SUPPLEMENT DATED 9 AUGUST 2024 TO THE BASE PROSPECTUS DATED 13 MARCH 2024

BANCO SANTANDER, S.A.

(incorporated with limited liability in Spain)

PROGRAMME FOR THE ISSUANCE OF DEBT INSTRUMENTS

This first supplement (the "**Supplement**") is supplemental to, forms part of and must be read and construed in conjunction with the base prospectus dated 13 March 2024 (the "**Base Prospectus**"), in each case, prepared by Banco Santander, S.A. ("**Santander**", "**Banco Santander**", the "**Issuer**" or the "**Bank**") in connection with its programme (the "**Programme**") for the issuance of debt instruments (the "**Instruments**"). Terms given a defined meaning in the Base Prospectus shall, unless the context otherwise requires, have the same meaning when used in this Supplement.

This Supplement constitutes a supplement to the Base Prospectus for the purposes of Article 23 of Regulation (EU) 2017/1129 of the European Parliament and of the Council of the EU of 14 June 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market, and repealing Directive 2003/71/EC (as amended, the "**Prospectus Regulation**") and has been approved by the Central Bank of Ireland as competent authority for the purpose of the Prospectus Regulation. The Central Bank of Ireland only approves this Supplement as meeting the standards of completeness, comprehensibility and consistency imposed under Irish and European Union ("**EU**") law pursuant to the Prospectus Regulation. Such approval by the Central Bank of Ireland should not be considered as an endorsement of the Issuer or the quality of the securities that are the subject of this Supplement. Investors should make their own assessment as to the suitability of investing in the securities that are the subject of this Supplement.

This Supplement has been prepared for the purposes of (i) updating certain risk factors in respect of the Issuer to disclose the latest developments in the legal proceedings of the Group, the data breach occurred in May and the changes in the ratings assigned to the Group by the major rating agencies and (ii) incorporating by reference the June 2024 Financial Statements and the 2024 January-June Financial Report (both terms as defined below).

IMPORTANT NOTICES

The Issuer accepts responsibility for the information contained in this Supplement and declares that, to the best of its knowledge, the information contained in this Supplement is in accordance with the facts and contains no omission likely to affect its import.

To the extent that there is any inconsistency between (a) any statement in this Supplement or any statement incorporated by reference into the Base Prospectus by this Supplement and (b) any other statement in, or incorporated by reference into, the Base Prospectus, the statements in (a) above will prevail.

Save as disclosed in this Supplement, no significant new fact, material mistake or inaccuracy relating to information included in the Base Prospectus which is capable of affecting the assessment of the Instruments issued under the Programme has arisen or been noted, as the case may be, since the publication of the Base Prospectus.

AMENDMENTS OR ADDITIONS TO THE BASE PROSPECTUS

With effect from the date of this Supplement the information appearing in, or incorporated by reference into, the Base Prospectus shall be amended and/or supplemented in the manner described below.

RISK FACTORS

The following risk factor shall replace in its entirety the risk factor "The Group is exposed to risk of loss from legal and regulatory proceedings" in the sub-section of the Base Prospectus entitled "Risk Factors—2. Risks Relating to the Issuer and the Group Business":

*"**The Group is exposed to risk of loss from legal and regulatory proceedings.***

The Group faces risk of loss from legal and regulatory proceedings, including tax proceedings, that could subject it to monetary judgements, regulatory enforcement actions, fines and penalties. The current regulatory and tax enforcement environment in the jurisdictions in which the Group operates reflects an increased supervisory focus on enforcement, combined with uncertainty about the evolution of the regulatory regime, and may lead to material operational and compliance costs.

The Group is from time to time subject to regulatory investigations and civil and tax claims, and party to certain legal proceedings incidental to the normal course of its business, including, among others, in connection with conflicts of interest, lending and derivatives activities, relationships with its employees and other commercial, data protection or tax matters. In view of the inherent difficulty of predicting the outcome of legal matters, particularly where the claimants seek very large or indeterminate damages, or where the cases present novel legal theories, involve a large number of parties or are in the early stages of investigation or discovery, the Group cannot state with certainty what the eventual outcome of these pending matters will be or what the eventual loss, fines or penalties related to each pending matter may be.

