First Data®

First Data Code of Conduct 2019

TABLE OF CONTENTS

Introduction

As Owner-Associates of First Data, we are all responsible for upholding the integrity of our company. Building and preserving the trust and credibility of our organization requires that you take personal responsibility for your actions, honor your commitments, and do the right thing. The standards set forth in this Code of Conduct (the Code) reflect the spirit by which First Data Owner-Associates should conduct themselves in their work lives.

Each of us is responsible for reading, understanding, and applying the Code of Conduct to our daily work. Complying with the Code is a condition of employment at First Data. Failure to follow its standards, or failure to report a known violation, can lead to disciplinary action up to and including termination.

The Code of Conduct is supported by the First Data Board of Directors and the entire First Data leadership team.

Commitment to Our People

Creating a culture of openness and candor – one in which we treat each other with the dignity we all deserve – supports a strong and vital First Data. Leaders have an added responsibility to lead by example. Their actions set the tone the rest of us follow.

Follow Our Code with Ethical Decisions

While no manual can replace thoughtful decision-making by the people who work here, the Code of Conduct does help promote honest and ethical conduct. It does so by helping you understand what it means to live your standards in the workplace, by discouraging wrongdoing, by guiding you in recognizing and dealing with ethical issues, and by pointing you to resources that can help address those issues.

When there is an internal investigation or audit related to the Code of Conduct, financial reporting or Owner-Associate relations, you must fully cooperate in the investigation; provide truthful, honest and complete responses; and maintain the confidentiality of the investigation.

Seek Guidance and Report Concerns

You are expected to promptly raise concerns that you have about possible violations of law, the Code of Conduct or other improper conduct. First Data has several resources available to express your concerns. They include your immediate supervisor, Human Resources, the Ethics Helpline, First Data's General Counsel's Office, First Data's Chief Compliance Officer, First Data's Ethics Officer, First Data's Data Protection Officer, and First Data's Global Privacy Office and contact information is listed at the end of this document. Concerns may be reported anonymously and will be kept confidential to the extent allowable by law. No effort will be made to identify persons who choose to remain anonymous (by withholding their name or other identifying information).

Non-Retaliation

First Data will not tolerate any adverse action against an Owner-Associate because he or she questions a First Data or business unit practice, or raises a suspected violation in good faith. Good faith means that you believe the information you provide is truthful, even if later it turns out there was a misunderstanding. First Data will take appropriate disciplinary action against anyone who retaliates or encourages others to do so because of a reported suspicion of a Code of Conduct violation.

Waivers

The Code of Conduct applies to all Owner-Associates and sets forth First Data's business conduct and values. Accordingly, waivers to the Code of Conduct would be uncommon. A waiver request for any provision of this Code for executive officers must be approved by the Board of Directors or its designated committee and will be disclosed promptly to the extent required by law. First Data recognizes that questions may arise when the Code of Conduct applies to conduct that is legal and acceptable under the circumstances. If you have any questions regarding applicability of the Code of Conduct, contact First Data's General Counsel's Office, First Data's Chief Compliance Officer, First Data's Data Protection Officer, First Data's Global Privacy Office, or other resources listed at the end of this document.

Treatment of Owner-Associates

First Data values its Owner-Associates and strives to maintain a culture where all are treated with dignity and respect. First Data is committed to providing a work environment that is free from harassment, discrimination, bullying, threatening behavior, violence, and retaliation (victimization); provides equal employment opportunities for all Owner-Associates and applicants; and is built upon a foundation of mutual respect.

You must respect and comply with employment laws wherever in the world our businesses operate, and be sensitive to actions or behaviors that may be acceptable in one culture but not another. Because we all share a responsibility to promote a respectful environment, you have a duty to report any harassment, discrimination, or bullying that you may see. You are encouraged to speak up when other's words or actions make you uncomfortable.

First Data does not tolerate sexual harassment in any form. Sexual harassment may be verbal, physical, or visual in nature and may include unwelcome sexual advances, improper touching, sexually suggestive language, requests for sexual favors or using sexual overtones as a means or condition of employment or advancement. Reports of harassment and bullying are treated seriously.

