



03.05 Speak-Up Policy

Policy Owner:	Russell, Carrie
Contact:	fiethicsoffice@fisglobal.com
Domain:	Corporate Legal
Scope:	Enterprise Wide
Published Date:	November 17, 2023
Effective Date:	November 17, 2023
Mandatory Review Date:	November 17, 2024
Provision for Exception:	Exceptions require Policy Exception Committee approval unless otherwise delegated within the policy.

03.05 Speak-Up Policy	3
03.05.01 Definitions	4
03.05.02 Making a Report	5
03.05.03 Confidentiality and Anonymity	5
03.05.04 Investigation and Outcome	6
03.05.05 Protection and Support for Reporters	6
03.05.06 External Disclosures	7
03.05.07 Data Privacy	7
03.05.08 Retention of Records	7
03.05.09 Appendix: External Reporting	8
03.05.09.01 Part A: Violations of European Law that May Be Reported Externally	8
03.05.09.01 Part B: EU Member-States Agencies to Whom Whistleblower Concerns May Be Reported	8

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in [Best Current Practice – Key Words](#).

03.05 Speak-Up Policy

Purpose

Our policy intends to:

- **Encourage** reporting of suspected wrongdoing as soon as possible, with the knowledge that concerns will be taken seriously and investigated in a timely manner, and that confidentiality will be respected.
- **Provide** guidance as to how to raise those concerns.
- **Reassure** Reporters that genuine concerns may be raised in Good Faith without fear of reprisals or Retaliation, even if such concerns turn out to be mistaken.
- **Prevent/detect harm** to FIS and prevent financial loss and regulatory sanctions.
- **Demonstrate a commitment** to FIS' values, Code of Business Conduct and Ethics ("Code"), policies, laws, and regulations.

Scope

This policy applies to all FIS legal entities and affiliates ("Company"). It identifies how colleagues ("employees"), contract labor, consultants, and others acting on behalf of FIS can raise risks and concerns.

It also sets out how clients, customers, suppliers, business partners and other third parties may report irregularities or wrongdoing concerning FIS or its colleagues.

The **types of behavior that should be reported** include but are not limited to:

- Criminal activity;
- Failure to comply with any legal or professional obligation or regulatory requirements;
- Miscarriages of justice;
- Danger to health and safety;
- Damage to the environment;
- Bribery and/or corruption;
- Facilitating tax evasion;
- Financial fraud;
- Breach of our Code or other company policies;
- Conduct likely to damage the Company reputation or financial well-being;
- Unauthorized disclosure of confidential information;
- Negligence; and
- The deliberate concealment of any of the above matters.

This policy does not apply to **personal** work-related grievances such as decisions relating to the terms and conditions of employment, suspension, termination, or performance evaluations. If a complaint relates to a colleague's own personal circumstances and does not involve a behavior identified above, colleagues should reach out to **The People Office Support Center** to [raise a concern, a grievance or a complaint](#).

If a complaint relates to a colleague's own personal circumstances but they also have wider concerns regarding one of the behaviors set out above (*i.e.*, a violation of the Code or other company policies), colleagues are encouraged to engage with their management, [The People Office](#), or the **Ethics Office** to determine which route is the most appropriate.

For clients, customers, suppliers, business partners and other third parties, the Speak-Up Policy would not apply to commercial dissatisfaction arising from a contract unless it also involves a behavior identified above.

All colleagues are responsible for the success of this policy. Colleagues are invited to comment on this policy and suggest ways in which it might be improved. Comments, suggestions, and queries should be addressed to the **Ethics Office** at fisethicsoffice@fisglobal.com.

NOTE: This policy does not form part of any contract of employment or other contract to provide services and may be amended at any time.

Statement

FIS is committed to:

- Conducting business honestly and with integrity and high standards in accordance with our Code;
- Maintaining a culture of openness and accountability;
- Strengthening a culture of transparency and trust; and,
- Protecting the integrity and reputation of the Company.

However, companies face the risk of things going wrong from time to time, or of unknowingly harboring illegal or unethical conduct. A culture of transparency and trust with accountability is essential to prevent such situations from occurring and to address them when they do occur.

If colleagues have any genuine concerns related to suspected wrongdoing or danger affecting any of FIS' activities, they are required to report it under this policy.