The amount of the Group's reserves in respect of these matters, which considers the likelihood of future cash outflows associated with each of such claims, is substantially less than the total amount of the claims asserted against it, and, in light of the uncertainties involved in such claims and proceedings, there is no assurance that the ultimate resolution of these matters will not significantly exceed the reserves currently accrued by the Group. As a result, the outcome of a particular matter may be material to its operating results for a particular period. As of 31 December 2023, the Group had provisions for taxes, other legal contingencies and other provisions for €4,634 million (€4,873 million as of 30 June 2024).

For example, in Poland the Group is exposed to significant litigation in connection with CHF indexed and CHF denominated loans in which it is facing claims that those loans or clauses included in them are abusive. Whilst the Court of Justice of the European Union ("CJEU") and the Polish Supreme Court have issued several rulings on this matter (including the CJEU ruling of 15 June 2023), sufficient case law has not yet been developed. The case law of the Polish national courts implementing the CJEU rulings (including the ruling of 15 June 2023) and the possible position of the Polish Supreme Court will be crucial for the final assessment of the legal risk related to this matter. On 25 April 2024, the Supreme Court issued a resolution on CHF loans, in which it considered contract invalidation to be the primary consequence of finding abusive contractual clauses. At the same time, nine judges of the Supreme Court declined to participate in the resolution raising questions of a constitutional nature and six judges submitted dissenting opinions mainly on issues related to the maintenance of the agreement after the elimination of abusive clauses. The full text of the resolution has not yet been released.

As of the date of this Base Prospectus, it is not possible to predict the Polish Supreme Court's and CJEU's decisions on individual cases. As of 31 December 2023, Santander Bank Polska S.A. and Santander Consumer Bank S.A. maintained a portfolio of mortgages denominated in or indexed to CHF for an approximate gross amount of zł6,398.1 million or €1,473.1 million (zł5,739.4 million or €1,332.2 million as of 30 June 2024) and the total value of the adjustments to gross carrying amount in accordance with IFRS9 as well as the provisions recorded under IAS37, amount to zł5,030.3 million or €1,158.2 million (€5,815.2 million or zł1,349.8 million as of 30 June 2024). The provisions and adjustments recorded are deemed sufficient to cover the risks associated with the legal claims against the Group. However, in the event that the Group is required to make higher payments than estimated, either with respect to existing or new claims, there could be a significant adverse effect on its results and financial situation."

The following risk factor shall replace in its entirety the risk factor "Any failure or disruption of the Group's operational processes or systems, or data breaches and other security incidents with respect to the Group or its third-party vendors' systems could adversely affect the Group's business or reputation, and create significant legal, regulatory or financial exposure" in the sub-section of the Base Prospectus entitled "Risk Factors—2. Risks Relating to the Issuer and the Group Business":

"Any failure or disruption of the Group's operational processes or systems, or data breaches and other security incidents with respect to the Group or its third-party vendors' systems could adversely affect the Group's business or reputation, and create significant legal, regulatory or financial exposure.

Like other financial institutions, in conducting the Group's banking operations, the Group receives, manages, holds, transmits and otherwise processes certain proprietary and sensitive or confidential information, including personal information of customers and employees as well as a large number of assets. Accordingly, the business of the Group relies on its ability to process a large number of transactions efficiently and accurately, and on its ability to rely on its digital technologies, computer and email services, software and networks, as well as on the secure storage, transmission and otherwise processing of proprietary confidential, sensitive and personal data and other information using the computer systems and networks of the Group or those of its third party vendors. The Group's operations must also comply with complex and evolving laws and regulations in the countries in which the Group operates. The proper and secure functioning of its financial controls, accounting and other data collection and processing systems is critical to its business and to its ability to compete effectively. Data breaches, data losses and other security incidents, including fraudulent withdrawal of money, can result from, among other things, inadequate personnel, inadequate or failed internal control processes and systems, or external events or actors that interrupt normal business operations and may include cyberattacks, disruptions, failures, unauthorised access or misuse, software bugs, server malfunctions, software and hardware failure, malware and ransomware, social engineering and phishing attacks, denial-of-service attacks, misconduct, fraud, and other events that could have a serious impact on the Group. The Group also faces the risk that the design of its or its third-party vendors' cybersecurity controls and procedures prove to be inadequate or are circumvented such that its data or client records are incomplete, not recoverable or not securely stored. Moreover, it is not always possible to deter or prevent employee errors or misconduct, and the precautions the Group takes to detect and prevent this activity may not always be effective. Any material disruption or slowdown of the systems of the Group could cause information, including data related to customer requests, to be lost or to be delivered to its clients with delays or errors, which could reduce demand for its services and products, produce customer claims and materially and adversely affect the Group.

