated Party and the clients of the Group Company to whom the attestation refers to;
d. the Delegated Party will provide the Group Company with the underlying CDD information and any other information related to the identification of the client upon request;
e. the Delegated Party will forward as soon as practicable after a request from the Group Company, copies of the documents that have been obtained by the Delegated Party.

The Group Companies, responsible of the CDD, determine whether they are satisfied that the evidences collected from the Delegated Parties are adequate and sufficient to the purpose of complying with the applicable AML & CTF regulations and verify, within the limits of and according to the professional diligence, the truthfulness of the documents received. In case of doubts on the identity of the client, executor, beneficial owner, the obliged entities are required to carry out the identification and CDD measures directly on their own.

Group Companies are not permitted to appoint Delegated Parties resident in High Risk – Third Countries for the provision of CDD services.

As at the date of this Group Policy, the Bank does not avail of Delegated Parties to carry out CDD obligations.

14. Measures for preventing the financing of terrorism and the activity of countries that threaten international peace and security - Guidelines

Over the years, the need to combat international financing of terrorism has greatly increased. This has led to the adoption of a series of international measures (UN resolutions) and EU measures (EU regulations implementing these resolutions) designed to combat terrorism on a financial level.
The financing of terrorism is different from *money laundering*, as with *money laundering* the proceeds come from illegal activities and are then put back into the legal circuit through "cleaning" or re-investment, whereas in the case of the financing of terrorist activity, the activities from which the funds are obtained may also be legal, but their subsequent use is illegal (*money dirtying*).
Therefore, as with cases of money-laundering, activities carried out by terrorist groups operating internationally require the use of large amounts of money, which can be transferred through banking and financial channels.
As stated in the Global Policy and Global Rules – Financial Sanctions, the Group Companies must not open accounts with natural or legal persons who are included on the EU, UN, UK or OFAC lists. The Bank must observe this prohibition also in cases where it operates in non-EU countries and in the USA, as failure to observe this prohibition may lead to reputational risks and compromise the Group's business relations.

The Group Companies implement and maintain procedures that provide for:

- restrictions on the assets, economic activities and natural resources of legal and natural persons included on the EU and OFAC blacklists, if provided for or required by law;
- the reporting of these restrictions to the Authorities, or of accounts held with customers who are not subject to restrictive measures, but who are included on the blacklists published by these Authorities;
- the reporting to the Authorities of any known or suspected activity (or the existence of reasonable grounds for knowledge or suspicion) which may be linked to the financing of terrorism; and
- a prohibition on undertaking certain commercial activities, as determined by the EU, with countries that
- threaten international peace and security.

For detailed provisions on the measures used to combat the financing of terrorism imposed at Group level, please see the relevant internal regulations.

14.1 Parent Company – Transfers of funds

The adoption of the measures described in these paragraphs does not exclude the possibility that money launderers or supporters of terrorism can access payment systems to transfer their funds.
The possibility of tracking the origin of the funds transfers with certainty is a particularly important tool in order to:

- prevent abuse of the financial system for the purposes of money laundering or financing of terrorism;
- investigating and identifying cases referred to in the above paragraph.

With Regulation EC No. 1781 of 15 November 2006 the European Union had already laid down rules on information pertaining to the payer which is required for transfers of funds in any currency, by parties operating as Payment Services Providers or Intermediate Payment Services Providers.
Regulation EU No. 847 of 20 May 2015, which came into force on 26 June 2017, repealing and replacing Regulation 1781/2006, extended the scope of these controls to include details pertaining to the beneficiary and to intermediate payments.
Regulation EU 847/2015 applies to transfers of funds in any currency which are sent or received by a Payment Services Provider or by an Intermediate Payment Services Provider established in the EU.
The obligations imposed on Payment Services Providers are:

- to obtain and/or provide information necessary in relation to the payer and the beneficiary;
- to check that the information is accurate, truthful and up-to-date;
- to guarantee the correct transfer of all the information received;
- to monitor any transfers with no information or incomplete information by reporting the matter to the regulatory authorities where there is a suspicion of money laundering or the financing of terrorism.

All the information accompanying the transfer of funds and/or subsequent communications must be archived for at least five years.

14.2 Cases of exclusion

The Regulation does not apply to funds transfers made using a payment card, e-money instrument or mobile phone or other digital or prepaid or post-paid computer device with similar characteristics, provided that the following conditions are met:

a. the card, instrument or device is only used for the payment of goods or services;
b. the number on the card, instrument or device accompanies all the transfers generated by the transaction.

However, the Regulation does apply if the payment card, e-money instrument or mobile phone or other digital or prepaid or post-paid computer device with similar characteristics is used to make transfers of funds from a person to another person.
The Regulation does not apply to transfers of funds:

- that involve the withdrawal of cash by the payer from their own payment account;
- that transfer funds to a public authority for the payment of taxes, fines or other duties in a member state;
- in which the payer and the beneficiary are both Payment Service Providers operating on their own account;
- which are executed with the transmission of images of the cheques, including the cheque stubs;
- the amount of the funds transferred does not exceed € 1,000.

14.3 The obligations imposed on Payment Services Providers

Regulation 847/2015 identifies the roles and responsibilities of the following parties:

- Payment Services Provider on behalf of the payer
- Payment Services Provider on behalf of the beneficiary
- Intermediate Payment Service Providers

14.3.1 The obligations imposed on the Payment Services Provider of the payer (payer's PSP)

The transfers of funds must be accompanied by the following data:

a) the name of the payer;
b) the payer's payment account number;
c) the address of the payer, the number of their personal official document, their customer identification number or the date and place of birth.

