FINANCIAL CRIME COMPLIANCE CORPORATE FRAMEWORK

JULY 2021

TABLE OF CONTENTS

1 INTRODUCTION

The purpose of the Financial Crime Compliance Corporate Framework ("the Framework") is to:

- Establish the principles that must be adhered to by entities of Santander Group (the "Group") in relation to the prevention of financial crime;
- Define the roles and responsibilities necessary for effective financial crime risk management;
- Identify the financial crime compliance (FCC) key processes to be developed and embedded within the entities of the Group in compliance with the Group policies and procedures that must be adopted locally; and
- Define the essential features of FCC governance at a Corporation and local level.

2 DEFINITIONS AND SCOPE

Santander Group is wholly committed to the fight against financial crime and shall not tolerate compliance failures with financial crime regulations both internationally and in the countries in which it operates.

2.1 Definitions

The following definitions are established for the purposes of this Framework to capture holistically the concept of "financial crime related risk" as managed at Corporation and across the entities of the Group:

- **Money laundering (ML):**
    - The conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in such activity to evade the legal consequences of his or her actions.
    - The concealment or disguise of the true nature, source, location, disposition, movement, beneficial ownership of property or rights, knowing that such property is derived from criminal activity or involvement in criminal activity.
    - The acquisition, possession or use of property, knowing, at the time of receipt, that such property is derived from criminal activity or from an act of participation in criminal activity.
    - Participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the actions mentioned in the foregoing points.
- **Terrorist financing (FT):** the provision, depositing, distribution or collection of funds or property, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, to carry out a terrorist offence.
- **Violation of international sanction programmes:** failure to comply with instruments of a political, diplomatic and economic nature used by international institutions and countries to exert influence in areas such as the prevention and pursuit of terrorism, support and defence of human rights and civil liberties, deterrence of possible armed conflicts or the prohibition of the development of weapons of mass destruction.

- **Bribery:** acts that give someone a financial or other advantage to encourage that person to perform his or her functions or activities improperly or to reward that person for having already done so. This could cover seeking to influence a decision-maker by giving some kind of extra benefit to that decision-maker rather than what can be legitimately offered.
- **Corruption:** acts taken by an individual in abusing their position of power or responsibility for their own personal gain.
- **Tax evasion:** the illegal non-payment or under-payment of taxes, usually resulting from the making of false or misleading declaration of facts or no declaration at all of income to the relevant tax authorities.
- **External fraud:** losses arising from any attempt at fraud, misappropriation of assets or breach of laws or regulations by a third party.

- **The FCC Programme** refers to the compliance programme designed by the FCC Corporate Function to ensure consistent management of financial crime related risks across Group entities. The Programme establishes and develops, via policies, procedures, protocols and associated guidance, the criteria, key processes, roles and responsibilities and governance associated with financial crime related risk, including: AML/CFT, sanctions compliance, ABC compliance, customer lifecycle due diligence (which incorporates controls to respond to priority criminal activity reportable under AML/CFT regulation, such as tax evasion and fraud), and the underlying risk and control strategy.

- **Obliged Entity** refers to a branch or majority-owned subsidiary of the Group or controlled by the Group that is an obliged entity in line with the EU directives related to the prevention of money laundering and countering the financing of terrorism.

2.2 Scope

The possibility of committing a crime represents both a reputational and regulatory compliance risk. In the context of this Framework, the principal risk resides in the exploitation and/or utilisation of the financial system, and as such, the possibility that Santander Group would give the appearance of legitimacy and legality to funds or assets with illicit origin and/or permit criminal activity to occur.

The failure to prevent financial crime can have a negative economic risk, real or perceived, and can erode confidence in the perception of the bank by its employees, clients, shareholders/investors and society in general. Not complying with FCC regulations can result in significant economic penalties including, in the extreme case, the loss of the banking license.

Financial crimes are universal, globalised phenomena that take advantage of the international economy, and thus their detection, deterrence and disruption call for a coordinated global response by the international community and the financial sector to prevent the sector from being used for illicit purposes.