The Group prioritises early identification, monitoring and mitigation of risks (including those resulting from its interactions with third parties) in its goal to provide a resilient and secure operational environment. In this regard, although (i) the Group has policies, procedures and controls in place designed to safeguard proprietary sensitive and confidential information, including personal information, (ii) the Group takes protective technical measures and monitor and develop the Group's systems and networks to protect the Group's technology infrastructure, data and information from misappropriation or corruption, and (iii) the Group works with its clients, vendors, service providers, counterparties and other third parties to develop secure data and information processing, collection, authentication, management, usage, storage and transmission capabilities and to ensure the eventual destruction of proprietary, sensitive and confidential information, including personal information, the Group, its third-party vendors or other third parties with which the Group does business have been and may continue to be subject to cyberattacks and other cybersecurity incidents. For example, on 14 May 2024, the Group announced that it had become aware of an unauthorized access to a Santander database that included certain customer and employee information hosted by a third-party provider (the "**2024 Unauthorized Access**"). For more information on the legal and regulatory risks arising from the data privacy and cybersecurity laws and regulations the Group is subject to, which, among other things, impose certain obligations with respect to cyberattacks, data breaches, data losses, and other cybersecurity incidents, see risk factor *"The Group is subject to extensive regulation and regulatory and governmental oversight which could adversely affect its business, operations and financial condition"*.

The implementation of the Group's cybersecurity policies, procedures, controls and technical measures is designed to reduce the risk of such cybersecurity incidents but does not guarantee full protection against potential threats or cyberattacks or a risk-free environment. This is especially applicable in the current global environment, with the war in Ukraine and the conflict in the Middle East resulting in an increased risk of cyberattacks, and other disruptions in response to, or retaliation for, the sanctions and costs imposed on Russia and certain other countries directly or indirectly involved in the wars. Additionally, the shift to remote work

policies for a significant portion of the Group's workforce, as they access the Group's secure systems and networks remotely and its customers' increased reliance on digital banking products and other digital services, including mobile payment products, has also increased the risk of cyberattacks (see *"The global covid-19 pandemic materially impacted the Group's business, and the continuance of this pandemic or any future outbreak of any other highly contagious diseases or other public health emergencies, could materially and adversely impact its business, financial condition, liquidity and results of operations*).

While the Group generally performs cybersecurity due diligence on its key vendors, because it does not control its vendors and its ability to monitor their cybersecurity is limited, the Group cannot ensure the cybersecurity measures they take will be sufficient to protect any information it shares with them. Due to applicable laws and regulations or contractual obligations, the Group may be held responsible for security breaches, cyberattacks or other similar incidents attributed to its vendors as they relate to the information the Group share with them.

In addition, the Group may also be impacted by cyberattacks against national critical infrastructures of the countries where it operates, such as telecommunications networks. The Group's information technology systems are dependent on such critical infrastructure and any cyberattack against such critical infrastructure could negatively affect its ability to service its customers. As the Group does not operate such critical infrastructure, it has limited ability to protect its information technology systems from the adverse effects of a cyberattack.

