CANAL ABIERTO POLICY
OPEN BANK AND OPEN DIGITAL SERVICES

Openbank

TABLE OF CONTENTS

Openbank

1 Introduction

1.1. Purpose and context

An effective communication system reinforces our commitment to driving an ethical and honest culture aligned with the Corporate Culture Policy (*Política Corporativa de Cultura*), the Responsible Banking strategy (*Estrategia de Banca Responsable*), to which Openbank is firmly committed, and *The Santander Way*.

Open Bank, S.A. (hereinafter, "Openbank")[1] will implement an Internal Information System called Canal Abierto[2] (hereinafter also referred to as "Open Channel"), the bank's whistleblowing channel, to detect and respond to any conduct that violates the General Code of Conduct (*Código General de Conducta*) or goes against: our simple, personal and fair values, our corporate conduct, and our leadership principles. It also aims to foster an environment in which employees, senior managers, board members and any third parties with whom Openbank establishes a relationship, can speak clearly and be heard, strengthening the culture of information and compliance at and within the Santander Group.

The purpose of this Canal Abierto Policy (hereinafter also referred to as the "Open Channel Policy" or the "Policy") is to define the criteria that will govern the establishment and management of information systems provided to stakeholders, in order to:

- Align them with the Open Channel model defined and promoted by both the Santander Group and the Openbank Board of Directors and its senior management; and
- To ensure that complaint reporting channels have consistent and robust principles and procedures that allow the consistent reporting of information to the corresponding governing bodies.

Openbank actively promotes the communication and reporting of any irregularities.

This Policy is supplemented by the management guidelines established in the Canal Abierto Use and Operating Procedure (hereinafter also referred to as the "Open Channel Use and Operating Procedure").

1.2. Definitions and scope

The following definitions are used in the publication of this Policy:

- Open Channel: the Internal Information System model established by Openbank, covering the various channels available for submitting communications, the person responsible for it, and its governing principles, which are included in this Policy and the Open Channel Use and Operating Procedure.

Open Channel can be used to report any suspected **professional conduct** violations relating to:

- Unlawful acts in the workplace.
- Irregularities and violations of the General Code of Conduct and its implementing regulations that could constitute a violation subject to disciplinary action.
- Inadequate accounting or auditing practices, internal control or undue influence on external auditors (SOX).
- Violations of the prevention of money laundering and terrorist financing regulations or internal compliance regulations, as well as the regulations against corruption and bribery.
- Violations of Securities Market regulations.
- Conduct that could constitute an unlawful act or contravene any applicable regulations and, in particular, a serious or very serious criminal offence or administrative violation, or a violation of European Union law[3].

[1] References to Openbank throughout this Policy will, where applicable, be understood to refer to Open Digital Servicies, S.L. (ODS).

[2] Canal Abierto is the Internal Information System established by Openbank, covering the various channels available for submitting communications, the person responsible for it, and its governing principles, which are included in this Policy and the Canal Abierto Use and Operating Procedure.

[3] Any person who reports such conduct will also be protected under the specific protection regime established in Law 2/2023.

- Actions or conduct suspected of being inconsistent with the Code of Conduct in force at all times in the Santander Group and Openbank's leadership principles.

Annex I of this Policy includes details of the types of conduct that can be reported through Open Channel, and their definitions.

1.3. Scope of application and transposition to subsidiaries

This Policy is prepared and approved by Openbank's governing bodies and is of direct application.
Approval of this Policy must have prior validation from the Corporation.

2. Criteria

As Open Channel is a global model at the Santander Group, this Policy is structured into the following levels for effective implementation:

a) **Common standards (Section 2.1):** the pillars of the Open Channel Internal Information System model. These have been designed considering international standards and best practices. All channels must comply with these standards in order to be aligned with the Santander Group Open Channel (*Canal Abierto de Banco Santander*) model.

b) **Management criteria (Section 2.2):** elements agreed on to achieve standard and consistent management of all the channels included in the Internal Information System, to ensure Open Channel fulfils its purpose as a tool to foster corporate culture, for risk management and to identify the main concerns within the Group, so that such issues can be addressed and reported to Group's senior management.

c) **User Guarantees (Section 2.3):** the guarantees Open Channel gives its users.

d) **Local initiatives (Section 2.4):** Openbank may implement any and all initiatives it deems appropriate to promote the use of its respective information systems and their optimal management.

