Document type: *Policy (v.2)*

Financial Sanctions Policy

Responsible Structure: Compliance & AFC

illimity Bank S.p.A

illimity
BANCA OLTRE LA FORMA

Summary

1. OBJECTIVES OF THE DOCUMENT AND AREAS OF APPLICATION

This policy has been prepared to regulate the obligations that the illimity Group (from now on also referred to as the "**Group**") must meet to comply with the obligations set out in the current regulatory framework on financial penalties in all relevant business processes and to ensure compliance with the applicable provisions.

In particular, the Policy defines the general principles to which the conduct of business activities should be subject and contains provisions regarding:

- Roles and responsibilities of the Group's corporate bodies and their functions;
- Safeguards for compliance and management of restrictive measures and embargoes;
- Controls on transactions;
- Assessment of the risks associated with financial sanctions imposed for internationally defined embargoes and restrictions violations.

This Policy and subsequent updates are approved and adopted by resolution of the Board of Directors of illimity Bank S.p.A. (from now on, "**illimity**," "the **Bank**" or "the **Parent Company**") and the individual Group Companies.

The Compliance & AFC structure, which is centralised in the parent company following the organisational model adopted, is responsible for updating the policy in the event of significant changes in the reference sector or the composition and/or activities of the Group.

The Policy and its updates are published on the relevant section of the Parent Company's intranet, accessible to the corporate bodies and employees of the Bank and Group companies.

2. RELEVANT ACTIVITIES OF THE PARENT COMPANY AND GROUP COMPANIES

The Group's business model is based on distinct activities, followed by specific areas of activity within the Bank's various divisions and subsidiaries. The activities relevant to compliance with financial sanctions imposed for violations of internationally defined embargoes and restrictions are listed below:

DIVISIONS/ STRUCTURE PARENT COMPANY	ACTIVITIES RELEVANT TO FINANCIAL SANCTIONS
Growth Credit Division	• Provision of credit to SMEs, structured finance transactions and acquisition financing (acquisition of loans or shares in syndicated loans) - *i.e., Crossover;* • *Factoring* operations; • Purchase of loans and/or new disbursements (refinancing) in the context of debt restructuring - *i.e., turnarounds;* • Purchase of impaired (*distressed) corporate loans - i.e.,* loans classified as *non-performing* loans (NPLs) and probable defaults (UTPs), with and without collateral (limited to UTPs managed to restore performing loans - so-called "going concern" loans).
Specialised Credit Division	• Purchase of impaired (*distressed*) *corporate loans - i.e.,* loans classified as non-performing loans (NPLs) and probable defaults (UTPs), with and without collateral (limited to UTPs managed for liquidation purposes - so-called "going concern" loans).
Digital Structure	• Offer of own and third-party banking services and products through a multi-channel digital platform (*web, app*) *www.illimitybank.com*;
b-ilty Division	• Offering credit products, payment services, and "Over the Counter" ("OTC") derivatives to SMEs and small economic operators (POEs) via our digital platform
Investment Banking Division	• Offering Capital Markets services (strategic advisory to SMEs and structuring of Equity Capital Markets and Debt Capital Markets transactions); • Support in the issuance of so-called Alternative Debt, such as securitisation notes, minibonds, basket bonds, and other hybrid debt instruments; • Transactions in Over the Counter (OTC) derivatives traded on the Bank's own account to hedge the interest rate risk of loans granted by the Bank or third-party banks and exchange rate risk.
GROUP COMPANIES	**ACTIVITIES RELEVANT TO FINANCIAL SANCTIONS**
Arec neprix S.r.l.	• The recovery of non-performing loans acquired by the Bank and on behalf of third parties per Article 115 of the Consolidated Law on Finance (TULPS) and the mandate to sell assets pledged as collateral for loans classified as probable default (UTPs) and non-performing loans (NPLs), in cases where legal proceedings have not been initiated.
illimity SGR S.p.A.	• New financing by Alternative Investment Funds (AIFs) for investment/disinvestment in claims against companies in temporary financial distress but with a reasonable prospect of revitalising and restructuring the debt of such companies (so-called target companies).

3. GLOSSARY

Acronyms	
AML	*Anti-Money Laundering*
CFT	*Countering the Financing of Terrorism*
SOS	Reporting Suspicious Transactions
UIF	Financial Intelligence Unit for Italy
KYC	*Know Your Customer*

Definitions	
Customer	The person who establishes ongoing relationships or carries out transactions, or the person to whom the Bank provides a professional service following the granting of a mandate.
Freezing of Funds	The prohibition under EU and national law on the movement, transfer, alteration, use, or management of funds or access to them to change their volume, amount, location, ownership, possession, nature, destination, or any other change that enables funds to be used, including portfolio management.
Level II Checks	These are controls designed to ensure, among other things: a) the proper implementation of the risk management process; b) compliance with the operational limits assigned to the various functions; c) compliance of the Company's operations with regulations, including self-regulation.
Identifying Data	This means the first name and surname, place and date of birth, registered address and domicile if different from the registered address and, if assigned, the tax code or, in the case of persons other than natural persons, the name, registered office and, if assigned, the tax code.
Anti-Money Laundering Decree	Legislative Decree 231/07 and the subsequent amendments and additions to it.
Dual Use	Refers to products, including software and technology, that can have both civilian and military uses, including products that can be used in the design, development, production, or use of nuclear, chemical, or biological weapons or their means of delivery, including all products that can have both a non-explosive use and any use in the manufacture of nuclear weapons or other nuclear explosive devices.
Embargoes	Measures to interrupt or reduce, in whole or in part, economic and financial relations with one or more third countries.
Executor	The person delegated to act in the name and on behalf of the customer or who has otherwise been vested with powers of representation enabling him to act in the name and on behalf of the customer.
Terrorist Financing	Any activity aimed at the collection, provision, intermediation, deposit, custody, or disbursement of funds or economic resources intended to be used to commission one or more terrorist acts.
Funds	Financial assets and benefits of any nature whatsoever, including income derived therefrom, owned, held or controlled, even partially, directly or indirectly, or through nominees, or by natural or legal persons acting on behalf of or under the direction of nominees, including but not limited to: (1) cash, cheques, money claims, bills of exchange, payment orders and other payment instruments;

	(2) deposits with financial institutions or other entities, account balances, claims and obligations of any kind; 3) publicly and privately traded securities as well as financial instruments as defined in Article 1(2) TUF; 4) interest, dividends, or other income and increases in value generated by the assets; (5) credit, right of set-off, guarantees of any kind, securities and other financial commitments; 6) letters of credit, bills of lading and other securities representing goods; (7) documents showing an interest in funds or financial resources; 8) all other export financing instruments.
Manager	The person responsible for managing the commercial relationship, who is in charge of analysing the client's financial and asset situation and identifying strategic, financial and operational criticalities.
Group	Indicates the Bank and the Entities of the illimity Banking Group.
Means of Payment	Cash, bank and postal cheques, bankers' drafts and other cheques assimilated or assimilated to them, money orders, credit or payment orders, credit cards and other payment cards, transferable insurance policies, pledge policies and any other instrument available that enables the transfer, movement or acquisition, including by telematic means, of funds, values or financial assets.
Non-customers (or other counterparties)	Persons other than customers who participate in transactions involving the Bank's customers.
OFAC (*Office Foreign Assets Control*)	OFAC is an office of the US Department of the Treasury responsible for planning and executing economic and trade sanctions to achieve objectives in support of US national security and foreign policy. OFAC acts under national emergency presidential powers and conducts its activities vis-à-vis foreign states, as well as a variety of risky organisations and individuals, such as terrorist groups, international drug traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction, who are considered a national security threat to US foreign policy and the economy. OFAC has the power to order transaction audits and impose significant sanctions including large fines, asset freezes and a ban on operating in the United States. Many of the sanctions imposed by OFAC are based on decisions of the United Nations and other international bodies.
Operation	Activity consisting in the movement, transfer or transmission of means of payment or in the performance of acts of negotiation with an asset content; the conclusion of an act of negotiation, with an asset content, falling within the scope of professional and commercial activity also constitutes a transaction.
Occasional Operation	Transaction not attributable to an ongoing relationship; an occasional transaction also constitutes an intellectual or commercial service, including those with instantaneous performance, rendered in favour of the customer.
Embargoed countries	This means countries for which there is any economic or trade sanction (other than administrative sanctions of local authorities) or restrictive measure promulgated, enforced, imposed or enforced by the Office of Foreign Assets Control (OFAC) of the United States Department of Treasury, the United States Department of State, the United Nations Security Council and/or the European Union and/or any authority of the Republic of Italy including the Internal Revenue Service, or any other competent sanctions authority.
Third countries	Non-European Economic Area countries other than high-risk third countries.
High-risk third countries	These are the non-EU countries whose systems have strategic deficiencies in their national AML/CFT prevention regimes, as identified by the European Commission in the exercise of its powers under Articles 9 and 64 of Directive