The Group has seen in recent years the information technology systems and networks of companies and organisations being increasingly targeted, and the techniques used to obtain unauthorised, improper or illegal access to such information technology systems and networks have become increasingly complex and sophisticated, including through the use of AI. Furthermore, such techniques change frequently and are often not recognised or detected until after they have been launched and can originate from a wide variety of sources, including not only organised crime, hackers, activists, terrorists, nation-states, nation-state supported actors and others, any of which may see their effectiveness enhanced by the use of AI. As attempted attacks continue to evolve in scope and sophistication, the Group may incur significant costs in order to modify or enhance its protective measures against such attacks, or to investigate or remediate any vulnerability or resulting breach, or in communicating cyberattacks or other security incidents to its customers, affected individuals or regulators, as applicable.

If the Group cannot maintain effective and secure proprietary, confidential, sensitive and personal data, or if the Group or its third-party vendors fall victim to successful cyberattacks, penetrations, compromises, breaches or circumventions of the Group's information technology systems or networks, such as the 2024 Unauthorised Access, or experience other security incidents in the future, the Group may incur substantial costs and suffer other negative consequences, such as disruption to its operations, misappropriation of personal, proprietary, confidential or sensitive information, remediation costs (including liabilities for stolen assets or information, repairs of system damage, among others), increased cybersecurity protection costs, lost revenues arising from the unauthorised use of personal, proprietary, confidential or sensitive information or the failure to retain or attract its customers following an operational or security incident, litigation and legal risks (including claims from customers, employees or other third parties, regulatory action, reporting obligations, investigation, fines and penalties), increased insurance premiums, reputational damage affecting its customers' and the investors' confidence, as well as damages to the Group's competitiveness, stock price and long-term shareholder value. In addition, the Group's remediation efforts may not be successful, and it may not have adequate insurance to cover these losses. While the Group maintains insurance coverage, it cannot assure that such coverage will be adequate or otherwise protect the Group from liabilities or damages with respect to claims alleging compromises of proprietary, confidential, sensitive or personal data or otherwise relating to data privacy and cybersecurity matters. In addition, the Group cannot be sure that its existing insurance coverage will continue to be available on acceptable terms or at all, or that its insurers will not deny coverage to any future claim. Moreover, even when a failure of or interruption in the Group's or its third-party vendors' systems or facilities is resolved in a timely manner or an attempted cyberattack, data breach or security incident is successfully avoided or thwarted, substantial resources and management attention are expended in doing so, and to successfully avoid or resolve any such incidents, the Group may be required to take actions that could adversely affect customer satisfaction or retention, as well as harm its reputation.

Any of the cyberattacks, data breaches, data losses and other security incidents described above could have a material adverse effect on the Group's business, financial condition and results of operations."

The following risk factor shall replace in its entirety the risk factor "Credit, market and liquidity risk may have an adverse effect on the credit ratings of the Group and its cost of funds. Any downgrade in the credit rating of the Group would likely increase its cost of funding, require the Group to post additional collateral or take other actions under some of its derivative and other contracts and adversely affect its interest margins and results of operations." in the sub-section of the Base Prospectus entitled "Risk Factors—2. Risks Relating to the Issuer and the Group Business":

"Credit, market and liquidity risk may have an adverse effect on the credit ratings of the Group and its cost of funds. Any downgrade in the credit rating of the Group would likely increase its cost of funding, require the Group to post additional collateral or take other actions under some of its derivative and other contracts and adversely affect its interest margins and results of operations.

Credit ratings affect the cost and other terms upon which the Group is able to obtain funding. Rating agencies regularly evaluate the Group, and their ratings of its debt are based on a number of factors, including its financial strength and conditions affecting the financial services industry. In addition, due to the methodology of the main rating agencies, the credit rating of the Group is affected by the rating of Spanish sovereign debt. If Spain's sovereign debt is downgraded, the credit rating of the Group would also likely be downgraded.

Any downgrade in the Group's debt credit ratings would likely increase its borrowing costs and require the Group to post additional collateral or take other actions under some of its derivative and other contracts, and could limit the Group's access to capital markets and adversely affect its commercial business. For example, a ratings downgrade could adversely affect the ability of the Group to sell or market some of its products, engage in certain longer-term and derivatives transactions and retain the Group's customers, particularly customers who need a minimum rating threshold in order to invest. In addition, under the terms of certain of the derivative contracts and other financial commitments of the Group, the Group may be required to maintain a minimum credit rating or terminate such contracts or require the posting of collateral. Any of these results of a ratings downgrade could reduce the liquidity of the Group and have an adverse effect on it, including on its operating results and financial condition.