Santander recognises the importance of the fight against financial crime as it affects essential aspects of social life. As such, this Framework covers all customers, operations and activities of the Group universally and without exception. This Framework must be read in conjunction with the *General Code of Conduct* and with all relevant Corporate frameworks, including the *Risk Corporate Framework* and the *Compliance & Conduct Corporate Framework*, as well as associated models, policies and procedures, particularly the FCC Corporate policies and procedures.

3 SCOPE OF APPLICATION AND IMPLEMENTATION BY SUBSIDIARIES

This framework:

• Is applicable throughout the whole Group on a mandatory basis and compliance with it must be evidenced.

• Shall be adopted by the Board of Directors of Subsidiaries subject to the Group Subsidiary Governance Model (GSGM). Any adaptation or waiver for any part of this Framework must be limited to those required by local law and regulation and submitted to the Corporation for consideration and approval.

• Shall be adhered to by all Subsidiaries within the Group with any adaptations being strictly limited to those required by local law and regulation.

• Includes reference to specific elements for its local implementation, all of which must be submitted to the Corporation for validation to ensure they are consistent with this Corporate Framework. These should also be subject to periodic review and updates.

4 PRINCIPLES

The following principles reflect the minimum expectations of the Corporation. They are obligatory to Group entities and must be applied at all times.

- **Zero tolerance** with respect to customers, suppliers, employees, contractors or other third parties, and all transactions, that could be related to financial crime, including the failure to comply with the requirements and principals established in this Framework.
- **The obligation within the organisation to prevent financial crime** by all employees, the executive leadership, and the members of governance forums and committees across the Group; the application of high ethical and conduct standards in the recruitment and conduct of directors, employees, agents, suppliers, intermediaries and introducers.
- **Corporate policies and procedures** to be adopted formally and applied across Group entities to ensure consistent implementation of minimum requirements and a robust and effective management of financial crime risk.
- **Risk-based approach to an effective financial crime compliance programme** to maximise the bank-wide effectiveness in the fight against financial crime by: (1) establishing requirements and designing controls based on their demonstrated ability to identify and mitigate the specific financial crimes risks faced by the Group; and (2) providing highly useful information on financial crime to relevant competent authorities on priority threat areas.
- **Information exchange** related to financial crime investigations among entities of the Group, in accordance with the applicable law, to detect, deter and disrupt transnational networks of criminal activity; the prompt reporting of suspicious operations and activity to internal governance bodies responsible for FCC and competent authorities; and absolute confidentiality and prohibition of disclosure of related analysis.

- **Personal data protection and record retention** of electronic and hard copy files related to FCC, protected by sufficient security measures that control data use, storage, dissemination, protection and access, in line with the relevant data protection policies in order to ensure the protection of data owners' rights, for a period of at least 6 years or that which is established by local regulation.
- **An adequate organisational structure** in the Corporation and the entities within the Group that ensures sufficient staffing, training, resources, technology and procedures, as necessary to comply with the internal requirements of FCC.

5 ROLES AND RESPONSIBILITIES

The roles and responsibilities for effective financial crime risk management must respect the three lines of defence model and the need to achieve collaboration among the Group, Santander entities and the functions. All employees have the responsibility to comply with this Framework and the associated policies and procedures, and to escalate any indications of financial crime.

Entities within the Group must have an appropriate organisational and governance structure to detect, deter and disrupt financial crime, report in line with the requirements established in law, and block or freeze funds or economic resources following the application of controls of sanctions or international financial countermeasures.

- **The Business – the First Line of Defence:**

The business functions and all other functions that generate exposure to risk constitute the first line of defence. Risk generation must be aligned with the approved risk appetite and the associated limits. The head of each unit generating a risk has the primary responsibility for managing this risk and to support and promote the organisation's risk culture.

For **Santander obliged entities**, the **Santander Obliged Entity Accountable Executive** for FCC ensures that this Framework and the underlying FCC Programme are embraced by the Business and implemented and executed effectively. If necessary, **Business Line Accountable Executives** may be identified to make related operational decisions to their own business line/unit.