	(EU) 2015/849 (as amended by Directive (EU) 2018/843, of the European Parliament and of the Council, of 30 May 2018).
Adequate verification questionnaire	Forms used to fulfil customer due diligence obligations as required by the Anti-Money Laundering Decree.
Continuous Relationship	Relationship of duration, falling within the exercise of the institution's activity carried out by the obliged parties, which is not exhausted in a single transaction.
First Level Manager	The Head of the Digital Branch (for customers of illimitybank.com and b-ilty, but for the latter, limited to customers holding only a current account[1]) and the Heads of the Parent Bank's Business Divisions (*i.e.* Growth Credit, Specialised Credit, Investment Banking and b-ilty limited to entrusted customers) who are responsible for the administration and management of relations with the relevant customers.
Economic Resources	Assets of any kind, whether tangible or intangible, and movable or immovable property, including any accessories, appurtenances and fruits thereof, which are not funds but which may be used to obtain funds, goods or services, owned, held or controlled, even partially, directly or indirectly, or through intermediaries, by designated persons, or by natural or legal persons acting on behalf of or at the direction of such persons.
Sanction List/Lists of Sanctioned Persons/ Lists of Designated Persons	Lists of names of sanctioned persons disseminated by the UN Security Council, the European Union and OFAC, as well as lists of names of persons subject to restrictive measures provided by the *infoprovider* World-Check, such as the lists: EMBARGO VESSEL, CRIME - TERROR; NONCONVICTION TERROR and CRIME - WAR.
Sanctions Compliance Officer	The Sanction Compliance Officer ensures and monitors the effective implementation of internal procedures to prevent risks arising from non-compliance with international sanctions.
Financial Penalties	Financial sanctions are restrictive measures used to counter the activities of states, individuals or organisations that threaten international peace and security and consist of freezing funds and economic resources held by persons or organisations in a foreign country and thus prohibiting them from disposing of them.
International Sanctions	International sanctions include (but are not limited to) embargoes and asset freezes. They are restrictions of an economic, financial, administrative nature, imposed from time to time, by Italian, European, the United Nations (UN) Security Council, the United States.
Customer and Counterparty Screening	Verification of the presence of customers' and counterparties' names in the *sanction lists* provided by *World-Check*.
Designated Persons	Persons or entities subject to sanctions. They are identified as any person (natural or legal) on an official international sanctions list.
Organisational Structures (or Structures)	This refers to the types of structures described in the illimity organisational chart, which are entrusted with the activities and responsibilities defined in the relevant internal rules and regulations 'Organisational Structure'.
Level 1 Facilities	Operating units within the Bank's Business Divisions responsible for the concrete management of customer relations.
Beneficial Owner	Natural person(s), other than the client, in whose interest or interests the continuing relationship is ultimately established, the professional service is eventually provided, or the transaction is finally carried out.
Transactions	This includes transactions with customers but also transactions with non-customers and other counterparties.

[1] The management of corporate clients under the retail model, who only have current accounts managed by the b-ilty digital platform, is characterised by the absence of dedicated relationship managers, who are instead present in managing customers once they have been entrusted.

4. REGULATORY CONTEXT

4.1 EXTERNAL REGULATIONS

4.1.1 International Regulations

The primary international regulatory references are listed below:

- Charter of the United Nations (1945) on restrictive measures to promote the maintenance or restoration of international peace and security;
- Treaty on the European Union of 1992, Title V on Common Foreign and Security Policy provisions, et seq;
- Treaty on the Functioning of the European Union of 1957, Title IV on Provisions on the Common Foreign and Security Policy, with particular reference to the application of restrictive measures, et seq;
- Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit, and transfer of dual-use items;
- EU regulations implementing both UN resolutions and autonomous Common Foreign and Security Policy (CFSP) decisions containing restrictive measures against regimes involved in severe human rights abuses and countries involved in the development of illicit nuclear enrichment programmes;
- FATF Recommendations to provide operational guidance for the application of financial sanctions;
- Code of Federal Regulations, Title 31 - Money and Finance: Treasury, Subtitle B - Regulations Relating to Money and Finance, Chapter V - Office of Foreign Assets Control, Department of the Treasury, Part. 501 - Reporting, Procedures and Penalties Regulations;
- Appendix A to CFR Part 501 - Economic Sanctions Enforcement Guidelines;
- “A Framework for OFAC Compliance Commitments.”

4.1.2 National regulations

The primary national regulatory references are listed below:

- Legislative Decree 109/2007, "Measures to prevent, counter and suppress the financing of terrorism and the activities of countries threatening international peace and security, implementing Directive 2005/60/EC", which transposes the anti-terrorist financing provisions and establishes the Financial Security Committee (FSC) to monitor and implement measures to freeze funds and economic resources, as amended;
- Legislative Decree No. 231 of 21 November 2007 (hereinafter referred to as the "Decree"), as amended by Legislative Decree No. 90 of 25 May 2017 (hereinafter referred to as the "Implementing Decree") and Legislative Decree No. 125/2019, which provides for amendments and additions to Legislative Decree No. 90/2017, as amended;
- Bank of Italy Decree of 27 May 2009 laying down operational instructions for the exercise of enhanced controls against the financing of weapons of mass destruction proliferation programmes;
- Legislative Decree No. 221 of 15 December 2017, implementing the delegation of powers to the Government referred to in Article 7 of Law No. 170 of 12 August 2016, for the adaptation of national legislation to the provisions of European legislation, to reorganise and simplify the procedures for the

authorisation of exports of dual-use items and technologies and the application of sanctions in the field of trade embargoes, as well as for any export transaction involving proliferation materials;

- FIU Notice of 24 March 2022 on Russian and Belarusian deposits according to Regulations 328/2022 and 398/2022.

4.2 INTERNAL REGULATIONS

Below are the primary references to the internal regulations adopted by the Group, which define the tasks, operational, and control activities to protect against the risk of money laundering and terrorist financing. The reference to the following internal regulations for the prevention of money laundering and the financing of terrorism is necessary due to the existence of common elements between the relative controls and those adopted for the management and control of the risk of violation of financial sanctions:

- Anti-Money Laundering Policy;
- Anti-Money Laundering Manual.

The internal framework adopted by the Group for the management and control of the risk of financial sanctions violations is completed by the Sanctions Compliance Officer's communications and by the "Country Table and Guide to Controls," available on the Group's intranet, which contains the list of countries affected by financial sanctions, the relevant restrictions, and the controls to be carried out about the types of rules applied.

5. GENERAL PRINCIPLES AND OPERATIONAL LIMITS

The Group ensures appropriate monitoring of financial sanctions regulations according to the type of client, the type of product or service offered, and the geographical area of reference using:

- Establishing strategic guidelines and policies to ensure compliance with financial sanctions;
- Organisational systems and procedures to ensure the proper handling of transactions involving, directly or indirectly, counterparties and countries subject to restrictive measures;
- The clear definition of the roles, tasks, and responsibilities of each organisational unit;
- The appointment of a Sanctions Compliance Officer as the person specifically responsible for overseeing the prevention and management of the risk of financial sanctions violations;
- Ongoing monitoring of staff compliance with internal procedures and legal and regulatory obligations relating to financial sanctions.

The Group applies, where necessary, the financial restrictions (e.g., freezing of assets and resources, prohibition of certain financial transactions, prohibition of documentary transactions related to the export of dual-use and/or dangerous goods) established by the relevant national or international bodies according to the legislation in force at the time.

In addition, it is firmly committed to ensuring compliance with applicable financial sanctions laws and regulations by adopting control measures and safeguards commensurate with the risk associated with each financially sanctioned country.

In particular, due to the nature and scope of the international sanctions imposed by the relevant authorities on the above countries, the authorisation/execution of the transaction in respect of clients domiciled, resident or located in Iran, Syria, or North Korea is subject to the binding opinion of Compliance & AFC.

Failure to comply with these regulations and this Policy could expose the Group and its entities to reputational damage, civil and criminal liability, fines, and/or severe restrictions on their business activities.
Please also note that any action aimed at facilitating, directly or indirectly, the circumvention of external regulations and the provisions of this Policy is prohibited. Any acts and/or omissions that may create potential or actual risks must be reported to the Sanctions Compliance Officer.

6. INTERNAL ORGANISATION

6.1 ROLES AND RESPONSIBILITIES OF CORPORATE BODIES

6.1.1 Strategic Oversight Body

The Board is ultimately responsible for supervising and effectively implementing financial sanctions legislation. In particular, this body:

- Approves the policy that illustrates and justifies the choices made by the intermediary for the different profiles in terms of organisational structures, procedures, and internal controls (the so-called Financial Sanctions Policy);
- Approves the guidelines of an organic and coordinated system of internal controls, functional for the prompt detection and management of the risk of violation of financial sanctions;
- Appoints and removes the Sanctions Compliance Officer;
- Ensures that tasks and responsibilities in the area of financial sanctions are clearly and appropriately allocated, that operational and control functions are separated, and that they are adequately resourced in terms of quality and quantity;
- Ensures that there is an adequate, complete, and timely flow of information to the governing bodies and between the control functions;
- Ensures deficiencies and anomalies identified as a result of controls are promptly brought to its attention, promotes the adoption of appropriate corrective actions, and evaluates their effectiveness.