Equal Employment Opportunities

First Data does not discriminate on the basis of race, color, religion, sex (including pregnancy, childbirth or related medical conditions), gender identity/expression, national origin, ancestry, age, disability, family care status, protected veteran and military status, marital status, sexual orientation, genetic information, or any other characteristic protected by local law or regulation.

To provide equal employment and advancement opportunities to all individuals, employment decisions at First Data are based on merit, qualifications, and abilities. While the principles of this policy must be adhered to globally, they will be interpreted in accordance with relevant local legislative requirements and practices.

Diversity

Diversity and inclusion keep our business strong and successful. First Data values the people with whom we work and their many dimensions of diversity, including culture, ethnicity, color, race, sex, national origin, age, religion, marital status, sexual orientation, gender identity and/or expression, disability, veteran status, education, life experience, opinions, ideas, beliefs, and work styles.

At First Data, supporting diversity means more than simply observing legal and policy requirements. It means actively promoting community, being comfortable with differences, and recognizing that those differences are valuable. It also enhances good management practices by preventing discrimination and promoting inclusiveness.

A workplace that values diversity can provide tremendous benefits in terms of improved morale, innovative thinking, greater teamwork, and an atmosphere of mutual understanding and respect. First Data recognizes that maintaining diversity is vital not only to our success as an employer of choice, but also in meeting the demands of an increasingly diverse client base.

It is the expectation that all Owner-Associates promote and foster an inclusive work environment at all times. Deviations from such expectations will not be tolerated.

Health and Safety

As a First Data Owner-Associate, you have a right to enjoy a work environment that is safe and free from hazards. Thus, you have a duty to know and follow your facility's safety and security guidelines. You must report any accidents, injuries, and unsafe conditions to Management.

While at work, you must not be under the influence of alcohol, illegal substances, or anything that could impair your judgment. Owner-Associates who are under the influence of alcohol or drugs while on the job, pose serious safety and health risks to themselves and those that work, or come into contact with them. The distribution, possession, or sale of drugs or alcohol in the workplace also creates unacceptable risks to the safety of our operations and is strictly prohibited.

Safeguarding Personal Information

First Data is committed to maintaining the highest standards for the protection of the data privacy of its Owner-Associates. As part of that commitment, First Data has adopted an Employee Data Privacy Policy for handling Owner-Associate information.

Personal data is any information relating to an identified or identifiable person, whether or not the information by itself is enough to identify a particular person.

Manager Responsibility

The attitudes and actions of managers influence the attitudes and actions of Owner-Associates. As leaders, managers are expected to show integrity and respect in their dealings with everyone: Fellow Owner-Associates, clients, suppliers, and the community. Their words and actions must show that business results are never more important than our ethical standards. They must confirm that Owner-Associates are trained in First Data's Code of Conduct and related topics and policies. They should create a workplace where Owner-Associates can safely and freely raise questions and express concerns. Managers have the responsibility to carefully watch for indications that unethical or illegal behavior has occurred.

Compliance Training

The First Data Regulatory Compliance Training Program promotes an organizational culture that encourages ethical conduct and a commitment to compliance with the law. Our Compliance Training Policy establishes expectations of Owner-Associates and managers with respect to Regulatory Compliance Training.

Regulatory Compliance Training:

- Enables First Data Owner-Associates to have appropriate knowledge of the laws, regulations, and policies that apply to our business
- Establishes expectations for maintaining a strong control environment
- Creates awareness and provides guidance to Owner-Associates relating to First Data compliance obligations
- Provides clear and understandable information for Owner-Associates

Assigned Compliance Training is mandatory and it is expected that all training be completed by the due date.

Commitment to Our Company

Delivering value goes beyond financial performance. It means we never compromise our ethics for a financial goal. Accurate reporting and a balanced view of our financial priorities will ultimately reap great rewards.

Accurate Business Records

Business Records are the basis for managing the company's business and fulfilling our obligations to shareholders, Owner-Associates, clients, suppliers, and regulatory authorities. You must maintain business records accurately and completely. Owner-Associates must follow the company's internal controls, approved accounting practices, and all securities and reporting regulations. Where estimates and accruals are necessary in company reports and records, we support them with good, honest judgment and appropriate documentation, and must do so with honest and appropriate documentation.