2.1. Common standards

The common standards with which all Group channels must comply are as follows:

- **Tone from the top.**

Senior management support and involvement in Open Channel and its management is key to ensuring its correct operation and the trust of employees and other stakeholders.

It is highly recommended that the Openbank CEO sponsor the channel through internal communications and/or other forms of communication (such as videos), highlighting the importance of using these channels to communicate irregularities for their investigation and improvements.

The Board of Directors made the *Chief Compliance Officer* responsible for managing Openbank's Internal Information System (Open Channel), because they perform their role independently and autonomously and have the necessary staff and material resources. The Independent Whistleblower Protection Authority (*Autoridad Independiente de Protección del Informante*) is informed of their appointment.

The departments involved in managing Open Channel act by delegation from the person responsible for it, and must keep them informed of the result of any investigations undertaken and the main actions carried out as part of these investigations.

Regulatory Compliance will coordinate the Open Channel management.

- **Duty to report potentially unlawful acts or compliance failures**

All workforce professionals, including senior management and members of the board of directors, are required to report any presumed serious or very serious criminal offences or administrative violations, or violations of European Union law, as well as any suspicions of unlawful acts to Openbank.

- **Awareness-raising initiatives.**

It is important to make the channels available to all employees so that they are aware of the importance of using them to create a positive work environment.

To this end, awareness and/or training initiatives will be implemented on a regular basis, so that all employees understand the importance of this channel, as well as its characteristics, operating and use.

- **Easy access to the Channel.**

Open Channel must be easily accessible and available through the intranet, website, or any other channel, and easy for any employee or third party to find.

- **Communication of statistical data, results or lessons learned from communications received through Open Channel to employees.**

General communications will be used to inform employees of the management and consequences of Open Channel communications.

This is to promote channel use by demonstrating the action undertaken when cases are reported, to provide information about the measures taken, and to ensure that the measures and improvements implemented serve as an example to prevent similar conduct in future.

- **Anonymity of Open Channel communications, at the whistleblower's request.**

Anyone who accesses the channel has the right to do so anonymously, and their anonymity will be guaranteed using appropriate mechanisms to the extent permitted by the law.

Irrespective of whether anonymity is selected, all communications are completely confidential.

- **Open Channel can be used to report any conduct not aligned with Openbank's corporate conduct and leadership principles**.

Respect for our corporate culture, conduct and values is fundamentally important. The Channel can be used to report any professional conduct that does not align with Santander Group culture, including Openbank's corporate conduct and leadership principles, as well as serious or very serious criminal offences or administrative violations, violations of European Union law, or more serious irregularities or violations with respect to the General Code of Conduct.

- **Open Channel is managed by an external provider to guarantee communication confidentiality and anonymity.**

Best practice uses externally managed communication platforms to guarantee confidentiality and anonymity, without prejudice to all of the other channels available and set out in Section 2.3 of this Policy.

- **Provision of mechanisms to prevent conflicts of interest during the investigation of communications received.**

This channel is designed to prevent conflicts of interest during investigations (Section 2.3), so it is essential to establish suitable mechanisms and controls that mitigate these situations.

- **Periodic Open Channel review by Internal Audit.**

Open Channel will be inspected by the Internal Audit team. As part of its functions, and in accordance with its Risk Assessment and annual audit plan, this department will periodically assess whether the channels comply with these common standards.

2.2. Management criteria

Open Channel must use the following management criteria:

- **Categories of the types of cases that can be reported through Open Channel**

The classification and definition of cases to be applied on approval of this Policy are described in **Annex I**. The Compliance team can review these categories and they can be updated by Compliance Committee agreement. Corporate Compliance may also review and modify the categories and will notify Openbank Compliance of any modifications, in order to ensure consistent classification.

- **Channels for employees or third parties (service providers, customers, etc.)**

Open Channel can receive communications from:

- Openbank professionals[4].
- Members of the Board of Directors.
- Interns.
- Openbank service providers.
- Customers.
- Any other third party who, pending appointment to any of the above positions or following the termination thereof, has been affected by the conduct reported during that process.