6.1.2 Body with a Management Role

The Chief Executive Officer oversees the implementation of the strategic guidelines and governance policies approved by the Board of Directors and is responsible for adopting all measures necessary to ensure the effectiveness of the organisation and the internal control system. In adopting the operating procedures drawn up from time to time by the relevant structures, he takes account of the instructions and guidelines issued by the competent authorities and international bodies.

The CEO defines and oversees the implementation of an internal control system for the timely detection and management of the risk of financial sanctions violations and ensures its effectiveness over time. In addition:

- Defines a system of internal controls and oversees the implementation of the necessary initiatives and procedures to ensure the timely resolution of deficiencies and compliance with financial sanctions;
- Ensures the implementation of the Policy approved by the Board of Directors;
- Defines and oversees the implementation of information procedures to ensure that all relevant corporate functions and supervisory bodies are aware of risk factors;
- Sets up training programmes for staff on the obligations laid down. The training shall be continuous and systematic, considering the evolution of the rules and procedures established by the beneficiary;
- Puts in place the appropriate tools to monitor the activities carried out by employees to detect any anomalies, particularly in their behaviour, the quality of communications with contacts and company departments, and employees' relations with customers.

6.1.3 Body with a Supervisory Role

The body with a supervisory role (identified as the Management Control Committee for the Bank and the Board of Statutory Auditors for the beneficiary companies) monitors compliance with the rules and the completeness, functionality, and adequacy of the control systems, including concerning financial sanctions, and reports on any shortcomings and irregularities detected, requiring the adoption of appropriate corrective measures and verifying their effectiveness over time.

6.2 ROLES AND RESPONSIBILITIES OF CORPORATE FUNCTIONS

The system of safeguards to prevent, mitigate, and manage the risks of non-compliance with financial sanctions involves corporate bodies and functions, which continually align their activities with the regulations in force.

6.2.1 Compliance & AFC

Following a risk-based approach, the Compliance & AFC oversees the management of the risk of non-compliance with financial sanctions concerning the Company's business activities by assessing the adequacy of internal procedures designed to prevent non-compliance with applicable laws and regulations, regulatory requirements, internal policies, and self-regulatory sources to which the Group subscribes.
To carry out its duties, the Compliance & AFC, which reports directly to the Board of Directors, has access, as it deems appropriate, to all activities and information it considers relevant to the performance of its duties, such as:

- The definition of financial sanctions policies;
- Advising and assisting corporate bodies on financial sanctions, with particular reference to regulatory changes and their impact on the Bank's businesses and individual Group companies;
- Regulatory impact analysis with updated operating instructions for the Bank's businesses and individual Group companies;
- Updating of internal rules and procedures to integrate the controls adopted by the Group to manage the risk of financial penalties;

- The application of enhanced due diligence, in particular, the acquisition of authorisation (so-called PAC, "Customer Acceptance Process") if a customer declares to do business with a country subject to financial sanctions;
- Assess the reliability of the information system to ensure compliance with the restrictive measures;
- Manage relations with FIUs and supervisors regarding reporting obligations related to the application of freezing measures;
- Checks on the appropriateness of the assessments made by the first level;
- Fulfilment of training obligations, in particular concerning the Bank's business units and individual Group companies, as well as concerning operators involved in Level I financial sanctions controls;
- Reporting concerning the activities carried out under the financial sanctions risk assessment.

6.2.2 Sanctions Compliance Officer

To ensure compliance with financial sanctions, the Group appoints a Sanctions Compliance Officer (hereinafter also referred to as "**SCO**"), who is the Chief Compliance & AFC Officer (head of the structure of the same name), appointed and dismissed directly by the Board of Directors of the Parent Company, after informing the Risk Committee.

The role of the SCO is to ensure and monitor the effective implementation of this policy to prevent risks arising from non-compliance with financial sanctions. The Sanctions Compliance Officer reports on his activities directly to the Board of Directors and the Parent Company's controlling body and liaises with the corporate bodies of the Group companies, informing them of the results of the activities carried out within their competence.

The Sanctions Compliance Officer must:

- Have the necessary authority to perform all their tasks;
- Have the necessary experience and qualifications (i.e., be aware of the financial sanctions and risks associated with non-compliance with all relevant regulations, know the risk profile associated with the imposition of sanctions concerning the activities undertaken in terms of products, services, customers, and geographical locations);
- Have the necessary IT tools and systems at its disposal to perform its tasks effectively;
- Be actively involved in all matters relating to the effective implementation of compliance policies to prevent risks arising from non-compliance with financial sanctions (e.g., involvement in the development of new products, expansion into new markets/countries, review, or termination of customer relationships);
- Ensure the effective implementation of this Policy to prevent risks arising from non-compliance with financial sanctions;
- Set up and review procedures to prevent risks arising from non-compliance with financial sanctions;
- Ensure daily monitoring and internal controls on the proper implementation of the programme to prevent risks arising from non-compliance with financial sanctions;
- Validate the training plan to ensure compliance with the prevention of risks arising from non-compliance with financial sanctions and develop specialised training to achieve these objectives;
- Ensure and regularly monitor regulatory changes in financial sanctions;

- Monitor, where applicable to the Group, customer, and counterparty screening activities.

7. MANAGING RISKS RELATED TO FINANCIAL SANCTIONS

In the context of financial sanctions obligations, the legal framework provides for restrictive and sanctioning measures directed at third countries, as well as non-state entities and natural or legal persons, in particular:

- Arms embargoes;
- Other specific or general trade restrictions (e.g., export and import bans);
- Financial restrictions (e.g., freezing of assets and resources, bans on financial transactions, restrictions on export credits or investments);
- Restrictions on admission (e.g., visa or travel ban);
- Criminal sanctions for those who finance terrorist or subversive associations;
- Penalties for those who carry out export transactions of dual-use goods in violation of the prescribed administrative “dual-use” regulations.

Enhanced due diligence measures are in place to ensure that the Group does not breach the law in the course of its institutional activities, including:

- Background checks and checks on transactions. In this regard, the Group has adopted the so-called sanctions lists, i.e., the lists of names of sanctioned parties disseminated by the United Nations Security Council, the European Union, and OFAC, as well as the lists of countries subject to restrictive measures by third parties, and the "CSSE Transfers" procedure for monitoring transactions involving counterparties on the sanctions lists and/or countries subject to embargoes or restrictive measures;
- The traceability of controls applied to transactions originating in or destined for countries, persons, and entities subject to restrictions;
- The freezing of assets and resources traceable to designated persons subject to the restrictive measures and the transmission of the resulting notifications to the FIU;
- Suspicious Transaction Reporting.

To mitigate the risk of financial sanctions violations, Compliance & AFC continuously monitors the measures issued by the competent authorities (e.g., UN, EU, OFAC) and any changes to them and updates the internal reference documentation ("Country Table and Guide to Controls") available on the company's intranet, which contains the list of countries concerned, the relevant restrictions and the controls to be carried out concerning the types of rules applied.

7.1 RISK-BASED APPROACH: CUSTOMER PROFILING AND DUE DILIGENCE

The Group's risk-based approach to anti-money laundering and anti-terrorist financing obligations, which provides for the intensity and scope of customer due diligence modulated according to the level of risk associated with each customer, also considers the risk factors of breaching financial sanctions.
For the purposes of risk assessment, therefore, the following are considered:

- General assessment criteria relating to the customer, the beneficial owner (if any) and, where appropriate, the executor, and in particular, the country or geographical area of origin (including of

funds); business relationships; the activities carried out and the countries with which there are significant links; the economic and financial profile (in terms of income and assets). The staff will also consider the conduct at the time of opening the relationship or carrying out the transaction;

- General assessment criteria relating to the relationship or transaction, and in particular the nature of the product or service offered, its structure (assessed in terms of complexity and transparency), the channels used to distribute it, whether more than one party is involved, the technologies and payment methods that distinguish it, the amount, frequency and volume of transactions, the appropriateness of the ongoing relationship or transaction concerning the activity carried out and the overall economic profile of the customer (and the beneficial owner, if any), and the geographical area to which the funds are sent. Staff must pay greater attention to new or innovative products and services that allow for the frequent use of cash or the execution of substantial transactions.

In light of these criteria, the Group applies a profiling model based on four risk bands (insignificant, low, medium, and high), each of which is associated with a consistent level of depth, scope, and frequency of appropriate verification measures, so that the adequacy of their scope is always ensured. This model enables the automatic assignment of a risk profile based on consistent logic and centrally defined algorithms. Group companies establish models that are consistent with this profiling model.
The Parent Company and the Group companies assign a risk profile to each client using IT procedures or tools defined on an ad hoc basis to ensure that the risk profile automatically proposed by the system or calculated by the tool used is consistent with the customer's knowledge.