Records Management

Documents and records shall be clear, concise, accurate and appropriate, and avoid exaggeration and derogatory remarks regarding other companies. Owner-Associates must not create or report information which is false or misleading. When you end your employment with First Data, all company records that are in your possession must be immediately returned to the company. Documents are to be kept and destroyed according to First Data's Global Records and Information Management Policy. Prior to any destruction, employees must take into consideration any Legal Hold they are under for any pending Legal matter. If there are any questions, employees should contact the Legal/Litigation team. When there is a pending or possible audit, government investigation, claim or litigation, you may be responsible for retaining all documents (including e-mails) related to the investigation, overriding any normal document destruction schedule. If you have questions or concerns, please seek guidance from the General Counsel's Office.

Company Assets

You are responsible for using company assets for legitimate business purposes in an effective manner and for protecting them from carelessness, damage, loss, waste, misuse, or theft.

Intellectual Property

Many of First Data's most valuable assets are not in tangible form but instead are intellectual property, which includes trademarks, service marks, patents, and copyrighted material. First Data's Intellectual Property also includes confidential, proprietary information such as trade secrets, client lists, computer software and source code, sales and profit data, and strategic or business plans (for instance, possible mergers and acquisitions). Intellectual property created at First Data or maintained by First Data is considered First Data property and any such related Intellectual Property is protected.

Since our company's continued success depends on the careful development, use, and protection of our intellectual property, you have a duty to protect it. Take care not to discuss it where others may hear. You must also be sure not to transmit it in any form, by any means, or to any recipient where unauthorized persons might receive it. Before transmitting intellectual property outside of the company, including to a consultant or contractor, obtain the approval of the General Counsel's Office.

Your obligation to preserve the confidentiality of First Data's proprietary information continues even after you are no longer an Owner-Associate of First Data.

In the course of performing your job functions, you may receive information about possible transactions with other companies or receive confidential information about other companies. This type of material is often the third party's intellectual property and is subject to the same confidentiality guidelines; you should respect their property and be careful to preserve their confidential information.

You should also respect all applicable copyright and intellectual property laws and confirm fair and proper use of others' protected intellectual property rights.

Commitment to Complying with Legal and Ethical Business Practices

Clients and partners are essential to our livelihood as a company. They trust us with vital aspects of their business and we earn that reliance by keeping our focus on doing the right things. We commit to our clients and partners that we will carry through on agreements and comply with the law.

Compliance with the Law

The fundamental obligation you owe to the communities in which you do business and to our clients and partners is to obey the law. Adhere to all applicable laws everywhere that First Data does business. There is no business excuse, no supervisory pressure, and no unwritten understanding that justifies violating the law. If you ever feel pressured to violate a law, immediately contact the General Counsel's Office, Regulatory Compliance, or the Ethics Helpline. While this requirement refers to all applicable laws and regulatory expectations, a few areas warrant special mention.

Client Privacy

First Data's Privacy Principles and Binding Corporate Rules (BCRs) express First Data's commitment to the privacy of Personal Data that First Data obtains and processes in the course of its business. "Personal Data" is any information relating to an identified or identifiable person, whether or not the information by itself is enough to identify a particular person. First Data's BCRs for controller and processor data have been approved, providing an additional level of protection. They emphasize the key role that Owner-Associates play in providing protection for the privacy of Personal Data, and set out First Data's overall approach in providing business services that may involve the handling of Personal Data. You must be committed to protecting the privacy of Personal Data that you receive or process as an Owner-Associate at First Data. Business Confidential Information is generally related to a business' operations and may include financial data, product plans, and pricing and needs to be handled in a secure manner. Collect, use, and share Personal Data and Business Confidential Information in a secure manner and in accordance with client contracts, First Data's Privacy Principles and Binding Corporate Rules and the privacy laws that apply to First Data. In addition, you must be familiar with and adhere to First Data Privacy Principles, Binding Corporate Rules, and the approval process for Data Across Borders.