In addition, clients, customers, suppliers, business partners and other third parties should raise concerns via the [FIS Ethics Helpline](#) or contact the FIS Ethics Office at fisethicsoffice@fisglobal.com.

03.05.01 Definitions

- **Anonymous** reporting is a process whereby individuals can submit a report without revealing their identity.
- **Anonymity** is the condition of remaining Anonymous.
- **Good Faith** means having reasonable grounds at the time a report is made, based upon the circumstances and information available, that the information in the report is true.
- **Reporter** is any person who raises information or reports a concern about illegal or unethical conduct in Good Faith. All Whistleblowers will be Reporters but not all concerns will be Whistleblower Concerns.
- **Retaliation** in the workplace is when a Reporter is punished by the Company, a manager, a colleague, or other third-party for reporting illegal or unethical conduct that is legally protected. Retaliation can come in many forms of detrimental treatment, including lowering a colleague's pay, withholding a promotion, not hiring a colleague who cooperated as a witness or terminating a colleague solely for raising a concern.

Retaliation is not expecting colleagues to perform tasks in their job description, continuing to manage performance after a report is made, or disciplining a colleague for knowingly making a malicious or fraudulent accusation. In addition, reporting concerns does not protect a colleague from discipline for any misconduct learned in connection with the investigation or otherwise.

- A **Whistleblower** is a person who raises Whistleblower Concerns in “Good Faith”.
- **Whistleblower Concern** can encompass illegal activity and/or various types of behavior or wrongdoing as further listed as examples in this policy’s Scope section.

NOTE: The disclosure of violations protected by European Union law is described further in the Appendix to this policy.

03.05.02 Making a Report

It is the responsibility of all colleagues to comply with the Code, Company policies, and the law, and to report violations or suspected violations in accordance with this Speak-Up Policy.

Managers have an even greater level of responsibility and must lead with integrity and reinforce the Company’s ethical culture. They are often the first resource for colleagues who have questions on ethical issues or potential violations of Company policy, and national or international laws. They may be held responsible for their failure to report misconduct or to take steps to address or remediate an issue.

1. Colleagues should raise concerns orally or in writing with:
 - Their line manager;
 - The People Office through [The People Office Support Center](#);
 - The FIS Ethics Office at fisethicsoffice@fisglobal.com; or
 - The [FIS Ethics Helpline](#).

Concerns raised to the Ethics Helpline can be made anonymously where permitted under local laws.

If preferred, a face-to-face meeting can be arranged. Colleagues are asked to provide as much detail as possible to aid in a thorough investigation of their concerns.

2. Clients, Customers, suppliers, business partners and other third parties should raise concerns via the [FIS Ethics Helpline](#) or contact the FIS Ethics Office at fisethicsoffice@fisglobal.com.

03.05.03 Confidentiality and Anonymity

FIS encourages Reporters to voice their concerns openly under this policy. The Company will make every effort to only disclose the identity of the reporting person, and anyone mentioned in the reported concern, as necessary and proportionate in the context of the investigation. For any Whistleblower Concern under EU law, the identity of the Reporter will not be disclosed without their express consent.

The Company permits Anonymous reports, as per local laws, but encourages Reporters to disclose their identity if they feel comfortable doing so. While every effort will be made to investigate Anonymous reports, Anonymous reporting can limit the ability to fully investigate the matter. It may be difficult or even impossible to conduct a proper investigation if the Company cannot obtain further information from the Reporter.

03.05.04 Investigation and Outcome

Upon receipt of a concern, the Company will acknowledge receipt within seven (7) days and will aim to provide further feedback to the Reporter within 90 days. The Company will respect any stricter time restrictions that apply to a Whistleblower Concern, such as those concerns raised under EU law.

All reported concerns will be assigned to an investigator by the Company. The investigator is selected based on relevant experience or specialized knowledge of the subject matter with no conflicts of interest identified regarding the reported concern. Following the investigation, the investigator may make recommendations for change to enable the Company to minimize the risk of future wrongdoing (*i.e.*, process improvements, educational opportunities, potential risks, or control enhancements).

The Reporter should not conduct their own investigation, but they may be asked to assist with an investigation. Reporters are expected to cooperate with the investigation, and not interfere with it, offer false information, or alter or destroy records. All colleagues are obligated to cooperate with investigations and provide complete, accurate and truthful information whenever asked to do so.