Risk assessment is particularly relevant at the following stages:

- At an early stage, to fulfil due diligence obligations by assessing the elements of identification of the customer, the authorised representative, and the beneficial owner for the establishment of an ongoing relationship or the execution of an occasional transaction;
- Throughout the relationship with the customer, review the customer's entire business and verify and update the data and information obtained during the due diligence process.

At each stage, non-compliance risk factors related to financial sanctions may influence the level of risk assigned to clients.
In particular, at the onboarding stage, the person's name on the so-called sanctions list will lead to a refusal to open the relationship. During the continuation of the relationship, the presence of the name of the subject among those included in the lists entails the obligation to abstain from the execution of the transaction or the continuation of the relationship with the application of the freezing measures in the cases provided for (see point 7.2.1, Measures for the freezing of funds).

In addition, a customer who declares that he is trading with a country subject to financial sanctions is assigned a high-risk profile when the relationship is opened. The following month, in the absence of any other high-risk factors for money laundering and terrorist financing, the customer will be assigned the appropriate risk profile based on the pre-defined algorithms of the GIANOS3D information procedure, as it is

envisaged that the enhanced monitoring of the possibility of operating with countries subject to financial sanctions will be carried out directly during the assessment of the transactions carried out by the customer. In particular, any transactions with countries subject to restrictive measures will be intercepted later by applying procedural safeguards that block transactions in the CSSE transfer procedure before they are entered into the accounts to allow specific assessments by the competent functions.

The risk-based approach is specifically applied in the context of customer due diligence measures, which is the primary obligation of those subject to anti-money laundering and terrorist financing requirements.
The content of this obligation consists of the following activities:

1. Identification of the client and the executor, if any;
2. Identification of the beneficial owner, if any;
3. Verification of the identity of the customer, the executor, and the beneficial owner, if any, based on documents, data, or information obtained from reliable and independent sources;
4. Obtaining and assessing information about the purpose and nature of the ongoing relationship and, where there is a high risk of money laundering and terrorist financing, the occasional transaction;
5. Exercise constant control during the ongoing relationship.

The above activities are also relevant in monitoring the risk of breaching financial sanctions. In particular, it is essential to identify customers and their habitual counterparties and continuously monitor them to determine whether the customer/counterparty is subject to sanctions and/or does business with countries subject to restrictive measures. Accordingly, the Bank and the Group companies take all the measures needed to obtain sufficient information to know their customers well.

Where there is a high risk of a breach of financial sanctions, determined based on specific regulatory requirements or an independent assessment of the customer's risk profile, enhanced customer due diligence measures are in place, characterised by a greater depth, breadth and frequency than standard measures.
According to the principle of the risk-based approach, if the customer declares during the due diligence process that it does business with countries subject to restrictive measures, authorisation ("PAC," "Customer Acceptance Process," for high risks) is obtained for the relevant customers, or, for Recipient Companies only, the Chief Executive Officer or General Manager (as applicable) or the respective heads of the organisational structures into which the Parent Company's business units are divided, who may act as their proxies, for the establishment or continuation of the ongoing relationship, subject to the prior opinion of Compliance & AFC.

To issue the above opinion, Compliance & AFC verifies (i) the information obtained during the due diligence phase, also analysing its congruence with the supporting documents provided, (ii) the correct identification of the beneficial owner carried out by the relevant functions based on the information reported by reliable and independent sources (e.g., Chamber of Commerce Visura), (iii) the presence on the sanctioned person lists and AML/CFT sensitive lists of the customer and the persons connected to him, and (iv) the nature of the restrictions adopted concerning the country in question. Chamber of Commerce Visura), (iii) the presence of the Customer and its related parties on the lists of sanctioned persons and AML/CFT sensitive lists, and (iv) the nature of the restrictions adopted concerning the country in which the Customer has declared to operate

during the due diligence concerning the activity carried out by the Customer, tracing the results of the analyses carried out and the documents examined in the document called "Customer File - PAC."

Companies should regularly update the customer due diligence information during the relationship. In particular, customer due diligence should be reviewed when events indicate that the risk associated with the customer has changed (e.g., transactions have been blocked or rejected, information obtained means that the customer's business has changed, and negative news has been obtained from public sources).

Because of this obligation, the necessary safeguards have been implemented to manage transactions with countries subject to restrictive measures, as better described in the context of continuous monitoring.

For anything not explicitly detailed here concerning customer profiling and due diligence, please look at the Anti-Money Laundering Policy and the Anti-Money Laundering Manual.

7.2 CONSTANT CONTROL AND OPERATION WITH SUBJECTS AND COUNTRIES SUBJECT TO RESTRICTIVE MEASURES

The Group is required to carry out continuous monitoring during the relationship with the customer to keep the customer profile up to date and to identify any anomalies that may constitute a breach of certain obligations (application of enhanced due diligence measures, suspicious transaction reports, refusal to execute the transaction or continue the relationship and application of freezing measures).

To ensure constant monitoring of customers in the context of financial sanctions risk management, the Group has set up a system for monitoring sanctions lists, thanks to the monthly processing of possible matches between customers and persons on the following lists provided by the World-Check infoprovider:

- UN, EU and OFAC;
- FBE - Financial Sanctions Database;
- EMBARGO VESSEL;
- CRIME - TERROR;
- NON-CONVICTION TERROR;
- CRIME - WAR.

In addition, with particular reference to incoming and outgoing transactions involving potential Designated Parties as counterparties, the Group's "CSSE Credit Transfers" procedure provides for the blocking of transactions before their entry into the accounts for verification by the relevant staff to exclude that the transaction involves counterparties on the lists of Designated Parties.

Similarly, the "CSSE Credit Transfers" procedure provides for the freezing of transactions before they are entered into the accounts for verification by the staff in charge to exclude that the transaction may fall within the scope of the restrictive measures imposed on the embargoed country.

Where appropriate or necessary, the results of the monitoring controls shall lead to (i) updating the information released during due diligence, (ii) raising the risk profile, (iii) identifying anomalies and inconsistencies that may lead to a Suspicious Transaction Report, (iv) freezing funds; (v) refraining from executing the transaction; (vi) terminating the relationship; and (vii) sending notifications to the authority.

7.2.1 Measures to Freeze Funds

In compliance with the obligations set out in Legislative Decree No. 109/2007 concerning the application of measures to freeze the funds and economic resources of persons who engage or attempt to engage in one or more forms of conduct aimed at financing programmes for the proliferation of weapons of mass destruction or one or more forms of conduct that threaten international peace and security, the Group carries out checks on the persons identified in the lists of designated persons when a new customer is registered and, every month, on existing customers.

For these checks, the Group uses, as mentioned above, the following lists of designated persons provided by the information provider World-Check:

- UN, EU and OFAC;
- FBE - Financial Sanctions Database;
- EMBARGO VESSEL;
- CRIME - TERROR;
- NON-CONVICTION TERROR;
- CRIME - WAR.

If the customer's name appears on the lists of designated persons, it is essential to verify the nature of the list on which the person appears. In this respect, it should be noted that the regulatory provisions of Legislative Decree 109/2007 provide specific obligations to freeze funds and notify the authorities only regarding persons on the UN and EU lists.

In particular, if the Bank's various business units or Group companies detect, through the use of the World-Check infoprovider, a positive correlation between a potential customer and one of the persons designated by the UN Security Council and the European Union, they will refrain from opening a relationship and, if the name is traced back to a person already associated with an active connection, they will immediately apply restrictive measures and freeze funds and economic resources.

This activity is immediately reported by email to the Sanctions Compliance Officer and SOS Manager. They are responsible for:

- Informing the FIU of the freezing measures applied to the designated persons, indicating the names of the persons concerned, the data relating to the transactions or relationships, and the amount and the nature of the funds or economic resources; in the latter case, it also informs the Special Currency Police Unit of the Guardia di Finanza;
- Forwarding a suspicious transaction report on terrorist financing or WMD proliferation activities to the FIU.

The funds and economic resources of persons subject to freezing measures may not be the subject of any act of transfer, disposal, or use on pain of the nullity of such actions.

It is also prohibited to make funds or economic resources available, directly or indirectly, to or for the benefit of designated persons or to participate in activities the object or effect of which is, directly or indirectly, to circumvent freezing measures.

The Bank's various business units and individual Group companies also report to the SOS/Sanctions Compliance Officer the presence of persons on lists drawn up by other institutions and bodies involved in the

fight against international terrorism, such as the US Treasury Department's Office of Foreign Asset Control (OFAC), even if there is no obligation to freeze their funds.

7.3 COMMUNICATIONS FROM THE SANCTION COMPLIANCE OFFICER

On the occasion of the introduction and/or amendment of the sanctions regimes applied by the competent authorities, the Sanctions Compliance Officer shall issue notices setting out the operational instructions to be followed by the Bank's Business Areas and individual Group Companies to ensure timely compliance with international and national external regulations and this Policy.