First Data Privacy Principles are Set Out in the Binding Corporate Rules and Can Be Summarized as Follows:

- We process Personal Data fairly and lawfully
- We obtain Personal Data only for carrying out lawful business activities
- We limit our access to, and use of Personal Data and we do not store Personal Data longer than necessary
- We keep Personal Data up-to-date
- We implement data protection by design and default
- We transfer Personal Data only for limited purposes
- We use appropriate security safeguards
- We provide transparency, choice, and respect data subject rights as required by applicable data protection and privacy law
- We recognize a person's right to object to direct marketing by First Data
- We recognize the importance of data privacy and hold ourselves accountable to our Privacy Principles and BCRs

If you ever believe there has been a breach of these Privacy Principles, the BCRs, data protection, or privacy laws, immediately contact the Data Protection Officer, the Privacy or Security Incident Hotline, or the other resources listed at the end of this document.

Insider Trading and Tipping

You may not use confidential or proprietary information that you receive as a result of working at First Data to influence a decision to trade in First Data securities. Trading is broadly defined as the purchase or sale of securities, including stocks, options, and bonds. This prohibition also applies to using confidential or proprietary information related to other companies securities such as that of a client or supplier received as a result of your First Data employment regulations related to the protection of Material Non-Public Information (MNPI).

Violations of these rules may result in severe civil and criminal penalties to Owner-Associates individually, as well as to First Data. MNPI is defined as any non-public information about First Data that, if disclosed publicly, would likely affect the market price of First Data's securities, or is information that a reasonable investor would consider important in making a decision to purchase, sell, or hold the security. Insider trading is the prohibited activity of trading a security while possessing MNPI pertaining to the security and/or the issuer of the security. Only authorized individuals within First Data may share information publicly regarding First Data's financial position or future.

Examples of Material Non-Public Information:

- Non-public financial information, including quarterly and year-end earnings, forecasts, projections of cash-flow, revenue, sales, expenses, or other financial metrics
- Strategic business initiatives or activities, such as corporate reorganization, mergers, acquisitions, tender offers, asset purchases or sales, divestitures, recapitalizations, partnerships, joint ventures or alliances, or other significant business development
- The creation (or loss) of significant products, services, technologies, intellectual property (e.g., patents), and other proprietary information
- Obtaining (or losing) a significant or key client, contract, or supplier
- Corporate finance activities, including the offering or sale of public or private equity and/or debt securities, loans or other forms of borrowing, or financing activity
- Material corporate organizational changes, such as reorganizations and material changes to a business unit, geographic locations, key management (e.g., board members)
- Information related to material litigation or regulatory investigations

If you have any questions about MNPI, or inadvertently become aware of MNPI and are not authorized to have such information, promptly contact the General Counsel's Office.

Antitrust and fair competition laws and regulations are designed to preserve free and open competition and to promote fair business practices between companies. The antitrust laws of the United States and other countries where First Data operates are a critical element of the business environment.

Fair competition laws can be extremely complex and vary considerably from country to country. If you encounter an issue that may have antitrust implications, you should consult with your Compliance Officer or the Global Head of Antitrust Compliance.

Nevertheless, as General Guidelines, the Following Are Unacceptable Practices Under First Data's Standards:

- Formal or informal agreements with competitors, and sometimes even discussions regarding bids, contacts, prices, distributions, conditions of sale, geographic territories and any other matter which could impact the competitive environment
- Attempts at restricting a client's ability to sell a product, including telling them how much they can charge for goods or services or agreeing to sell an item or service only on the condition that they buy another
- Offering differences in pricing (especially pricing products below cost), or terminating a business relationship, except for approved business reasons. Approval may only be granted by your Compliance Officer or the General Counsel's Office

Anti-Bribery and Corruption

First Data is committed to maintaining the highest level of professional and ethical standards in the conduct of business.

Any corruption in First Data's operations harm our reputation and position of trust; exposes First Data and its Owner-Associates, officers, and directors to possible civil and criminal penalties; and jeopardizes our ability to conduct business.

The United States Foreign Corrupt Practices Act (FCPA), the UK Bribery Act, and various other similar federal, state, and international laws prohibit both government and private sector corruption. Under anti-corruption laws, First Data can be held responsible for any bribery or corruption conducted on its behalf by directors, officers, Owner-Associates, third party representatives or agents.