- **Financial Crime Compliance – the Second Line of Defence:**

Within the Compliance & Conduct Function, the FCC Corporate Function, in coordination with other functions from the second line of defence, such as Non-Financial Risk and Regulatory Compliance, must:

- Define the criteria for considering an entity of the Group an obliged entity.
- Independently supervise and question the risk management activities carried out by the first line of defense.
- Propose, with the collaboration of the first line of defense functions:
    - FCC's risk appetite to the Board for approval; and
    - Risk thresholds in accordance with FCC's risk appetite for approval by the Board.
- Define metrics to be used in risk measurement, and review and challenge risk appetite and lower-level limit proposals.

- Review the risk appetite of each subsidiary to ensure it is consistent with the Group's risk appetite and strategy, prior to the subsidiary submitting the risk appetite to the local Board for approval.
- Check that adequate policies and procedures have been implemented to manage the business within the risk appetite level.
- Ensure that risks are managed in accordance with the financial crime risk appetite defined by the Board.
- Promote and adopt a strong culture of risk throughout the organization.
- Report, when necessary, the FCC risks outside of risk appetite, to the relevant governing bodies.

The role of the FCC Function is limited to the prevention of financial crime and the management of financial crime risk – while such a focus may result in decreased fraud loss, or minimising reputational risk, those objectives are beyond the responsibilities of the FCC Function (and the FCC Programme) and are addressed explicitly in the internal regulation to which those concerns pertain.

As a function within the second line of defence, the FCC Function is responsible for monitoring and overseeing financial crime risks, assessing the impact on risk appetite and the risk profile of the entity and taking account of the provisions of this Framework. The Corporation must have a designated **Corporate Head of FCC**, responsible for implementing this Framework, the FCC Programme, and associated policies and procedures across the Group. The Corporate Head of FCC will determine those policies and procedures that require Corporate validation of local transposition in the Santander entities.

For **Santander obliged entities**, each entity must have a designated **Local Head of FCC**, responsible for the application of this Framework and its implementation in their geography. The **Local Head of FCC** is responsible for dialogue with local supervisors on matters of FCC; if applicable, the **Local Head of FCC** will coordinate engagement on FCC supervisory issues with the function formally assigned to manage relations with regulators and supervisors.

Group entities may appoint an individual responsible for FCC (second line of defence) in the specific business areas, which operate under the coordination and dependency of the Local FCC function (and not as a substitute for the Local Head of FCC).

The Compliance & Conduct Function, led by the Chief Compliance Officer, is responsible for the control and supervision of the Corporate Defense model and to comply with the reporting duties to the governance bodies in this regard consolidating and/or considering, as appropriate, the information provided by the FCC Function.

Within the Risk Function, the Non-Financial Risk Function is responsible for consolidating all operational risks, including those arising from compliance and conduct risks, into the broader non-financial risk to present a holistic view of risks of this type to which the entity or the Group is exposed, assessing the impact on risk appetite and the risk profile. Additionally the Non-Financial Risk Function is responsible for the overarching oversight of all operational risks, including oversight of consolidated events, losses, the risk and control self-assessment (RCSA), operational risk indicators (ORIs), scenarios, operational risk capital and losses regulatory reporting. Conduct & Regulatory and Financial Crime have their own Risk Type Framework but are subject to the Non-Financial Risks toolsets and processes.

- **Internal Audit – the Third Line of Defence:**

The third line of defence, the Internal Audit Function, regularly assesses that policies, methodologies and procedures are adequate and effectively implemented for the management and control of the FCC system.

6 KEY PROCESSES

The entities of the Group must have effective internal regulation in place enabling them to demonstrate that the FCC activities and related processes are properly executed and in line with (1) applicable local laws and regulations and (2) the Corporate level policies and procedures, which reflect the laws and regulations of the European Union.

Specifically, Group entities must have policies and procedures in place to respond to the risks of money laundering and terrorist finance, sanctions violations, and to the risk that the Santander entity facilitates or is utilised for criminal activity, specifically bribery, corruption, external fraud, tax crimes, and any other criminal activity assessed by the FCC Corporate Function as representing a significant financial crime threat to the Group.