- **Processing of cases received from other internal sources (from Human Resources, Internal Audit, monitoring roles, etc.) or external sources**

Open Channel receives all communications from employees or third parties who report them using this Channel.

The Compliance team may also use Open Channel to report any cases involving a suspected violation of the law or General Code of Conduct, particularly, any suspected serious or very serious criminal offences or administrative violations, or a violation of European Union law, of which it becomes aware through other internal or external source, without the prior consent of the employee concerned[5].

Human Resources will not include employee communications and/or conversations regarding employment issues or conduct that is not aligned with Openbank's corporate conduct or leadership principles in Open Channel, unless a whistleblower expressly asks them to do so.

Anyone who receives a communication that must be submitted through Open Channel, and who is not responsible for its management, must transfer it to Open Channel immediately, and must respect the whistleblower protection measures included in this Policy, the data protection provisions and other applicable regulations at all times.

Accordingly, training and awareness initiatives will be designed and implemented so employees know how to respond whenever they receive a communication that they are not required to manage.

Anyone who becomes aware of any violation and, in particular, any conduct that could constitute a serious or very serious criminal offence or administrative violation, or a violation of European Union law, through any other communication channel, can process it through Open Channel, provided that it meets the admissibility criteria set out in Section 1.3 of this Policy.

- **Mechanisms to prevent conflicts of interest**

The general principles for managing conflicts of interest will be taken into account when managing cases reported through Open Channel: i) prevent; ii) disclose and; iii) refrain from any involvement in decision-making, acting in accordance with the provisions of the Conflicts of Interest Policy.

---

[4] Communications must refer to known facts within the scope of an existing (terminated or ongoing) professional relationship (for example, former employees or candidates involved in employment selection processes).

[5] It is not necessary to include any violations the Compliance team identified as part of its regular controls.

Whenever a potential conflict of interest affecting the person conducting the investigation or their team is identified, the case will be referred to a different person or team.

It may be necessary to call upon the services of an external investigator in special cases.

- **Whistleblower and investigated party rights**

Internal investigations must respect the fundamental rights of the whistleblower and the investigated party.

Anyone who makes a complaint through Open Channel has the right to confidentiality of the reported facts, anonymity, and may not be subject to retaliation for using Open Channel in good faith.

All information, documentation, evidence, deliberations, etc., relating to the internal investigation must be kept confidential. Therefore, only those specifically designated to do so, will take part in internal investigations.

If the documentation generated through the investigation (including the final report) needs to be shared with anyone other than those appointed to carry it out, authorisation from the heads of Regulatory Compliance and Labour Relations must be obtained.

The investigated party will be informed of their alleged actions or omissions (in the time and manner deemed appropriate to ensure successful investigation), and have the right to be heard at any time, so that they can prepare their arguments and appropriate means of defence.

In all cases, investigated parties' presumption of innocence, honour and access to the file will always be ensured during the investigation. Access to the file is understood as the right to know the allegations against them without revealing information that could identify the whistleblower, and without compromising the outcome of the investigation. This duty to inform the investigated party will not apply in cases where the complaint is not directly processed through this channel or in cases regarding money laundering and terrorist financing, which will be governed by the applicable legislation and internal regulations, particularly regarding the prohibition of disclosure regarding communications and investigations into operations. This duty to inform the investigated party will also not apply when it implies compromising the confidentiality of the reporting party, in accordance with the provisions of the data protection regulations.

Investigated parties may explain their version of events and provide the evidence they deem necessary, and may submit allegations in writing.

Whistleblowers' anonymity will be guaranteed, along with the confidentiality of the facts and details of the procedure.

The internal investigation procedure carried out must be independent, free from any (even potential) conflicts of interest, in accordance with the provisions of this Policy, the Open Channel Use and Operating Procedure, and the Conflicts of Interest Policy (*Política de Conflictos de Interés*).

Similarly, the actions taken by the investigating team must be commensurate and must always respect the rights to privacy, honour and reputation of those involved.