The payer's PSP will ensure that the transfers of funds are accompanied by the following data for the beneficiary:

a) the name of the beneficiary;
b) the payer's payment account number.

If the transfers are not made from a payment account or to an account, the payer's PSP will assure that the funds transfers are accompanied by a unique transaction identifier, instead of by the number or numbers of the payment account.
The payer's PSP must ensure that the funds' transfer message has included all the identifying details of the payer. For operations which are ordered through an account debit, the data will automatically be collected by the procedure. For operations ordered by occasional customers (or through cash) it is necessary to verify and indicate the details of the payer if the amount of the transaction is higher than € 1,000.
The accuracy of the payer's details is guaranteed by observing the due diligence obligation, which relates to new customers and also to existing customers, as provided for in the AML regulations (see section 6)

- *Transfers of funds within the European Union*

For transfers of funds ordered in favour of the beneficiary within the EU, it is sufficient for the operation to contain at least the payment account number of the payer and of the beneficiary, or in cases where the operation takes place outside of the current account (debit or credit), the unique transaction identifier.

The full details of the payer are to be provided if requested by the bank of the beneficiary or intermediary, within three working days from receipt of the request.

- *Transfers of funds outside the European Union*

For transfers of funds ordered for a beneficiary outside of the European Union, the operation must contain the full details of the payer (name, address and account number or other equivalent information).
At Fineco, funds transfer procedures have online checks to ensure that the payer's and beneficiary's details are present, as required by Regulation 847/2015, before the funds transfer message is sent.

14.3.2 The obligations imposed on the Payment Services Provider of the beneficiary (beneficiary's PSP)

The beneficiary's PSP must apply effective procedures to ensure – in relation to the details of the payer and the beneficiary – that the fields in the messaging or payment and settlement systems used to make the funds transfer have been completed with the permitted data or characters, in accordance with the conventions used by this system.
They must also apply efficient procedures that, when necessary, include ex-post monitoring or instant monitoring to verify the absence of details of the payer or beneficiary as referred to in the foregoing paragraph 9.2.1.
Where this data is absent or incomplete or if it has not been completed with permitted characters or data in accordance with the payment and settlement messaging system conventions, they must:

- reject the funds transfer
- or ask the payer's PSP to provide the details of the payer or of the beneficiary, before or after having made the funds available to the beneficiary, based on the risk assessment.

14.3.2 Monitoring, assessment and notification obligations

Regulation 847/2015 provides for obligations of monitoring, assessment and reporting for the beneficiary's PSP and intermediary's PSP in order to identify

- payments which are received without any of the required data, or with inaccurate data
- payer's PSP that repeatedly fails to provide information

If a PSP repeatedly fails to provide the required information about the payer or beneficiary, the beneficiary's PSP must take measures, which may include warnings and reminders, before refusing any future transfers of funds from that PSP, or placing limits upon or even terminating their business relations with that PSP.
The beneficiary's PSP must report these failings and the measures adopted to the authority responsible for supervising compliance with provisions to combat money laundering and the financing of terrorism.
The beneficiary's PSP must take into account the absence or incompleteness of the details relating to the payer or the beneficiary to evaluate whether the transfer of funds or any related operations are suspicious and whether they need to be reported to the Financial Information Unit.

14.3.3 Controls and monitoring

On the incoming payments, the Bank monitors operations which are received without the details of the payer and of the beneficiary in order to assess the relationship/position of the payer's PSP if it is repeatedly failing to provide information;

- re-evaluates the position of a beneficiary whose transfers do not contain details of the payer and the beneficiary, if this is a source of suspicion;
- identifies suspicious transactions;
- reports the systematic omissions by the PSP to the relevant authority.

The Compliance Unit - Risk Assessment & Controls Function, using a risk-based approach, will carry out random level II checks

14.3.4 Evaluation and reporting

For operations which are found to be incomplete or for which the details of the payer and/or beneficiary are missing, or where the details do not conform with the messaging system, the Bank will consider whether or not there any indications of suspicious transactions to be reported to the FIU. It must also consider whether or not to limit or suspend operations with correspondence banks who repeatedly fail to provide necessary information.

15. Monitoring of controls

The Group Companies have set up a system of level II controls in order to test the level I AML controls to guarantee they are effective and are being performed correctly.

16. Fines and sanctions

Failing to comply with the obligations under the AML laws and regulations may lead the Group to face reputational risks and risks of fines and sanctions. Accordingly, where a Group Company is liable of serious, repeated, and systematic, multiple violations related to:

- Customer due diligence requirements
- Record keeping requirements
- Reporting of suspicious transactions

or other offenses in the area of the organisation, procedures and internal controls, implementing provisions adopted by the competent authorities, sanctions are applicable as specified in the local law applicable to the Group Company (for example.for the Parent, according to the Italian AML law a fine from 30.000 Eur to 5.000.000 Eur or otherwise equal to 10% of the annual revenues, when that percent amount is above 5.000.000 Eur and the revenue is available and identifiable).
In addition to the above, fines may be applicable to designated persons covering administrative, direction and control functions who have not complied in total or partially with the tasks directly or indirectly assigned to them or their function or if they have facilitated or made possible the above violations or have contributed significantly to expose the Group Company to the money laundering and terrorist financing risk (i.e. for the Parent the fine may go from 10.000 Eur to 5.000.000 Eur).
The sanction framework described above, is for the Parent and the Italian Group Companies only, also complemented by the AML criminal laws (art. 648, 648 bis and ter of the penal code) which include in the money laundering presumption not only fraudulent conduct but also unintentional behaviour and fines.