The First Data Anti-Bribery & Corruption Policy Prohibits Bribery and Corruption of Any Kind by or on Behalf of First Data. To Comply with Anti-Corruption Laws and First Data's Policy You Should:

- Never give or receive anything of value that could be perceived as being in exchange for an improper benefit or as a condition or expectation of providing business (quid pro quo)
- Verify whether the client or third party with whom you are conducting business is a government employee or official. Specific rules and limitations apply to providing business entertainment to government officials, and such rules vary greatly by jurisdiction.
- Follow all procedures for obtaining pre-approval, where applicable, for the giving or receiving of any gifts, entertainment, hospitality, charitable donations, or political contributions
- Follow all First Data requirements for authorization of payments and disposition of First Data assets

Report any requests for bribes or suspected corruption to the Global Head of Anti-Corruption Compliance or through the Ethics Helpline.

Gifts and Entertainment

Generally, gifts, entertainment, meals, hospitality, travel, or sponsored events (collectively, "Business Courtesies") may be offered or received in the normal course of business with First Data clients and other third parties. Such good faith Business Courtesies can serve to develop and strengthen client relationships. However, this activity requires careful consideration and should always be performed within industry standards and with the highest ethical practices. You must never accept, provide, or offer kickbacks or bribes and must always comply with local laws and regulations.

To Mitigate These Risks, You Must Adhere to the Following Requirements:

- Obtain approval from the Global Head of Anti-Corruption Compliance or designee prior to giving of receiving any gift (of any amount) to or from a government official or entity; or giving or receiving any gift over $100 USD to or from any other non-government third party
- No gifts (of any amount) may be given or received in the form of cash or cash equivalents (e.g., gift cards, checks)
- Even when giving or receiving business-related entertainment, hospitality, or gifts of nominal value, do not do so with such frequency, or in excessive amounts, as to give the appearance of impropriety or a conflict of interest

Owner-Associates must also adhere to First Data's Global Travel and Entertainment (T&E) Policy, as well as procedures established by the Office of Corporate Citizenship for giving of charitable donations and the Global Government Affairs Office for giving of political contributions on behalf of First Data.

Money Laundering and Terrorist Financing

Money laundering is a process used to conceal the proceeds of illegal activities. Protecting First Data from being used by money launderers or terrorists is the responsibility of every Owner-Associate. Any involvement in money laundering or terrorist financing activity, even if inadvertent, could result in potential civil and criminal penalties for First Data and its Owner-Associates. First Data is dedicated to complying with applicable Anti-Money Laundering (AML) and sanctions laws, rules, and regulations. Any program questions or AML inquiries may be directed to the local Money Laundering Reporting Officer, the Global AML Compliance Officer, or the Ethics Helpline.

First Data complies with the U.S. OFAC regulations, as well as applicable sanctions requirements of other countries where First Data conducts business.

First Data will not enter into business arrangements with any third party on a sanctions list or otherwise subject to a sanctions program. Where an existing business partner is subsequently found to be on a sanctions list, First Data will take immediate action in order to terminate business relations with such party. Third parties include, but are not limited to, partners, clients, vendors, Owner-Associates, and contractors.

Third Party Oversight

First Data utilizes third party service providers to support and facilitate First Data's business and operational activities and to achieve strategic goals. However, third parties may expose First Data and its clients to significant risk including financial risk, reputational risk, legal & regulatory risk, and the risk that a third party fails to deliver products or services as expected. First Data is responsible for the management of risks arising from the usage of third party service providers.

If Owner-Associates seek to enter into a relationship or contract with a third party service provider, Global Strategic Sourcing (GSS) and Third Party Risk Management (TPRM) should be engaged prior to the signing of a contract or the commencement of business activities with a third party. Additionally, Owner-Associates should work with Accounts Payable to arrange payments to third party service providers.

Conflicts of Interest

Conflicts of interest arise when you take actions or have interests that may make it difficult to perform your work objectively in the best interests of First Data. Conflicts of interest also arise when an Owner-Associate or a member of his or her family receives improper personal benefits as a result of his or her position at First Data. Owner-Associates must ensure personal business-related activities and investments do not harm First Data, including improperly taking business opportunities which benefit our company. Owner-Associates must be vigilant in identifying and disclosing situations that may result in an actual or perceived conflict of interest based upon their job function, or more broadly, with First Data overall.