- **Maximum duration of the investigation and resolution of the cases received**

Whistleblowers will be sent an acknowledgment of receipt for any communication, from Open Channel, within a maximum period of five days.

Cases received through Open Channel must be managed within a maximum period of 60 days, except for cases of special complexity or where there are valid reasons that justify extending this period for a further 30 days.

The Information System Manager must be informed of cases in which the investigation period takes longer than the established 60-day period.

- **Processing the cases received.**

All cases reported through Open Channel will be duly processed, without prejudice to their inadmissibility under the circumstances established, or when processing determines whether or not they are substantiated.

Whenever additional information is required to initiate or continue the investigation, the whistleblower will be asked for this information. If it is not received within 15 days, the case will be closed and classified as "insufficient information".

The person responsible for the internal investigation will gather all the information and documentation they deem appropriate from any Group department or company.

Internal Audit and other departments may also be asked to provide any assistance deemed necessary.

Cases received will be processed in accordance with the provisions of the Open Channel Use and Operating Procedure.

- **Monitoring, reporting and escalation.**

○ Openbank must report quarterly KPIs for all cases received through the Channel to Corporate Compliance. Any cases reported by whistleblowers who identify themselves as employees must be specifically mentioned.

○ If a member of Openbank's senior management[6] or board of directors is affected by the complaint received, the severity of the facts will be assessed to determine whether Corporate Compliance or corporate bodies should be informed, given the involvement of a director or the managerial sector to which the investigated person belongs, without prejudice to the case being managed and investigated locally when the conduct took place in this field. Corporate Compliance will be informed of the outcome of the investigation.

○ Each Compliance role will analyse trends and patterns in the measures adopted in the event of any irregularities or violations, in order to identify fluctuations in the percentage of disciplinary actions taken at Openbank.

The competent governing bodies will be informed when outliers are identified.

○ Compliance will assess the case according to the severity of the facts, and will inform Corporate Compliance upon receiving complaints regarding accounting or auditing irregularities, and escalate these to the Openbank Audit Committee[7]. Their resolution will be escalated to the Openbank Audit Committee and Corporate Compliance so that it can be subsequently escalated to the Banco Santander, S.A., Audit Committee.

- **Disciplinary system**

On completing the investigation, the team will agree how to close the file, determining whether or not it is a violation of the law, internal regulations, or any other applicable law, such that:

○ If a violation is deemed unproven, the file is closed without any further action requirements, accordingly archived and the whistleblower and those affected are notified.

○ If a violation is considered proven, it will be transferred to Human Resources or any other body with the powers to take the appropriate disciplinary measures and/or adopt corrective and/or preventive organisational and/or training measures.

When the facts could constitute a crime, the person responsible for the management of Open Channel will send the file to Legal Advisory Services so that they can immediately proceed to send the information to the Prosecution Service or the European Public Prosecutor's Office in the event that the facts affect the financial interests of the European Union, unless the conduct is deemed atypical, which will be reported to Compliance. Notwithstanding the foregoing, if the evidence is clear, this referral decision will be adopted through the described channel before the investigation is completed.

Similarly, measures can be adopted to improve procedures, policies or tools to prevent the recurrence of the detected irregularity, and to foster a simple, personal and fair culture, and compliance with corporate conduct, leadership principles, or the applicable regulations.

2.3. User guarantees

The guarantees that define Open Channel are:

- **Open-Door Policy**

Whistleblowers can access Open Channel directly, as it is the preferred channel for reporting any of the above mentioned situations.

Open Channel allows communications in writing, through the website: www.openbank.esthicspoint.com.

[6] Understood as a collective belonging to the Solaruco, Faro and Promontorio corporate segment.

[7] Any references to the Openbank Audit Committee throughout this Policy will be understood, where applicable, to refer to the Open Digital Servicies, S.L. (ODS) Board of Directors.

An in-person meeting with Open Channel managers may also be requested.

Whistleblowers may also always report any conduct they consider may constitute a serious or very serious criminal offence or administrative violation, or a violation of European Union law, through the channel established by the Independent Whistleblower Protection Authority, as well as through the channels established by other bodies, given as examples in **Annex II**.

- **Confidentiality and anonymity**

Open Channel communications will be confidential, and can be anonymous.