Internal regulations drafted by the Santander entities in response to FCC Corporate policies and procedures, which capture the distinct components of the FCC Programme, as detailed below, must be validated by the FCC Corporate Function prior to local relevant body approval.

The Corporation may also issue additional guidelines or protocols for its subsidiaries to facilitate the proper interpretation, implementation and consistent application of internal policies and procedures within the Group.

The programmes defined below collectively capture the key processes and related activities and controls that constitute the overall FCC Programme, implemented by the FCC Corporate and Local Functions and embraced and executed by the Business. These programmes must be complied with by Santander entities to ensure adequate management and control of financial crime related risks, and that Group-wide compliance is appropriately focused on the activities and jurisdictions in which it operates.

6.1 Anti-money laundering and countering the financing of terrorism programme

- **Due diligence:** an explicit customer identification programme that captures on-going due diligence on all customers over the course of their relationship with the Group ("the customer lifecycle"), from onboarding to exit. See *6.4 FCC Customer Lifecycle Due Diligence Programme* for further detail.
- **Reporting obligations:** both the sharing of information between FCC functions in order to be effective in investigating financial crime as well as the exchange of the information with the relevant competent authorities, treated with the maximum level of confidentiality, in line with the relevant data protection policies and in compliance with local regulations, in order to ensure the protection of data owners' rights. Full cooperation with the competent authorities as it regards financial crime prevention.
- **Internal control:** a clear approach for understanding the inherent ML/FT risk within a Santander entity, how to evaluate the effectiveness of the controls that respond to that risk, and the method for ensuring the Group's understanding of risk drives strategic decision-making and the application of resources. See *6.5 FCC Risk and Control Programme* for further detail.

6.2 Sanctions compliance programme

- **Mandatory sanctions programmes:** the recognition and compliance with sanctions and financial countermeasure programmes, maintaining as minimum requirements the international sanctions programmes established by the United Nations (UN), the European Union (EU), the United Kingdom (UK), and the United States (US) that could affect the activities of the Group.
- **Sanctioned individuals and entities:** ensuring no relationships are established or maintained or business activity facilitated with sanctions targets.
- **Sanctioned countries and territories:** the definition of prohibited, highly restricted and restricted countries and territories subject to sanctions.
- **Restricted goods and merchandise:** not engaging in or facilitating payments/transactions or business activity related to restricted goods and merchandise without verifying that the underlying activity is lawful.
- **Sanctions compliance clauses:** including sanctions clauses in all account opening, trade contracts and other transaction agreements to ensure compliance with this Framework and associated policies and procedures.
- **Sanctions screening programme:** the implementation of a tailored programme that includes, as applicable, customer (including related party), counterparty, supplier, employee and payment/transaction screening (including securities transactions), which may be manual and/or automated according to risk.
- **Trade finance:** appropriate counterparty and transaction due diligence before entering into any trade finance operation or processing any related payments, in order to mitigate the risk of violating any applicable international sanctions programmes and/or restricted goods and merchandise regulations.

6.3 Anti-bribery and corruption (ABC) programme

- **Third parties:** establishing control and prevention measures regarding third parties (suppliers, agents, intermediaries, contractors, introducers, advisors and business partners) with whom the Group operates, including due diligence, procurement processes, ABC clauses and payment and accounting controls.
- **Sponsorships:** clear requirements that specify the criteria for the approval of, or limitations on, sponsorships.
- **Charitable contributions:** controls that include restrictions/limitations on giving, identification of high-risk activities, due diligence regarding the recipient organisation, and recordkeeping.
- **Political contributions:** established requirements that take local laws into account and implement controls to mitigate risks related to public officials.
- **New business opportunities including joint ventures and principal investments:** ABC-specific due diligence on new business opportunities, principal investments and joint ventures, with the establishment of contractual clauses related to ABC and risk-based post-acquisition oversight.