To this end, the notices shall include, but are not limited to:

- Normative references;
- The main innovations and measures provided for in the regulations and legislation;
- The requirements and operational procedures to be applied;
- The Business Areas of the Bank and the individual Group Companies to which the obligations and operating procedures are addressed.

8. CONTROL OVER TRANSACTIONS

8.1 SCREENING AND CONTROL OF COUNTRIES INVOLVED IN TRANSACTIONS

The Group has implemented a series of computerised and manual control measures concerning the screening and control of countries involved in transactions.

With particular reference to incoming and outgoing transactions involving embargoed countries, the procedural safeguards provided for the blocking of transactions in the "CSSE Credit Transfers" procedure before they are entered into the accounts to be checked by the staff in charge to exclude that the transaction may fall within the scope of the restrictive measures imposed on the embargoed country, with a subsequent mandatory formalisation in the procedure of the reasons underlying the transaction and justifying the exclusion, also attaching to the procedure the documentation collected in support of the checks made. Only after these checks have been carried out can the transaction be released for settlement.

In particular, computer blocks are foreseen in the case of a counterparty and/or a counterparty bank domiciled/headquartered in a country subject to restrictive measures or a counterparty and/or counterparty bank on the list of designated entities.

To process transfers blocked by the "CSSE Transfers" procedure, the operator accesses the core banking system (H20) in the "Services Menu" and, by selecting the "Listed Subjects" option, accesses the list of blocked transfers.

To guide the control activities to be carried out by the Business Areas, Compliance & AFC continuously monitors the measures issued by the competent authorities (e.g., UN, EU, OFAC) and the relevant amendments and prepares and updates the Country Table and Control Guide, which is available on the corporate intranet and contains the list of countries concerned, the applicable restrictions and the indication of the controls to be carried out concerning the types of rules applied. The Business Areas responsible for supervisory activities must look at the Country Table and Control Guide and follow the guidance, seeking assistance from Compliance & AFC as required.

Finally, to comply with commodity restrictions in commercial transactions, the Group also has general and transaction-specific declarations of compliance that must be submitted to its customers to collect the identifying elements of the transaction (e.g., type of transaction, currency, amount, originator, and beneficiary), the underlying commodity (e.g., seller subject, buyer subject, description of the supply) and the declaration of compliance of the transaction and indemnity. (e.g., type of transaction, currency, amount, originator, and beneficiary), the underlying commodity (e.g. seller subject, buyer subject, description of the supply, TARIC code) and the declaration of conformity of the transaction and indemnity in favour of the Group and the commitment of the customer to provide the technical, commercial and/or customs documentation.

8.1.1 Management of Customer Operations - Natural Persons: Control and Verification of Transactions

In the case of transactions with customers who are natural persons, and which involve a country subject to restrictive measures, the procedure alerts the operator with the following message:
"*Warning, counterparty country subject to restrictive measures and/or on the list of high-risk third countries."*
After receiving this notification, the operator must perform verification activities to ensure that the transaction is consistent with the characteristics and profile of the customer.

Once the transfer has been blocked by the "CSSE Credit Transfers" procedure, to authorise the transaction, the operator must verify that it corresponds to the customer's profile and the information collected during the due diligence process, in particular concerning transactions with countries subject to restrictive measures and information on the customer's income and assets profile.
For this purpose, the elements that should be considered are:

- The type of operation;
- The amount of the operation;
- The relationship between the counterparties involved.

If certain information necessary to complete the verification activities is missing, the control operator must contact the customer to obtain the missing information, retaining evidence of the attempt to contact the customer, the response provided, and any documentation collected during the in-depth investigation.
Evidence of the attempted contact (e.g., e-mails requesting further details and information about the reasons for the transaction and/or the relationships and links between the counterparties to the transaction) must be attached to the blocked transaction in the “CSSE Credit Transfers” procedure.

Limited to transactions carried out by Retail customers - natural persons, to standardise the verification activities and their results, the Operator - to be able to proceed with the unblocking of the transaction in the procedure - uses the following set of reasons prepared by Compliance & AFC.

In particular, based on the amount of the transaction, the type of transaction, and the parties involved, the operator must enter the justification in the appropriate field of the "CSSE Credit Transfers" procedure, which must reflect the analysis carried out and the characteristics of the credit transfer transaction and the counterparties involved (originator and beneficiary).

Based on the chosen justification, the operator can also attach any available related documentation.

In the case of transactions that cannot be attributed to any of the types of transaction/subject listed below, the release of the transaction will be subject to a review of the transaction in terms of gathering all relevant information to know the motivation behind the transaction and the nature of the relationship between the customer and the counterparty, to ensure that the transaction does not violate the restrictive measures in force in the country of origin/destination of the transaction.

Amount	***Type of actors involved***	***Type of operation***	***Motivation***	***Type of attachment***
Less than €500	Individuals with ties: family members, personal relationships with the individual	Recurrent entry/exit	Transaction of small value (< €500) in favour of/by a person whose family/personal relationship has been verified.	If first operation, evidence of the information issued by the customer. If repeated operation, evidence of the movement reporting the first operation of the same type.
		One-off transaction (e.g., loan)		
		Exchange of money for basic needs		
		Transfer operation	Transaction of small value (< €500) to/from another account of the same name opened with another intermediary (Giroconto)	Not necessary
Less than €500	Individuals with professional ties	Remuneration for collaboration (e.g. invoice for consultancy service)	Transaction of low value (< € 500) in favour of/by a person whose professional relationship has been verified	If first operation, evidence of the information issued by the customer. If repeated operation, evidence of the movement reporting the first operation of the same type.
		Payment of salary		Not necessary
		Life annuity		
		Pension		
Less than €500	Individuals with contractual ties	Transferring funds to and from wallets/prepaid cards	Transaction of small value (< €500) to/from a person whose transfer to/from digital *wallets* (*e.g. crypto assets*) and prepaid cards has been verified	Not necessary
		Deferred payment transaction	Transaction of low value (< €500) in favour of/by a person whose link has been verified by contract	If first operation, evidence of the information issued by the customer. If repeated operation, evidence of the movement reporting the first operation of the same type.
		Exchange of money for justified contractual needs		
Less than €500	Individuals with other ties	Entry/exit justified by appropriate act	Transaction of small value (< €500) in favour of/from a person whose ties have been verified through other types of relationships	If first operation, evidence of the information issued by the customer. If repeated operation, evidence of the movement reporting the first operation of the same type.
Greater than €500	Individuals with ties: family members, personal relationships with the individual	Recurrent entry/exit	High-value transaction (> €500) to/from a person whose family/personal relationship has been verified	If first operation, evidence of the information issued by the customer. If repeated operation, evidence of the movement reporting the first operation of the same type.
		One-off transaction (e.g. loan)		
		Exchange of money for basic needs		
		Transfer operation	High-value transaction (> €500) to/from another account in the same name with another intermediary (Giroconto)	Not necessary. Note: evidence required if value, even cumulated, > asset/income profile
Greater than €500	Individuals with professional ties	Remuneration for collaboration (e.g. invoice for consultancy service)	High-value transaction (> €500) to/from a person whose professional relationship has been verified	If first operation, evidence of the information issued by the customer. If repeated operation, evidence of the movement reporting the first operation of the same type.
		Payment of salary		Not necessary. NB: evidence required if value > income profile
		Life annuity		
		Pension		

Amount	*Type of actors involved*	*Type of operation*	*Motivation*	*Type of attachment*
Greater than €500	Individuals with contractual ties	Transferring funds to and from wallets/prepaid *cards*	High-value transaction (> €500) to/from a person whose transfer to and from digital *wallets* (e.g. crypto-assets) and prepaid cards has been verified	Not necessary. NB: evidence required if value, even cumulated, > asset/income profile
		Deferred payment transaction	High-value transaction (> €500) to/from a person whose ties has been verified by contract	If first operation, evidence of the information issued by the customer. If repeated operation, evidence of the movement reporting the first operation of the same type.
		Exchange of money for justified contractual needs		
Greater than €500	Individuals with other ties	Entry/exit justified by appropriate act	High-value transaction (> €500) to/from a person whose connection has been verified through other types of relationships	If first operation, evidence of the information issued by the customer. If repeated operation, evidence of the movement reporting the first operation of the same type.
All	All	Technical release of the operation	Incoming instant transaction, for which a technical release is required, to close the transaction as it has already been cancelled	Evidence of cancellation request
			Incoming/outgoing transaction for which the customer did not respond to the request made on dd/mm/yyyy and for which cancellation is being made	Evidence of request sent to customer

8.1.2 Management of Legal Entities - Customer Operations: Control and Verification of Transactions

In the context of the screening and control activities relating to the operations of legal entity customers, payment transactions are of a commercial nature as they relate, for example, to the supply of goods and services.

Even in these circumstances, the "CSSE Credit Transfers" procedure generates operational blocks to intercept *ex ante* incoming and outgoing credit transfers involving countries subject to restrictive measures to allow the necessary evaluations by the staff in charge.