Confidential communications protect the identity of the person reporting the events, without prejudice to the legal obligations and rights protections of individuals or legal entities accused of acting in bad faith.

Both Compliance and Human Resources will ensure that this confidentiality is maintained. They will identify any potential conflicts of interest or other circumstances that could compromise such confidentiality, and will take the steps necessary to resolve them.

All those aware of the communications received through Open Channel, including the affected parties, are required to keep the whistleblower's identity, and the facts and circumstances relating to the complaint, secret.

If the communication results in the initiation of legal or administrative proceedings, the competent legal or administrative authorities may need to be informed of the whistleblower's identity, in accordance with the provisions of the Law.

- **Non-retaliation**

Whistleblowers who submit communications in good faith will be protected against any type of discrimination and penalty for having reported the case. Taking any action against the whistleblower that might constitute retaliation, including the threat thereof, or any type of negative consequence for having reported any conduct suspected of being unlawful, irregular or inconsistent with the corporate conduct in force, is strictly prohibited.

Retaliation is defined as any act or omission that, either directly or indirectly, involves unfavourable treatment that places the persons who suffer them at a particular disadvantage with respect to another in the professional context, solely because they are a whistleblower or have made a public disclosure.

By way of example, retaliation will be understood as[8]:

i) suspension of the employment contract; dismissal or termination of employment or statutory relationship, including the non-renewal or early termination of a temporary employment contract after the probation period has elapsed; or early termination or cancellation of contracts for goods or service agreements; the imposition of any disciplinary action; demotion or denial of promotions and any other substantial amendment to working conditions; and the non-conversion of a temporary employment contract into a permanent contract, if the employee had legitimate expectations that they would be offered a permanent position;

ii) damages, including reputational damage, or financial losses, bribery, intimidation, harassment or ostracism;

iii) unjustified negative job or professional performance evaluations;

iv) the denial of training;

v) discrimination, or unfavourable or unfair treatment.

vi) Prohibition of service provider contracts.

[8] Examples extracted from Law 2/2023.

The scope of protection extends to persons related to the whistleblower (co-workers, family members, related legal entities, etc.). It will also cover any individual who assisted the whistleblower and, specifically, to employee legal representatives who advised or supported the whistleblower.

The prohibition of retaliation provided for in this section will not prevent the adoption of the appropriate disciplinary measures whenever the internal investigation determines that the communication is false and was made in bad faith, or that the whistleblower violated corporate conduct or acted illegally. Similarly, the measures provided for in items i, iii and iv above will not be understood as retaliation when adopted in the regular exercise of management authority under the labour legislation, for proven circumstances, facts or violations, unrelated to the presentation of the communication.

Anyone who reports information through Open Channel will be protected from retaliation, provided that the communication was made in good faith and in accordance with the requirements set out in this Policy and the other applicable regulations. Any person who commits the following is excluded from this protection:

- Submits a communication containing information from previous communications that have been previously found inadmissible for any of the reasons described in this Policy or in the Open Channel Use and Operating Procedure.
- Reports interpersonal conflicts that only affect the whistleblower and the persons mentioned in the communication.
- Communicates public information or mere rumours.
- Communicates information that refers to actions or omissions not included in the scope of Open Channel, in accordance with this Policy.

- **Managing conflicts of interest[9] when handling Open Channel communications**

Anyone who may be involved in a (potential) conflict of interest with those involved in the complaint will refrain from involvement in managing the communications received through Open Channel. This also applies to any person belonging to a department from which Open Channel will require support during the investigation.

The provisions of the Conflicts of Interest Policy will always apply and the mechanisms indicated in Section 2.2. of this Policy must always be implemented.

2.4. Local initiatives

Openbank may carry out its own initiatives independently of Open Channel. These initiatives will be shared with Corporate Compliance in order to promote best practice, sharing and learning between all Group banks, respecting the provisions of this Policy, in all matters that do not contradict the applicable legal regulations.

3. Governance and authority

The governing bodies with authority over Open Channel are:

3.1. Board of Directors

Responsible for the establishment of the Internal Information System (Open Channel) and the appointment of the person responsible for it at Open Bank, S.A., or Open Digital Services, S.L.