The Following Are Some Examples of Where a Conflict May Arise:

- Your employment by or relationship with (e.g., board member, consultant) a competitor of First Data or another entity, including Independent Sales Organizations (ISO) or a business that involves working during your First Data work hours or using First Data facilities or equipment
- Your ownership of, investment in, or relationship with another organization or business if its activities conflict with First Data's interests or if its time demands interfere with your job responsibilities at First Data
- You or your family members' current or potential financial interest in, or relationship with, an outside business that has or is seeking a business relationship with First Data
- Taking personal opportunities for you or others to profit, or helping others to profit, from opportunities that you find through the use of First Data property or information available to you because of your employment by or relationship with First Data

It is important to remember that you are responsible for identifying instances where a personal activity or investment may constitute a conflict of interest with First Data. If you have any questions as to whether a conflict of interest exists, you should discuss it with your manager and bring it to the attention of the General Counsel's Office for additional guidance.

Fair Dealing

Always deal fairly with our clients, suppliers, competitors, and fellow Owner-Associates. Strive to provide products, services, and solutions to our customers, which help them grow their business, doing so with integrity and fairness. When First Data is a party to a contract, deal with the other party or parties honestly, fairly, in good faith and without breaking our word, so as not to destroy or injure the right of the other party or parties to receive the intended benefits of the contract.

Confidentiality

Owner-Associates must maintain the confidentiality of proprietary or confidential information entrusted to them by First Data or its clients, except when disclosure is authorized by First Data's General Counsel or First Data's Chief Compliance Officer, First Data's Data Protection Officer, or First Data's Global Privacy Office on the basis that such disclosure is required by law or an appropriate regulator. The term "proprietary" or "confidential" information includes all non-public information that might be of use to competitors or harmful to First Data or its clients if disclosed, including contracts and pricing information, marketing plans, technical specifications, and Personal Data.

Competitive Intelligence

Contact the General Counsel's Office Immediately If:

- You are presented with information that might be the confidential property of a competitor before reviewing, copying, or distributing it
- You used to work for a competitor and have information that the competitor would deem confidential, before using or talking about the information

Use only legal and ethical methods to gather competitive information. Stealing proprietary information or inducing past or present employees of other companies to disclose trade secret information is prohibited.

Commitment to Our Community, the Public, and the Government

First Data is a member of the communities in which we do business. These communities include your families, neighbors, and public governments. First Data will conduct itself as an honorable corporate citizen.

Human Rights

First Data is committed to corporate and workplace practices and principles consistent with the requirements of the Universal Declaration of Human Rights and the International Labour Conventions. This commitment includes compliance with requirements related to working conditions and provision of a safe working environment, wage and hour laws, child labor laws, non-discrimination in the workplace, rights of Owner-Associates to associate and bargain collectively, prohibition of forced and compulsory labor, maintenance of reasonable working hours, and fair remuneration and investment in staff training and development.

First Data's approach to respecting human rights consist of several core elements, including adherence to corporate policies; compliance with applicable laws and regulations; regular dialogue and engagement with our stakeholders; and contributing, directly or indirectly, to the general well-being of the communities within which we work.

Company and Personal Political Activities

First Data encourages all Owner-Associates to participate individually in the political process and respects each Owner-Associate's right to do so; however, unless there is prior approval from the General Counsel's Office, that participation must not occur on work time or in First Data facilities, and must not include the use of First Data's name or the names of business units or subsidiaries.

Political Contributions and Activities

All corporate political contributions or the use of company funds or assets for political purposes must be budgeted, legally reviewed, and approved in advance by a Vice President-level (or above) member of the Global Government Affairs Department and the General Counsel's Office. This requirement includes fundraising events such as dinners. First Data is not permitted to reimburse individual Owner-Associate contributions to any campaign. Under U.S. federal law, First Data may not use general treasury funds to make or provide contributions, payments, loans, gifts, services, facilities, or other items of value to federal campaigns, although federal law does allow contributions to federal

candidates through a political action committee. First Data has established a federal political action committee, and all contributions to and expenditures on behalf of a federal campaign are approved by the political action committee board as permitted by that board's bylaws. U.S. state laws vary, which highlights the need to have the General Counsel's Office look into whether a contribution is permissible in advance of the contribution.