In the case of a country subject to restrictive measures, the procedure alerts the operator with the following message:

"*Warning, counterparty country subject to restrictive measures and/or on the list of high-risk third countries."*

In connection with the pre-issuance verification of payment transactions that are commercial and involve a country subject to restrictive measures, it is always necessary to proceed as described below to exclude the presence of dual-use items in the transaction:

- Check whether the transaction is customary and whether the customer has declared in the Due Diligence Questionnaire that it has business dealings with that country. If not, the operator will contact the customer to collect the updated information;
- Verify the nature of the transaction, the motive, and the counterparty - including by investigating open sources (company websites) to verify the consistency of the transaction with the counterparty's business purpose and stated motive;
- Perform a TARIC verification of the commodity code via the portal provided by the European Union (also accessible via the EU Sanctions Map page). The system will extract the details of the nature of the goods and whether they are subject to any particular restrictions - i.e., if the checks reveal evidence

such as "Country Russia - Code MG561: prior authorisation is required to sell, supply, transfer or export, directly or indirectly, the goods..." - the trader will ask the customer to produce a copy of the ministerial licence issued to them. Otherwise, they will not be able to authorise the transaction;

- To carry out these verifications, the operator may use the declarations of conformity, both general and for each transaction, available on the company's intranet, to be submitted to the customer to collect the identifying elements of the transaction (e.g., type of transaction, currency, amount, originator and beneficiary), the underlying commodity (e.g., seller subject, buyer subject, description of the supply) and the declaration of conformity of the transaction indemnity in favour of the Group and the commitment of the customer to provide the technical, commercial and/or customs documentation;
- Finally, the operator can contact the customer directly and ask him to carry out this check with his technical department; the result (sent by the customer by e-mail) will be checked and attached to the procedure among the documents collected.

By way of example, but not limited to, the documentation to be collected for the checks to be carried out on the operation is listed below:

- Copy of the invoice;
- Contract for the supply of goods and/or services;
- Company's visura (certificate of incorporation) to verify consistency between the transaction and the company's purpose;
- If the payer and invoice holder do not coincide, any documentation adequately justifying this circumstance (e.g., contract in place between the parties, unilateral declaration, correspondence);
- Documentation indicating the TARIC codes referring to the goods (in some cases, this information may also be on the invoice);
- Evidence from the TARIC Consultation portal about the code under analysis;
- Self-declaration of dual-use products;
- Potential technical report by an expert to exclude the dual-use nature of the asset;
- Presentation sheet of the exported products showing their characteristics to exclude the dual-use nature of the goods;
- Any authorisations held by the customer if the import/export regime provided for by the legislation provides for special ministerial authorisations (e.g., by the Ministry of Economic Development in the case of dual-use goods).

To fulfil the obligations to prevent, mitigate, and manage the risk of violation of financial penalties, the operator is required to:

- Verify that the counterparty, as indicated on the invoice, is not on the sanctions list by manually querying the World-Check database(s) by accessing the Refinitiv link and using the username provided, and (ii) the SGR-Liste nominativi Antiriciclaggio Italia database by accessing the H20 management software - Servizi - Soggetti da controllare;
- Verify that the goods on the invoice are not subject to special restrictions by checking the TARIC commodity code by consulting the portal provided by the European Union (TARIC Consultation, which

is also accessible via the page EU Sanctions Map), entering the TARIC code and the reference country of the transaction;

- Check that the country of residence of the counterparty is not listed in the Country Table and Control Guide, which is available on the company intranet and provided by Compliance & AFC. It is possible to identify the country of residence of the counterparty within the invoice or by using available open sources such as the counterparty's website;
- Keep evidence and the results of the above checks in the reference file of the customer requesting the transaction.

All documents collected for the verification activities carried out - including, for example, the reason for the blocking of the transfer in the procedure, any communications with the customer who may have been contacted, and technical and/or commercial documentation - must be adequately stored and attached to the procedure to allow ex-post verification of the consistency and legitimacy of the unblocking of transactions.

If certain information necessary for the completion of the verification activities is missing, the operator in charge of the control shall contact the customer to obtain the missing information, keeping evidence of the attempt to contact the customer, of the relevant response provided, and of any documentation collected during the investigations carried out.

8.2 SCREENING AND CONTROL OF CUSTOMERS AND COUNTERPARTIES INVOLVED IN TRANSACTIONS

The Group has also put in place several computerised and manual control systems for the screening and monitoring of customers and counterparties involved in transactions.

Among the computerised safeguards, with particular reference to incoming and outgoing transactions involving potential designated counterparties and/or counterparties' banks, is blocking transactions using the "CSSE Credit Transfers" procedure before they are entered in the accounts.

The first level of assessment of the matches with the sensitive AML/CFT lists is outsourced to the company Selir[2] whose Back Office verifies whether the counterparty and/or the counterparty's bank matches the lists through the compilation of a *checklist*[3] which is guided in the "CSSE Credit Transfers" procedure.

In the case of a false positive, Selir's staff will autonomously exclude the match without the intervention of the Group's staff. In contrast, in the case of doubt or a confirmed match, the evidence will be reported directly to the Group's staff in the core banking system to exclude that the transaction involves counterparties on the lists of designated parties, with subsequent mandatory formalisation in the procedure of the reasons underlying the

[2] Sella Group company.

[3] For natural persons, the checklist consists of the following four questions: (i) name of the counterparty other than the person on the sanctions lists, (ii) surname of the counterparty other than the person on the sanctions lists, (iii) other information available other than the sanctioned person, and (iv) whether the person is on the sanctions lists. In the case of legal persons, the checklist contains the following four questions: (i) name of the counterparty other than the person on the sanctions lists, (ii) initials (e.g., SpA) of the beneficial owner other than the person on the sanctions lists, (iii) other information available other than information relating to the sanctioned person, and (iv) whether the person is on the sanctions lists.

transaction and justifying the exclusion. Only after these verifications can the transaction be released for settlement.
In particular, in the case of a counterparty and/or counterparty's bank with a possible match in the lists of designated parties, the system indicates the counterparty and/or counterparty's bank on which the possible match was found. In such a case, the operator is requested to check the 'Evidence Detail' in H2O to confirm the match by answering the relevant questions suggested by the system in H2O via the checklist.

Also available on the Evidence Detail screen is the normative reference on which the name listing corresponding to the match is based.

For name match management, it is also possible to use the authorities' Internet portals, searching for the names and any aliases of persons on the lists:

- The search service is available for EU-designated entities at: *"Consolidated list of persons, groups and entities subject to EU financial sanctions."*
- The relevant search service is available for US and OFAC-designated persons at "*Sanction List Search,*" belonging to the OFAC.

In particularly complex cases, it is always possible to contact Compliance & AFC for specialist assistance in assessing the transaction and the match that has occurred.

8.3 SCREENING AND CONTROL OF THE CONTENT OF CAUSAL ENTRIES IN TRANSACTIONS

The Group has put in place controls, including IT controls, to review and control the content of transaction records.
With particular reference to incoming and outgoing transactions, the content of which includes (i) the name and/or pseudonym of potential designated persons, (ii) certain text strings included in a specific blacklist, the information safeguards provide for the blocking of transactions in the "CSSE Credit Transfers" procedure before they are entered in the accounts, with a record in the system of the decision taken (to confirm the block or to unblock the transaction) and the reasons for it, with the possibility of attaching the documents collected in support of the checks carried out.
If certain information necessary to complete the verification activities is missing, the operator will contact the customer to obtain the missing information, retaining evidence of the attempt to contact the customer, the response received, and any documentation collected during the in-depth investigation.

In particularly complex cases, it is always possible to contact Compliance & AFC for specialist assistance in assessing the match that has occurred.

9. ASSESSMENT OF RISKS ASSOCIATED WITH FINANCIAL SANCTIONS - SELF-RISK ASSESSMENT

Understanding the risk profile of non-compliance with financial sanctions enables the Bank and its subsidiaries to assess the nature and extent of the risks involved, take appropriate mitigating action, and identify possible areas for improvement and further action to strengthen the overall internal control system.
To this end, the Group assesses its exposure to financial sanctions every three years based on the framework established by the OFAC. This methodological framework provides that the level of risk to which it is exposed in the area of financial sanctions - residual risk - is determined based on a specific risk matrix contained in the Annex to the Code of Federal Regulation "Appendix A to Part 501 - Economic Sanctions Enforcement Guidelines". as a combination of two distinct elements: (i) the inherent risk, i.e., the potential risk to which the intermediary is exposed based on the nature, complexity, and scope of the business activities conducted; and (ii) the vulnerability analysis, i.e., the assessment of the adequacy and robustness of the organisational structure and corporate safeguards adopted by the intermediary to protect against and mitigate the inherent risk.
The final result of the self-assessment forms the basis of the risk-based approach, which is the prerequisite for (i) implementing specific corrective actions for any critical issues identified and (ii) defining appropriate risk prevention and mitigation strategies.