3.2. Risk, Regulation and Compliance Oversight Committee

The Risk, Regulation and Compliance Oversight Committee is responsible for supervising Open Channel. Similarly, responsibility is assigned to the following bodies:

- Audit Committee

Whenever the communication received through Open Channel refers to accounting or auditing matters, under the Sarbanes-Oxley (SOX) Act, based on the severity of the facts, upon completion of the investigation in accordance with this Policy, the resolution will be submitted to the relevant Audit Committee, which will decide on the appropriate actions, and on what will be reported to Corporate Compliance for subsequent escalation to the Banco Santander, S.A., Audit Committee.

- Appointment Committee
Issues the report on measures to be taken with respect to the directors in the event of a breach of the Group's code of conduct on the securities markets, which can be reported through Open Channel.

3.3. - Compliance Committee
The Compliance Committee is responsible for following up on the information regarding cases received through Open Channel.

4. Ownership, interpretation, validity date and review

4.1. Ownership of the Policy

The Compliance team is responsible for drafting this Policy.

Its approval is the responsibility of the Board of Directors of Open Bank, S.A and Open Digital Services, S.L.

4.2. Interpretation

The Compliance team is responsible for interpreting this Policy.

In the event of any conflict between the Spanish version and the English version, the Spanish version shall take precedence.

4.3. Date of validity and review of the Policy

This Policy will enter into force on the date of its publication. Its content will be subject to periodic review, and any changes or amendments deemed appropriate will be made at least every three (3) years. Changes that do not affect the substance of the procedure will be approved by the Compliance Committee and reported to the Audit Committee.

5. Version History

ID		Validation	Approval	
			Committee	Date
V1	Eva Yebra	N/A	Compliance Committee	30/04/2021
V2	Iliana Broschat	Corporate area	Board of Directors	22/05/2023

ID	Description
V1	First version of the policy.
V2	Second version of the policy. Adaptation to Law 2/2023, of 20 February, transposing the European Directive on whistleblower protection.

Openbank

ANNEX I: CATEGORIES OF THE TYPES OF CASES THAT CAN BE REPORTED THROUGH OPEN CHANNEL AND DEFINITIONS

Category	Subcategory	Definition
General Code of Conduct	**Marketing of products and services**	Marketing products or services without fulfilling the obligation to treat the customer fairly by acting honestly, impartially and professionally.
	Conflicts of interest/activities outside Openbank	Situations in which an employee's personal or financial interests (or those of their immediate family members or anyone with whom the employee has a close relationship) interfere in any way with their ability to serve the best interests of Openbank, its customers, and/or other stakeholders.
	Gifts and invitations	When a professional abuses their role at Santander by offering, giving, promising, requesting or accepting any kind of gift, benefit/consideration or invitation to obtain a personal advantage for themselves or a third party, affecting their impartiality.
	Corruption and bribery	A corrupt act can arise whenever an individual abuses their position of power or responsibility for their own personal gain. Bribery is any act that gives someone a financial or other advantage to encourage that person to perform their functions or activities improperly, or that rewards that person for having done so. This includes any attempt to influence a decision maker by granting them some form of additional benefit that goes beyond a legitimate offer. Bribery involving a national or international public official.
	Prevention of money laundering, terrorist financing and sanctions	Money laundering is: i) The conversion or transfer of assets, knowing that such assets are derived from criminal activity or involvement in criminal activity, for the purpose of hiding or concealing the illicit origin of the assets or to assist persons who are involved in circumventing the legal consequences of their acts; ii) The hiding or concealment of the nature, origin, location, disposal, movement or actual ownership of assets or rights over assets, knowing that such assets are derived from criminal activity or from involvement in criminal activity; iii) The acquisition, possession or use of assets, knowing that, upon the receipt thereof, they are derived from criminal activity or from involvement in criminal activity; iv) Involvement in any of the activities referred to in the previous items, any association with the perpetration of such acts, any attempt to perpetrate them, and the act of assisting, instigating or advising someone to perform or facilitate the execution thereof.
	Insider trading	Undertaking business transactions based on insider information. Recommending trading on the securities market on the basis of insider information. Unlawfully disclosing and using insider information. Manipulating the market by selling or disseminating fake news or rumours about individuals or companies for the purpose of altering or maintaining the price of a security or financial instrument.