The Company will aim to keep Reporters informed of the progress of the investigation and its likely time to completion. However, sometimes the need for confidentiality may prevent providing specific details of the investigation, an outcome or any disciplinary action taken as a result. Colleagues should treat any information about the investigation as confidential.

If the conclusion is that a Reporter has made allegations maliciously, the Reporter will be subject to disciplinary action up to and including termination, as per local law.

03.05.05 Protection and Support for Reporters

It is understandable that Reporters are sometimes worried about possible repercussions such as Retaliation. FIS aims to encourage openness and will support colleagues who raise concerns in Good Faith under this policy, even if they turn out to be mistaken.

FIS encourages colleagues and others to 'Speak-Up' about any suspected wrongdoing and will not tolerate Retaliation against anyone who, in Good Faith, reports any wrongdoing, a violation of the Code, an FIS policy or the law or who cooperates with an investigation, regardless of whether such report is protected by law.

Global applicable Whistleblowing laws provide statutory protection from Retaliation for Whistleblowers who raise Whistleblower Concerns in Good Faith. Facilitators who assist in reporting or disclosure, natural persons and non-profit legal entities (unions and associations) and those who are related to, or surrounding, the Whistleblower and legal entities controlled by a Whistleblower may also be protected under applicable Whistleblower laws.

If a Reporter believes that they have experienced a form of Retaliation, they should inform **The People Office** or **Ethics Office** at fisethicsoffice@fisglobal.com immediately. In addition, clients, customers, suppliers, business partners and other third parties should raise Retaliation concerns to the **FIS Ethics Office** at fisethicsoffice@fisglobal.com.

The Company has a zero tolerance for Retaliation. Colleagues must not threaten or retaliate against Reporters in any way. Anyone involved in such conduct will be subject to disciplinary action up to and including termination, as per local law.

03.05.06 External Disclosures

The aim of this policy is to provide guidance on the internal mechanism for reporting wrongdoing in the workplace. Colleagues are strongly encouraged to report any concerns internally so that FIS can investigate and resolve any issues.

In some circumstances it may be appropriate to report concerns to an external body such as a regulator. Colleagues are protected by law from Retaliation where they report certain violations to an external party. The Appendix to this policy sets out some of the Whistleblower Concerns that may be reported externally under EU law, together with the competent authorities in the EU member-states to which such reports may be made. Colleagues outside of Europe may also report externally in some circumstances.

Colleagues are not required to notify the company that they have made such reports or disclosures or obtain authorization from the Company prior to making such reports or disclosures.

03.05.07 Data Privacy

FIS is committed to safeguarding the privacy of those involved in the Speak-Up process. The Company is subject to various privacy and data protection laws in the jurisdictions in which it operates. FIS established Company policies to protect and secure personal data, including in particular the FIS Privacy Policy. Any personal data obtained in conjunction with this policy will be used for reasons outlined in this policy or as otherwise permitted by data protection laws. For further information, please review the FIS Privacy Center. For questions, please contact the FIS Privacy Office at PrivacyOffice@fisglobal.com.

03.05.08 Retention of Records

Reports of violations or suspected violations will be kept confidential to the extent possible - including for the retention of records, consistent with the need to conduct an adequate investigation. Creating and maintaining accurate and complete data is essential for our ability to meet our business needs as well as legal and regulatory requirements.

The Company has adopted a Records Management Policy and Records Retention Schedule to establish uniform guidance regarding the retention and destruction of information and records in conformity with applicable laws which includes investigations. For further general questions about our Record Management Policy, contact the FIS Privacy Office at PrivacyOffice@fisglobal.com. For any specific inquiries, please contact the FIS Ethics Office at fisethicsoffice@fisglobal.com.

03.05.09 Appendix: External Reporting

03.05.09.01 Part A: Violations of European Law that May Be Reported Externally

Violations in the areas of:

- Public procurement
- Financial services, prevention of money laundering and terrorist financing
- Corporate tax
- Product and transport safety
- Environmental and nuclear safety
- Food and feed safety, animal health and welfare and public health
- Consumer protection
- Protection of privacy, data protection and security of network and information systems
- Violations affecting the financial interests of the EU; and violations relating to the internal markets (including violations of EU competition and State aid rules).

The specific Whistleblower Concerns that may be reportable externally vary by member state.