The Group has the following ratings by the major rating agencies as of the report dates indicated below:

Rating agency	Long term	Short term	Last report date	Outlook
Banco Santander, S.A.				
Fitch Ratings (1)	A- (Senior A)	F2 (Senior F1)	March 2024	Stable
Moody's (2)	A2	P-1	April 2024	Positive
Standard & Poor's (3)	A+	A-1	April 2024	Stable
DBRS (4)	A (High)	R-1 (Medium)	September 2023	Stable
Santander UK plc				
Fitch Ratings (1)	A+	F1	May 2024	Stable
Moody's (2)	A1	P-1	February 2024	Stable
Standard & Poor's (3)	A	A-1	June 2023	Stable
Banco Santander (Brasil), S.A.				
Moody's (2)	Ba1	-	May 2024	Positive
Standard & Poor's (3)	BB-	B	December 2023	Stable

(1) Fitch Ratings Ireland Limited (Fitch Ratings).
(2) Moody's Investor Service Spain, S.A. (Moody's).
(3) S&P Global Ratings Europe Limited (Standard & Poor's).
(4) DBRS Ratings Limited (DBRS).

The Group conducts substantially all of its material derivative activities through Banco Santander and Santander UK. The Group estimates that as of 31 December 2023, if all the rating agencies were to downgrade Banco Santander's long-term senior debt ratings by one notch the Group would be required to post up to €210 million in additional collateral pursuant to derivative and other financial contracts. A hypothetical two-notch downgrade would result in a further requirement to post up to €178 million in additional collateral. The Group estimates that as of 31 December 2023, if all the rating agencies were to downgrade Santander UK's long-term credit ratings by one notch, and thereby trigger a short-term credit rating downgrade, this could result in contractual outflows from Santander UK's total liquid assets of £1.2 billion (equivalent to €1.4 billion) of cash and additional collateral that Santander UK would be required to post under the terms of secured funding and derivatives contracts. A hypothetical two-notch downgrade would result in a further outflow of £0.8 billion (equivalent to €0.9 billion) of cash and collateral under secured funding and derivatives contracts.

While certain potential impacts of these downgrades are contractual and quantifiable, the full consequences of a credit rating downgrade are inherently uncertain, as they depend on numerous dynamic, complex and inter-related factors and assumptions, including market conditions at the time of any downgrade, whether any downgrade of the Group's long-term credit rating precipitates downgrades to its short-term credit rating, and assumptions about the potential behaviours of various customers, investors and counterparties. Actual outflows could be higher or lower than the preceding hypothetical examples, depending upon certain factors including which credit rating agency downgrades the credit rating of the Group, any management or restructuring actions that could be taken to reduce cash outflows and the potential liquidity impact from loss of unsecured funding (such as from money market funds) or loss of secured funding capacity. Although unsecured and secured funding stresses are included in the stress testing scenarios of the Group and a portion of its total liquid assets is held against these risks, a credit rating downgrade could still have a material adverse effect on the Group.

In addition, if the Group were required to cancel its derivatives contracts with certain counterparties and were unable to replace such contracts, the market risk profile of the Group could be altered.

There can be no assurance that the rating agencies will maintain the current ratings or outlooks. In general, the future evolution of the Group's ratings is linked, to a large extent, to the general macroeconomic outlook which includes the impact of the continuance or escalation of the war in Ukraine and of the conflict in the Middle East on the asset quality, profitability and capital of the Group. Failure to maintain favourable ratings and outlooks could increase the cost of funding of the Group and adversely affect interest margins, which could have a material adverse effect on the Group."