From an operational point of view, the exercise is conducted using a model:

- Based on quantitative and qualitative data;
- That can offer a view also of the performance of risks concerning subsequent similar financial years;
- Capable of being promptly updated if new major risks emerge or if significant changes in operations, organizational, or corporate structure occur.

The methodology approved by the Parent Company's Board of Directors is attached to this Policy (see Appendix 1).

10. OTHER DUTIES OF THE COMPLIANCE & AFC STRUCTURE

Similar to the system of internal controls in the area of anti-money laundering, the system of internal controls to prevent the risk of violation of financial sanctions includes the following types of controls, both at the level of the Parent Company and at the level of the Group companies:

a) Line controls, carried out by the Back Office (e.g., systematic and spot checks), i.e., incorporated into IT procedures and aimed at ensuring the proper conduct of operations;
b) Second-level controls carried out by Compliance & AFC and reported every quarter to the corporate bodies of the Parent Company and Group Companies;
c) The Internal Audit Department carries out third-level controls.

Compliance & AFC, as part of the system of internal controls designed to protect against the risk of non-compliance with financial sanctions, periodically carries out various types of controls, using an approach based on the following guiding principles: (i) efficient control, through massive (and not random) controls on the entire

customer base, a volume that allows representative results of the entire database and a lower frequency of execution; (ii) data (lake) driven control, aimed at avoiding fragmentation of the sources used for controls, identifying the single database (the so-called "data lake in the illimity cloud") as the only and complete source for the execution of controls; (iii) control by progressive steps, aimed at searching, without the intervention of analysts, evidence of anomalies or even simple 'clues' of the same, the relevance of which (detected when tolerance thresholds are exceeded) triggers further human-based analysis steps.

This approach favours the streamlining of control activities using automation logic and rules for evaluating results through the study and development of algorithms that enable the automatic collection of information and, where possible, its interpretation and evaluation, thus achieving more significant savings in terms of time and resources devoted to *ex post* control, also in favour of greater control of *ex ante* control, functional to the compliance by design of processes, products, and services (also in the context of participation in the Group's project activities).

Compliance & AFC, in line with the dynamic nature of the control action, which implies a continuous review of controls, has defined a catalogue of Level II controls on financial sanctions, to assess (i) the correctness and adequacy of the first-level controls on transfers intercepted by the "CSSE Credit Transfers" procedure, (ii) compliance with the reference legislation and consequent timely updating of internal procedures, (iii) the correct application of the processes defined in the context of constant control to guard against the risk of violation of financial sanctions (i.e. customer profiling, application of the enhanced deliberative process - PAC). This control catalogue is drawn up and updated by the function based on the new business (and related processes and procedures) of the Bank and the Group companies to ensure ongoing compliance with financial sanctions legislation.

Extraction and sampling criteria, control scope, techniques, and timing for performing each control are defined by the function and illustrated in the Reference Catalogue to obtain meaningful and reliable results.

The catalogue consists of specific controls, in particular:

- Permanent controls - Standardised second-level controls on processes or individual process steps required by regulatory requirements (including internal requirements), performed by the Compliance & AFC Structure without recourse to delegation to third-party functions, formalised in a specific catalogue that is constantly updated;
- Controls performed within the processes - Controls performed within the processes are carried out directly by the Compliance & AFC Structure.

In addition, the methodology concerning the execution of second-level controls also consists of the following operational controls:

- Compliance tests for the execution of technical-functional checks carried out directly by the Compliance & AFC Structure, in particular concerning specific IT interventions involving the release of new developments or modifications (changes) in the production environment, also as a result of the corrective actions required to resolve detected non-compliance situations;

- Tangible evidence as the underlying principle of a timely and substantive review of documentation and factual evidence to demonstrate the correct implementation of recommendations;
- Increase in the level of risk associated with the previously identified deficiencies, starting from the second postponement of the agreed timetable for the implementation of the identified corrective actions, at the request of the risk owner and without any supervening and objective reasons being given to justify the delay.

The planning and execution of the different types of controls follow an 'adaptive' logic that provides for quarterly planning of the permanent controls in the catalogue, mainly according to the following drivers:

- Results of second-level checks carried out in previous quarters;
- Verification that the remedial measures defined as a result of the checks carried out have been implemented (according to the agreed timetable);
- Availability of the structured data sets needed for verification activities;
- Outcomes of control activities carried out by other corporate functions (e.g., Internal Audit, Risk Management) and/or outcomes of the same;
- Points of attention and/or critical issues that may have emerged in analysing customer complaints or reported by the competent supervisory authorities.

This approach allows for the flexibility to focus controls on contingent business developments, which does not necessarily imply executing the full range of controls in the Catalogue throughout the calendar year. It allows for the quarterly planning of controls to be modified at any time according to objective factors aimed at preventing and managing the risk of non-compliance, subject to adequate justification of the rationale behind the choices made.

The presentation of the results of the controls, reported quarterly in the *Tableau de Bord*, summarises the risk of non-compliance according to the following scale:

- Insignificant or no risk of non-compliance;
- Low risk of non-compliance;
- Medium risk of non-compliance;
- High risk of non-compliance.

Based on the risk of non-compliance underlying each control, the Compliance & AFC Structure defines remediation activities to be implemented and/or proposals to be adopted.

To identify the exposure to the risk of non-compliance with the regulatory requirements for financial sanctions and the relevant implementing provisions of each audit, each material situation with a medium or high risk of non-compliance, revealed during the audit, is associated with a summary indicator of the related risk of non-compliance, composed of four key elements *(i)* presumable impact of administrative sanctions imposed by the supervisory authorities, distinguishing between procedural violations and those to the direct detriment of customers (*business conduct risk*); *(ii)* presumable application of other measures, not sanctions, by the same authorities (and/or the A.G.) having an impact on the current or prospective *business* of the Group companies; *(iii)* reputational effects caused by such measures or by proven situations of non-compliance detected; *(iv) the*

likelihood of *litigation* with customers and/or counterparties as well as rulings according to Legislative Decree No. 231/2001.
This indicator is presented quantitatively in the *Tableau de Bord* to provide an immediate perception of the severity of the non-compliance situation and a breakdown of the individual contribution of the four factors mentioned above to the indicator value.

Finally, within the scope of its prerogatives and tasks, the Compliance & AFC Structure provides specialised advice and assistance to the operational functions concerned and to the bodies of the Parent Company and the Group companies on how to comply with the rules on financial penalties.

11. TRAINING

Aware that the effective application of financial sanctions regulations requires complete knowledge of their objectives, principles, obligations, and responsibilities, the Group implements specific staff training programmes on the obligations laid down in the regulations to spread a culture of financial sanctions risk among its employees and to make all staff aware of the issues related to this risk.
The training is designed to provide specific preparation for employees who have the most direct contact with clients and employees of the Compliance & AFC Structure, with specific initiatives designed to keep them abreast of developments in financial sanctions legislation.
The Compliance & AFC Structure is responsible for drawing up an annual training plan to ensure the continuous training of employees and collaborators of the Parent Company and the Group companies.

12. APPENDICES

APPENDIX 1

Methodology for Conducting Sanction Risk Assessment

The risk assessment exercise applies an operational process consistent with "A Framework for OFAC Compliance Commitments" and the OFAC Risk Matrix outlined in Appendix A to Part 501 of the Code of Federal Regulations. The exercise is conducted on a triennial basis or whenever events occur, such as changes/developments in the Parent Company and Group Companies business that directly increase business to/from foreign countries.

From an organisational point of view, the *risk assessment* exercise involves five different operational steps:

1. **Definition of indicators** for conducting the risk assessment, consistent with the elements provided in the OFAC Risk Matrix and with what is regulated in the document "A Framework for OFAC Compliance Commitments;"
2. **Identification of the inherent risk**, i.e. the current and potential risks to which the Group is exposed based on a series of indicators;
3. **Identification of the vulnerability of the safeguards** through the analysis of the organisational set-up, prevention and monitoring of the risks previously identified. This analysis is conducted regarding both the **set-up** and **functioning of the** safeguards;
4. **Determination of the residual risk**, i.e., the assessment of the level of risk to which the Group is exposed due to the level of inherent risk and the robustness of the safeguards in place. This assessment is made considering the three levels of assessment proposed in the OFAC matrix;
5. **Identification of remedial** actions that are understood as the corrective actions to address any existing critical issues and aimed at strengthening the measures to prevent and mitigate the risk of violation of OFAC regulations.

Definition of indicators

The preparatory phase for conducting the risk assessment consists of identifying the indicators against which the risk of OFAC violations will be assessed, taking into account the nature, characteristics, and corporate structure of the Group.

Identification of inherent risk

The inherent risk is evaluated based on the elements defined within the first section of the OFAC Risk Matrix, based on qualitative and quantitative indicators referable to specific risk factors. In particular, the following 6 risk factors are identified:

1. Level of customer articulation;
2. Riskiness of customers;
3. Foreign branches and correspondence accounts;
4. Electronic products and services;
5. Amount/number of transfers;

6. Other international transactions.

For each risk factor, specific - potentially applicable - indicators are identified.