03.05.09.01 Part B: EU Member-States Agencies to Whom Whistleblower Concerns May Be Reported

NOTE: *The following information is required to be provided under EU law. Colleagues outside of Europe may also report externally in some circumstances.*

Each EU member-state has designated competent authorities to whom Whistleblower Concerns may be made as follow:

Austria

- The Federal Office for Preventing and Combating Corruption
- Auditor Supervisory Authority
- Financial Reporting Authority
- Federal Competition Authority
- Financial Market Authority
- Money Laundering Reporting Office
- Notarial chambers
- Bar associations
- Chamber of Tax Advisors and Certified Public Accountants

Belgium

- The Competent Authority will vary depending on the field in which the violation is committed. The Belgian government will designate the Competent Authority for each sector. Where the government has not done so, the Federal Ombudsmen will be the Competent Authority

Czech Republic

- Ministry of Justice, with the Work Inspectorate retaining responsibility for fining employers for breaches of law

Denmark

- Danish data protection authority

France

- Defender of Rights (defenseur des droits) plus others for specific sectors

Germany

- Federal Office of Justice plus authorities competent to oversee the regulated financial sector

Ireland

- The Office of the Protected Disclosures Commissioner (OPDC)

Italy

- National Anti-Corruption Authority

Luxembourg

- The Luxembourg Financial Services Authority - CSSF
- The Luxembourg Insurance Commission - CAA
- The Luxembourg competition authority
- The Luxembourg Registration Duties, Estates and VAT Authority - AED
- The Luxembourg Inspectorate of Labour and Mines - ITM
- The Luxembourg Data Protection Commission - CNPD
- The Luxembourg Equal Opportunities Centre - CET
- The Mediator, as part of his mission to carry out external checks on places where people are deprived of their liberty
- The Ombudsman for children and youth
- Luxembourg Regulatory Institute - ILR
- Luxembourg Independent Regulator for Audiovisual Media Services - ALIA
- Luxembourg and Diekirch Bar Association
- Luxembourg Chamber of Notaries
- Luxembourg Medical Board
- Nature and Forest Administration - ANF
- Water Management Administration - AGE
- Air Navigation Administration - ANA
- National Consumer Ombudsman Service
- Order of Architects and Consulting Engineers - OAI
- Luxembourg Association of Chartered Accountants - OEC
- Luxembourg Institute of Auditors - IRE

- Luxembourg Direct Tax Administration – ACD

Netherlands

- Netherlands Authority for Consumers and Markets (ACM),
- Netherlands Authority for the Financial Markets (AFM),
- Netherlands Data Protection Authority (AP),
- the Dutch Central Bank (De Nederlandsche Bank N.V.),
- the Inspectorate for Health and Youth Care (IGJ) or
- the Dutch Healthcare Authority (NZa).

Romania

- National Integrity Agency

Slovakia

- Whistleblower Protection Office

Spain

- Independent Authority for the Protection of Informants (AAI)

Sweden

- Swedish Work Environment Authority is the authority with overall oversight over 30 competent authorities

All FIS Colleagues, contractors, and applicable third-parties are required to adhere to established policies, procedures, and standards. Violation of Company Policies, procedures and/or standards **MAY** result in disciplinary action up to and including termination of employment, as permitted by local law. Any suspected violation of Company Policies, procedures, or standards **SHOULD** be reported to either an FIS manager or the Ethics Office at fisethicsoffice@fisglobal.com in accordance with the Code and Company Policies. Suspected violations of the Code **MAY** also be reported, through the FIS Ethics Helpline utilizing the phone numbers within Appendix A of the Code or through the website at www.fisethics.com. Concerns raised to the Ethics Helpline can be made Anonymously where permitted under local laws. FIS does not tolerate any Retaliation against anyone who, in Good Faith, reports a suspected violation of the Code, Company Policies, or the law or who cooperates with an investigation. Colleagues also have the option of raising employee relations concerns through [TPO Support Center \(Raise a Concern, Grievance or Complaint - Employee Service Center \(service-now.com\)\)](#). Concerns related to information security can be reported using **Service Now (SNOW): Technology Service Catalog > Security Services > FIS Security Incident Reporting Form**. For urgent or critical information security incidents, please call +1.414.357.FSIRT (3747) (U.S. and International). In addition, privacy incidents can be reported through FIS & me Workplace Services > RISC Resource Center > Report a Privacy Incident.