- **Third party payments:** controls to address the risk of the Group's third party payment methods being used to fund bribes and corrupt activity, including limiting the use of urgent and manual payments and cash and the prohibition of facilitation payments.
- **Travel, gifts & hospitality, and marketing activities and events:** addressing the provision and receipt of gifts and business hospitality, including monetary thresholds for approval and record keeping.
- **Employment and work experience:** the establishment of requirements to ensure a consistent recruitment process, merit-based hiring procedures, and a review of candidates and compensation arrangements to ensure their suitability and the adequacy of their assigned functions, in line with the regulation on conduct and controls to prevent corruption.

6.4 Customer lifecycle due diligence programme

- **Customer due diligence – know your customer:** customer identification and verification, customer risk assessment and subsequent risk-based due diligence, screening, and risk-based on-going monitoring of the business relationship via manual and/or automated means.
- **Anti-impersonation controls:** to respond to identity fraud risk at on-boarding and during the lifecycle of the customer's relationship with the bank, using biometrics, device-related technical controls, and authentication measures, especially for non-face-to-face channels.
- **Transfer of funds:** compliance with payment (message) completeness and transparency requirements in both domestic and international payments.
- **Prohibited, restricted and special customer types:** the identification of customer types and/or activities that are prohibited or subject to specialised controls due to elevated financial crime risk. Includes politically exposed persons and diplomatic missions, as well as sectors/industries with established elevated exposure to criminal activities, including environmental crime, trafficking in human beings, sexual exploitation/child abuse, and any other criminal activity assessed to represent a significant threat to the Group.
- **Elevated risk products and activities:** the identification and implementation of tailored controls to respond to business lines within Santander Group that are recognised for their elevated financial crime risk, and thus require special attention and management, such as correspondent relationships, private banking, and activities associated with crypto-assets and innovative digital methods.
- **Alerts, analysis and reporting of suspicious transactions, and the termination of relations:** the prompt identification, investigation, in-depth analysis (if necessary) and communication of suspicious activity. The closure or termination of business relations with customers due to financial crime compliance issues.

6.5 FCC risk and control programme

- **Risk assessment and control effectiveness:** the management of the FCC risk and control self-assessment (FCC-RCSA), the Country Risk Matrix, and the assessment and approval of new products.
- **Oversight:** supervision of the implementation and embedding of the FCC Corporate policies and procedures, model validation, technical and quality assurance, the escalation of key events and the reporting of key risk indicators (KRIs), a process for tracking local Santander entity

exceptions to Corporate FCC policies and procedures, and an anonymous whistleblowing channel that allows employees of the Group to report FCC misconduct without fear of reprisal.

- **Corporate development transactions:** the evaluation of financial crime risks associated with corporate development transactions, including pre-acquisition due diligence and post-acquisition integration into the requirements as outlined by this Framework and accompanying policies and procedures.
- **Application of due diligence measures by third parties:** the recognition that the due diligence requirements as described in this Framework and accompanying policies and procedures must apply equally in the case of using or relying upon third parties, via expressed agreements and the establishment of the necessary controls.
- **Training:** the embrace of the measures necessary to ensure that all employees receive permanent training on the core aspects of regulation regarding FCC.
- **Record keeping:** data and documentation retention to maintain an accurate and accessible archive of relevant and required FCC information.

7 GOVERNANCE

The Governance applied in the Group must promote efficient structures that ensure adequate participation by all relevant functions. Governance must also be compatible with the functions at a local level, with coordinated management and oversight at the Corporate level.

The governance bodies for the Group's subsidiaries must be structured according to local regulatory and legal requirements, as well as the size and complexity of each subsidiary, whilst ensuring that they are consistent with those of the parent company. Such governance bodies must promote clear and effective decision-making and clarity in accountability.

Carrying out the FCC function properly in terms of decision-making, supervision and control requires a governance structure that can provide a response in an efficient and agile manner both at a corporate and subsidiary level.

The Board of Banco Santander, S.A. and its committees, in accordance with the provisions of its bylaws and Board regulations, are the most senior decision-making and monitoring bodies in connection with the management and control of preventing financial crime, except in the case of issues reserved for the general meeting.