	Anti-competitive practices	Conduct that prevents, restricts or falsifies free and effective competition to the detriment of the market, Openbank customers and all those with whom business and/or professional relationships are maintained. Such conduct includes exchanging sensitive information with competitors, pricing agreements, market sharing, or bid rigging.
	Privacy / Information security / Information confidentiality	Privacy and information security involves refraining from disseminating information to third parties; for example, personal information of customers, employees (salaries, authorisations, etc.), details of Santander security/strategy, as well as information relating to the banks with which Santander does business. These obligations are maintained even after termination of employment and the use of confidential information for financial gain is prohibited.
	Internal fraud	Fraud that is attempted or perpetrated, by one or more internal parties against the organisation, i.e., an employee or a subsidiary of the organisation, including cases in which an employee acts in collusion without external parties.
	Cybersecurity	Cybersecurity risks are: i) unauthorised access to or misuse of information or systems (for example, theft of personal information, merger and acquisition plans, or intellectual property); ii) financial fraud and theft (for example, diversion of payments, withdrawal of funds from customer accounts, credit card fraud, identity theft, etc.); iii) business disruption (for example, sabotage, extortion, denial of service).
	Equal opportunities and diversity	Conduct that is not aligned with the Openbank basic principles on providing equal opportunities to employment and professional promotion, and ensuring zero discrimination on the basis of gender or sexual orientation, race, religion, disability, origin, marital status, age or social status at all times.
	Sexual harassment	Disrespectful or unwelcome conduct of a sexual nature that is disruptive and creates an intimidating, offensive, or hostile work environment.
	Workplace harassment	Systematically hostile or degrading treatment that creates an intimidating, offensive or hostile working environment.
Fraud	**External fraud**	Fraud attempted or perpetrated by an external party (or parties) against the organisation or customers for whom the bank is responsible. An internal party may also be involved in the fraud in some cases.
Accounting and auditing	**Accounting and auditing**	Alteration or falsification of financial information, inaccuracies in financial statements, intentional misrepresentation of information, undue influence over auditors, questionable practices in terms of accounting, auditing or internal financial controls.
	Failure to comply with corporate conduct	Unprofessional conduct by co-workers or managers that is not aligned with the Santander Way.

Labour matters and non-compliance with corporate conduct	**Serious disrespect**	Conduct involving serious disrespect by co-workers or managers in the work environment.
	Failure to comply with labour regulations	Any failure to comply with the (legal or contractual) regulations, or Openbank internal procedures or policies that implies the breach of an obligation under employment law, or any obligations defined in the current collective bargaining agreement.
	Failure to comply with Openbank leadership principles	Unprofessional employee conduct that is not aligned with Openbank's leadership principles.
Others	Any breach of current legal or internal regulations and Openbank policies or procedures in relation to operational or organisational aspects not mentioned in the previous categories.	

ANNEX II: EXTERNAL CHANNELS FOR REPORTING VIOLATIONS UNDER THE SCOPE OF APPLICATION OF LAW 2/2023

- Channel established by the Independent Whistleblower Protection Authority. [INCLUDE CONTACT DETAILS ONCE ESTABLISHED]
- Bank of Spain: https://www.bde.es/bde/es/secciones/sobreelbanco/Transparencia/Informacion_inst/registro-de-acti/Canal_de_denuncias.html
- National Commission on Markets and Competition (Comisión Nacional de los Mercados y la Competencia, CNMC): https://sede.cnmc.gob.es/tramites/competencia/denuncia-de-conducta-prohibida
- National Securities Market Commission (Comisión Nacional del Mercado de Valores, CNMV): https://www.cnmv.es/portal/whistleblowing/presentacion.aspx#:~:text=Escribiendo%20a%3A%20Comunicaci%C3%B3n%20de%20Infracciones,revelar%20su%20identidad%20o%20no
- SEPBLAC (*Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias* [Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences]): https://www.sepblac.es/es/sujetos-obligados/tramites/comunicacion-por-indicio