Each indicator is associated with:

- Qualitative measure/evidence that allows each indicator to be associated with a specific value that is representative of the risk dimension under consideration;
- A "weight" (called a weighting factor) concerning its impact on the overall risk assessment;
- A "rating," which helps attribute to each indicator the relative level of inherent risk based on the three-level scale defined by the OFAC matrix; this level is determined based on the indicator's measure concerning the parameters defined and formalised according to the market reference metrics or representative values of the risk dimensions studied.

For the assessment of inherent risk, the summary judgement at the Group level is calculated as a weighted average of the value of each indicator considered and summarised by a numerical value.

Identifying the vulnerabilities of headmasters

The vulnerability assessment of the adopted safeguards concerns the components a sanctions compliance programme should have, as set out in “A Framework for OFAC Compliance Commitments.” In particular, the following five areas of analysis are identified:

- Management Commitment;
- Risk Assessment;
- Internal Controls;
- Testing & Auditing;
- Training.

The methodology used to assess the degree of vulnerability of OFAC facilities is structured according to the following logical steps:

1. Assessment of the conformity of the facility in terms of completeness and adequacy;
2. Assessment of the functioning of the controls conducted taking into consideration Key Performance Indicators ("KPIs") - potentially applicable to the Bank - with reference to the second section of the OFAC Risk Matrix;
3. Calculation of the degree of vulnerability of OFAC facilities;
4. Rescaling of the degree of vulnerability of OFAC facilities given the values in the Risk Matrix.

The summary judgement on the vulnerability of the Group's adopted OFAC safeguards is derived from the combination of the facility and operational assessments.

From an operational point of view, the plant assessment is conducted for specific "Macro requirements"[4] appropriately identified against each of the five areas of analysis mentioned above.

[4] The macro requirements define requirements to which the Bank must conform to ensure the compliance of its OFAC Sanction Compliance Programme, based on the provisions of the document “A Framework for OFAC Compliance Commitments.”

The purpose of the facility assessment is, in particular, to verify that the internal controls in place comply with the relevant regulations; to this end, specific checklists are prepared for each macro requirement to guide the assessment of the institutions, divided into the following categories[5]:

- Organisational, operational, and internal control systems;
- technical/information technology.

The facility assessment results in a compliance rating for the "completeness and adequacy of the OFAC facility" using a 3-point rating scale.

Following the assignment of this compliance rating to each macro requirement, the "overall compliance rating" (facility rating) is determined at the level of the scope of analysis as the average of the ratings assigned to each risk scenario to which it relates.

The scale adopted provides for the following overall compliance ratings:

- Inadequate;
- Partially adequate;
- Adequate

Key Performance Indicators (KPIs) of a qualitative/quantitative nature are used to assess the functioning of controls.

For each KPI, the following are identified:

- Qualitative measure/evidence that allows each indicator to be associated with a specific value that is representative of the risk dimension under consideration;
- A "weight" (called a weighting factor) concerning its impact on the overall risk assessment;
- A "rating," which helps attribute to each indicator the relative level of inherent risk based on the three-level scale defined by the OFAC matrix; this level is determined based on the indicator's measure concerning the parameters defined and formalised according to the market reference metrics or representative values of the risk dimensions studied.

For each area of analysis, the conformity of OFAC's performance is determined as a weighted average of the quantitative value attributed to each KPI within that area.

The scale adopted provides for the following ratings of operational conformity (plant abatement):

- Inadequate;
- Partially adequate;
- Adequate

The OFAC vulnerability assessment for each area of analysis, expressed in percentage terms, is determined using the following formula:

1-[Installation Overall Conformity Judgement×(1-Operating Conformity Judgement)]

To arrive at a final value consistent with the rating scale proposed by the Office of Foreign Assets Control (scale from 1 to 3), a rescaling formula is - finally - applied to the vulnerability rating determined in percentage terms for each area. The rescaling formula is as follows:

[5] Each control category is assigned a "weight" (a weighting factor) concerning its impact on the potential mitigation of the underlying risks. The weights are defined in such a way that their sum equals 1. The assigned weights are adjustable, considering both the possibility that the control category is not applicable and its importance concerning the area of analysis in question.

*Numerical vulnerability value OFAC=(Vulnerability assessment %)/(100%)*2+1*

The overall OFAC vulnerability rating for the Group is determined as a weighted average of the ratings assigned to each area of analysis.

The scale adopted in order to assign a rating to the degree of vulnerability is as follows:

- Very significant;
- Moderately significant;
- Insignificant.

Definition of residual risk

Once the overall level of inherent risk and the general degree of vulnerability has been determined, a residual risk rating can be determined by entering the findings into the matrix suggested in Appendix A to Part 501 - Economic Sanctions Enforcement Guidelines.

Residual Risk Graph					
Inherent risk	3. High Risk	3	Residual Risk Moderate	Residual Risk High	Residual Risk High
	2. Medium Risk	2	Residual Risk Moderate	Residual Risk Moderate	Residual Risk High
	1. Low risk	1	Residual Risk Low	Residual Risk Moderate	Residual Risk Moderate
			1	2	3
			Insignificant	Moderately significant	Very significant
			Vulnerability OFAC Presidia		

Rescaling

To combine the Sanction Risk Assessment with the Money Laundering Risk Self-Assessment exercise, a ***rescaling*** determined by using the following formula is applied to the numerical value of the **inherent risk** and **vulnerability of the safeguards:**

$$Rescaling\ rischio\ inerente = \frac{Rischio\ inerente * 4}{3}$$

$$Rescaling\ vulnerabilità\ dei\ presidi = \frac{Vulnerabilità\ presidi * 4}{3}$$

The following 4-value rating scale is therefore adopted for assessing the inherent risk:

- High risk;
- Medium-high risk;
- Medium-low risk;
- Low risk.

In addition, the following rating scale, again with 4 values, for assessing the vulnerability of facilities:

- Very significant;
- Moderately significant;

- Low significance;
- Insignificant.

Finally, once the overall level of inherent risk and the overall degree of vulnerability has been determined through rescaling, it is possible to determine the residual risk rating using the following matrix:

Residual Risk Graph						
Inherent risk	4. High Risk	4	Residual Risk Medium	Residual Risk Medium	High Residual Risk	High Residual Risk
	3. Medium-High Risk	3	Low Residual Risk	Low Residual Risk	Residual Risk Medium	High Residual Risk
	2. Medium-Low Risk	2	Residual Risk Not significant	Low Residual Risk	Residual Risk Medium	Residual Risk Medium
	1. Low risk	1	Residual Risk Not significant	Residual Risk Not significant	Low Residual Risk	Low Residual Risk
			1	2	3	4
			Insignificant	Low Significance	Moderately significant	Very significant
			Vulnerability OFAC Presidia			

Identification of Remedial Actions

Identifying corrective actions is required when the residual risk is high. In the case of low or insignificant residual risk, the definition of mitigating measures can be evaluated. In addition, ad hoc corrective actions shall be identified whenever the assessment of the vulnerability of the safeguards to specific risk scenarios is very significant.

APPENDIX 2

A. Owner *of* the "enhanced due diligence measures" area for illimity Bank: Approval by the First Level Manager to commence or continue the ongoing relationship, subject to the opinion of Compliance & AFC.

illimitybank.com	**Division b-ilty**	**Division Growth Credit**	**Division Investment Banking**	**Division Specialised Credit**
Digital Customer Operations	Digital Customer Operations	Digital Customer Operations (Factoring) Credit Middle Office (Turnaround, Crossover) Business Operation & Credit Support (*former* BIP)	Digital Customer Operations (Back Office Accounting & Treasury)	Credit Middle Office *(with support from the reference manager)*

Head of Digital Customer Operations	Head of Digital Customer Operations *(for b-ilty customers with current account only)* Head of Sales and Account Management *(for b-ilty customers with credit + current account)*	Head of Factoring Head of Turnaround Head of Crossover & Acquisition Finance (Crossover) Head of Business Operation & Credit Support (formerly BIP).	Head of Corporate Solutions Head of Capital Markets Head of Structuring	Head of Special Situation Real Estate Head of Senior Financing Head of Special Situation Energy

B. <u>Owner of the "enhanced due diligence measures" area for Group companies: Approval by the first-level manager</u> to commence or continue the ongoing relationship, subject to the opinion of Compliance & AFC.

illimity SGR	**Arec neprix**
Operations & Administration	Business Support *(with support from the reference manager)*
Head of UTP & Turnaround Funds *(for the iCCT, iREC and iRC Fund)* Head of NPL Small Medium Tickets Funds *(for the NPL Granular Fund)* Head of Private Capital Fund *(for the iSC Fund)*	Head of Loans Asset Management *(for NPL positions)* Head of UTP Corporate Asset Management *(for UTP positions)* Head of Leasing Asset Management *(for Leasing positions)*