The Boards of subsidiaries are also the most senior bodies at their level.

The Boards of each entity and of the Group are responsible for the:

- Adoption of Corporate frameworks and applicable Corporate policies and procedures.
- Supervision of compliance with FCC regulations and legislation, including any actions and measures as a result of inspections by supervisory and control authorities, in addition to internal control and assurance functions.

The risk supervision body (Board Risk Committee) is responsible for:

- Assisting and advising the Board in the definitions and assessment of the policies stipulated in this Framework.

- Assisting the Board with supervision of the application and analysis of the defined risk profile.
- Monitoring and assessing any regulatory proposals and new applicable regulations, and the potential consequences for the Group.

In its application of this framework, Group entities shall identify the executive governance bodies or committees responsible for defining, monitoring, controlling and overseeing FCC regulatory risks. For Santander obliged entities, such bodies must include senior management representatives from the different business areas, and address at a minimum the following responsibilities with respect to the effectiveness of the FCC Programme:

- The designation of the Santander Obliged Entity Accountable Executive and, as applicable, the Business Line Accountable Executives;
- Awareness of the results of the FCC-RCSA, any associated plans to improve the maturity of the control environment, and the monitoring of those plans;
- Awareness of the evaluations from the FCC Corporate Oversight function, according to the FCC Corporate Oversight Methodology;
- Awareness of the results of technical and/or quality assurance testing on key FCC controls;
- The escalation of locally proposed new products that include significant financial crime related risk;
- The escalation and management of FCC risk events to the FCC;
- Monitoring of the FCC KRIs;
- Monitoring of service level performance metrics and general oversight on the outsourcing or insourcing of any FCC controls;
- Approval of the annual training programme and tracking performance results; and
- Acknowledgement of waivers and/or temporary dispensations from FCC Corporate policies or procedures.

The audit body (Board Audit Committee) is responsible for:

- Oversight of the effectiveness of the internal control systems, by reviewing them periodically, in order to identify, manage and resolve adequately the principal risks.

8 OWNERSHIP, INTERPRETATION, VALIDITY DATE AND PERIODIC REVIEW

- This document must be approved by the Board of Banco Santander S.A.
- The General Compliance Committee is responsible for the interpretation of this Framework.
- This Framework will come into effect on the date of its publication.
- Its contents will be reviewed periodically, and any changes or modifications will be made as appropriate.

9 VERSION CONTROL

Document Version	Responsible for Maintenance	Approval	
		Committee	Date
2019	FCC Policies & Framework	Board of Directors	Dec 2019
2020	FCC Policies & Framework	Board of Directors	Jul 2020
2021	FCC Policies & Framework	Board of Directors	July 2021

Document Version	Comments
2019	Updated to reflect new concept of "FCC"
2020	Updated to reflect an improved definition of the First Line of Defence and clarify reference to Second Line of Defence
2021	Updated to reflect the expanded definition of FCC (including reference to priority criminal activity – bribery, corruption, external fraud specific to anti-impersonation controls, and tax crimes) and associated key processes; inclusion of Group-mandated FCC accountable executives in the first line of defence, and related governance.

APPENDIX: DEFINITION OF TERMS

Santander Group or the Group: group of companies comprising Banco Santander, S.A. as the parent company, and the dependent companies over which it has direct or indirect control. For clarification, it comprises the Banco Santander, S.A. parent company, including the Santander Spain organisational units, which are part of said company, and any other unit/subsidiaries of Banco Santander S.A.

Corporation: all the governing bodies, organisational structures and employees entrusted by Banco Santander, S.A. to exercise oversight and control across the entire Group, including those functions typically associated with the relationship between a parent company and its subsidiaries.

Subsidiary: a dependent company that forms part of the Santander Group or one directly or indirectly controlled by Banco Santander, S.A.

Governing Body: Governance Body or group of bodies of a company that are responsible for the supervision and management of the business at the highest level.

Senior management: individuals who exercise executive functions in the entity and who are responsible for the daily management of the entity, and who are accountable to the Governing Body.