DESCRIPTION OF THE ISSUER

The following text shall replace in its entirety the text in the section entitled "Description of the Issuer" on page 68 of the Base Prospectus:

"The description of the Issuer is set out in certain sections of the 2023 Annual Report and the 2024 January-June Financial Report. These sections have been incorporated by reference into this Base Prospectus (see "*Documents Incorporated by Reference*", which provides tables reconciling the content of this section with the corresponding page numbers of each of the 2023 Annual Report and the 2024 January-June Financial Report containing such information)."

DOCUMENTS INCORPORATED BY REFERENCE

The information set out below shall supplement the section of the Base Prospectus entitled "Documents Incorporated by Reference" on pages 69 to 70 of the Base Prospectus:

The following documents shall be deemed to be incorporated by reference in and to form part of, the Base Prospectus and will be published on the website of Banco Santander (www.santander.com):

1. The English language translation of the audited interim condensed consolidated financial statements of the Issuer prepared under IFRS-EU for the six-month period ended 30 June 2024, together with the relevant Independent Auditor's Report (the "**June 2024 Financial Statements**").

   https://www.santander.com/content/dam/santander-com/en/documentos/informacion-publica-periodica-c-n-m-v-/2024/cnmv-2024-informe-financiero-semestral-1s-2024-en.pdf

2. The financial report of the Issuer prepared for the six-month period ended 30 June 2024 (the "**2024 January-June Financial Report**")

   https://www.santander.com/content/dam/santander-com/en/documentos/resultados-trimestrales/2024/2q/rt-q2-2024-banco-santander-financial-report-en.pdf

In relation to the June 2024 Financial Statements and the 2024 January-June Financial Report, any information not specified in the cross-reference tables set out below but which is included in the documents from which the information incorporated by reference has been derived, is for information purposes only and is not incorporated by reference because it is not relevant for the investor.

Issuer Interim Financial Information and Interim Report

The tables below set out the relevant page references in the June 2024 Financial Statements and the 2024 January-June Financial Report where the following information incorporated by reference in this Base Prospectus can be found:

	Information incorporated by reference in this Base Prospectus	**June 2024 Financial Statements page reference[(1)]**
1.	Auditor's report on the interim condensed consolidated financial statements for the six-month period ended 30 June 2024	1-8[(2)]
2.	Audited condensed consolidated balance sheets for the six-month period ended 30 June 2024 and the comparative consolidated financial information of the Issuer for the year ended 31 December 2023	108-109
3.	Audited condensed consolidated income statements for the six-month period ended 30 June 2024 and the comparative consolidated financial information of the Issuer for the six-month period ended 30 June 2023	110
4.	Audited condensed consolidated statements of recognised income and expense for the six-month period ended 30 June 2024 and the comparative consolidated financial information of the Issuer for the six-month period ended 30 June 2023	111
5.	Audited condensed consolidated statements of changes in total equity for the six-month period ended 30 June 2024 and the comparative consolidated statements of changes in total equity for the six-month period ended 30 June 2023	112-113
6.	Audited condensed consolidated cash flow statements for the six-month period ended 30 June 2024 and the comparative consolidated cash flow statement of the Issuer for the six-month period ended 30 June 2023	114
7.	Explanatory notes to the interim condensed consolidated financial statements for the six-month period ended 30 June 2024	115-161

Notes:

(1) Not all the pages of the June 2024 Financial Statements are paginated continuously. See below for detailed indications on where the relevant sections incorporated by reference in this Base Prospectus are located.

(2) Page references are to the page numbers of the auditor's report which is located after the financial report (pages 1-96 of the document incorporated by reference) and precedes the June 2024 Financial Statements, located immediately after the front cover page and the interim consolidated directors' report.

Information incorporated by reference in this Base Prospectus		2024 January-June Financial Report page reference
1.	Financial Information by Segments	24-42
2.	Corporate Governance	45
3.	Financial Information	49-75
4.	Alternative Performance Measures	76-87
5.	Glossary	91
6.	Important information	92-93

GENERAL INFORMATION

The following text shall replace in its entirety the text in the sub-section entitled "Significant/Material Change" in the section of the Base Prospectus entitled "General Information":

"5. Since 30 June 2024 there has been no material adverse change in the prospects of the Issuer or the Group, nor any significant change in the financial or trading position of the Issuer or the Group."