Lobbying

From time to time First Data, as a responsible and engaged corporate citizen, may speak out on government issues of importance to First Data. The Global Government Affairs Department is responsible for formulating strategies in this area, as well as for hiring and registering any personnel who will be representing the company on public policy matters. If you are aware of a political issue where advocating a position on behalf of First Data may be appropriate, you must obtain approval from the Global Government Affairs Department before contacting a government official, publicly speaking out on such political issue, or retaining a representative to speak on First Data's behalf.

Environment

First Data is committed to conducting business in an environmentally sensitive manner. We must meet or exceed all environmental laws and regulations that govern our business. Make sure that the decisions you make on behalf of First Data reflect this commitment.

Communications with the Community

The Corporate Communications and Investor Relations Departments are solely responsible and authorized to confirm that requests for news releases and other information requests are handled properly and consistently. If you are contacted for an interview or comments by the media, an analyst, or other third parties, you must communicate to the requester that you are not authorized to speak on behalf of First Data and then contact one of these two departments.

Social Media

The Digital Communications team makes sure that First Data's branded social media accounts are managed professionally. You may use social media to talk about the company on your own time, but do not claim to speak on behalf of the company or create accounts using First Data names or imagery. When you do share your opinions on social media, make it clear who you are and that you are speaking for yourself. Even positive comments about the company can have legal consequences if they are made anonymously.

Requests from Government Officials and Agencies

It is First Data's policy to cooperate with reasonable requests for information from governmental agencies, including investigations of First Data activities. First Data is, however, entitled to all the safeguards provided by law to a person being investigated, including representation by legal counsel from the beginning of the investigation. For that reason, and to make sure only authorized individuals represent First Data's position and interests, you must contact the General Counsel's Office before responding to any non-routine governmental inquiries, inspections, subpoenas, or requests.

Relationships with Auditors and Government Investigators or Regulators

First Data is committed to complying with all U.S. federal, state, and non-U.S. laws and regulations. When dealing with regulators, First Data maintains the highest level of integrity. Owner-Associates should always present First Data in the best possible light and always be welcoming and professional. All interactions with regulators should be approached with transparency, accuracy, and timeliness.

Interactions with regulators should be conducted by senior-level subject-matter experts who have the authority and ability to respond with demonstrated ownership and accountability. Regular updates and escalation to leadership and accountable parties are essential. In order to make sure that only authorized individuals represent First Data's position and interests in exam or non-exam circumstances, Regulatory Compliance contacts must be consulted in advance of any communication with regulators. Regulatory Examination protocols and support are available from First Data's Regulatory Compliance department.

Resources and Certification

Resources to Help Us Live Our Commitments

This document describes your ongoing obligations and responsibilities for complying with First Data's Code of Conduct. In addition, your supervisor, and the resources listed below are available to help you fulfill your commitment. If you have a question or concern or feel the need to raise a concern, the first place to turn is your supervisor. If you do not feel comfortable going to your supervisor, use one of the resources listed below. The important thing is that your concerns are raised. Remember that First Data does not tolerate retaliation for reporting concerns in good faith.

Resource	Contact	Other
Ethics Helpline	800.337.3366 (U.S.)	Ethics Helpline Website See website for international phone numbers
Code of Conduct Questions First Data Ethics Officer	ethics.questions@firstdata.com	
Privacy or Security Incidents Joint Security Operations Center	800.368.1000 (global)	24-hour operator Reverse charges accepted
Privacy Inquiries First Data's Data Protection Officer First Data's Global Privacy Office	 dpo@firstdata.com dataprotection@firstdata.com	
Security Inquiries	JSOC@firstdata.com	
First Data General Counsel's Office	+1.212.266.3563	
First Data Chief Compliance Officer	+1.212.266.3564	
Antitrust Inquiries	antitrustinquiries@firstdata.com	
First Data Policies	First Data Today	

Certification

First Data Owner-Associates are required to certify their understanding of the Code of Conduct and their agreement to comply with the Code. Certification is required upon commencement of employment with First Data and annually thereafter.

First Data®

FirstData.com