DISCOVER®

Doing the Right Thing

Code of Conduct and Business Ethics 2024

Discover Financial Services
Code of Conduct and Business Ethics

Foreword from the Board of Directors

Discover® employees are united by a mission to help people achieve a brighter financial future. We are committed to doing so in a manner that reflects our shared Values, is consistent with our Leadership Behaviors, and follows the principles of our Code of Conduct and Business Ethics ("Code").

Our actions—both individually and collectively—define our culture and who we are as a Company. Our Board of Directors, members of the Executive and Management Committees, as well as senior and middle management, all set the "tone at the top" for our organization. Each of us has a role to play in shaping the future of Discover, and we must continue to prioritize compliance and risk management in all we do.

Failure to adhere to our Code has the potential to reflect negatively on the entire Company. To be our best, we need everyone to understand why ethical behavior and personal integrity are indispensable for the success of our Company. Every employee must understand and adhere to Company policies and procedures, including those outlined in the Code. Whether you are new to the Company or have been here since our inception, we ask that you review our Code and commit to Doing the Right Thing in every situation and in all relationships—with consumers, business partners, regulatory agencies, the communities in which we operate, and each other.

All employees must understand the importance of complying with all laws, regulations, and Company policies and procedures applicable to Discover. This includes managing risk and escalating issues and violations of the Code appropriately. Our Code cannot address every issue or situation that may arise. For this reason, Discover managers, officers, Corporate Risk Management, and the Legal Organization are expected to guide and provide employees with answers to questions they may have regarding issues and situations that may or may not be fully explained in the Code. Importantly, all employees have a responsibility to raise concerns to their management and have multiple avenues for reporting violations of our Code, including an anonymous option via the Integrity Hotline. The Office of Ethics and Conduct, in partnership with Employee Relations, oversees the handling, investigation, and resolution of violations of our Code.

Please join us in committing to our Code of Conduct and Business Ethics as we continue to work toward our goals and help millions of people achieve brighter financial futures.

We Succeed Together.

Thank you,

The Board of Directors

J. Michael Shepherd
Director, Interim Chief Executive Officer and President

Thomas G. Maheras
Chair

Jeffrey S. Aronin
Director

Gregory C. Case
Director

Candace H. Duncan
Director

Joseph F. Eazor
Director

Kathy "Moe" Lonowski
Director

Daniela O'Leary-Gill
Director

John B. Owen
Director

David L. Rawlinson
Director

Beverley A. Sibblies
Director

Mark A. Thierer
Director

Jennifer L. Wong
Director

Our Values

The non-negotiable promise we make to our consumers, shareholders, community, regulators, business partners, & each other

D - doing the right thing
I - innovation
S - simplicity
C - collaboration
O - openness
V - volunteerism
E - enthusiasm
R - respect

Our Leadership Behaviors

How we choose to act enables us to live our values & achieve our vision

DISCOVER® Behaviors

We Play To Win

We set ambitious goals
Focusing on value and transparently tracking our progress

We take responsibility
Keeping our promises and getting it done the right way

We stay ahead
Looking out for opportunities and risks

We Get Better Every Day

We are curious
Always searching for a better way

We innovate & simplify
Through problem solving and experimentation

We develop ourselves
Expanding expertise and acting on feedback

We Succeed Together

We are good partners
Working as one to deliver the most value

We create positive energy
Building a supportive and inclusive environment where all can thrive

We develop others
Helping everyone to reach their full potential

Contents

Foreword from the Board of Directors 2
Our Values 3
Our Leadership Behaviors 4

Introduction: our Code & our Culture 6

1.1 Our commitment to ethics & values 8
1.2 Raising concerns, reporting violations, & seeking help without fear of retaliation 10
1.3 Violations of the Code 12
1.4 Questions about the Code 12
1.5 Waivers 12

We treat everyone equally & with respect 14

We are trustworthy 16

3.1 Keeping confidential/private information safe & secure 17
3.2 Using our assets sensibly 20

We are transparent & fair 23

4.1 Delivering complete & truthful statements about products & services 24
4.2 Acting on behalf of the Company 24
4.3 Creating & maintaining accurate books & records 24
4.4 How we communicate with the public 25

We conduct business legally & ethically 27

5.1 Following both the spirit & letter of the law 28
5.2 Preventing money laundering & ensuring compliance with sanctions 29
5.3 Prohibiting bribery & corruption 30
5.4 Exchanging only appropriate gifts & entertainment 31
5.5 Competing legitimately 32
5.6 Protecting our consumers 34
5.7 Avoiding conflicts of interest 35
5.8 Abstaining from unethical political contributions & lobbying activities 39

We keep our work environment safe & professional 40

6.1 Prohibiting disruptive behavior, threats, and/or acts of violence 41
6.2 Preventing distracting solicitation 42
6.3 Professional dress code & workspace expectations 43

When we see something, we Say & Do something 44

7.1 Reporting illegal, unethical, or improper conduct 45
7.2 Involving the right stakeholders in litigation or a regulatory investigation 47

Introduction: our Code & our Culture

Introduction: our Code & our Culture

At Discover, we share a proud culture of "**doing the right thing,**" which means we act ethically and with honesty and integrity in a manner consistent with our policies and procedures, as well as with all laws and regulations applicable to Discover. We perform our jobs to the highest professional and ethical standards. It also means we are accountable for our actions, our conduct, and for the results we deliver.

In addition to our Values, the Discover Leadership Behaviors are a guide on how we choose to act. They complement our Values and promote continuous improvement of our performance while strengthening our culture.

This Code applies to all employees and members of the Board of Directors of Discover Financial Services and its subsidiaries and affiliates (together, the "Company") and is intended as a guide for the professional, ethical, and legal responsibilities we share, whether on or off the Company's premises or on or off duty. It helps us make the right decisions by providing guidance and direction.

Although our Code cannot cover every possible expectation to act professionally, ethically, or legally, the Key Principles (located in the left margin of each section) provide a summary of what is discussed in greater detail in the remainder of this document, as well as in other policies, standards, and procedures of the Company.

This Code neither constitutes nor should be construed to constitute a contract of employment for a definite term and does not alter anyone's "at will" employment relationship with the Company. This means that we recognize an employee's right to resign at any time for any reason; similarly, Discover or its affiliates may terminate an employee's employment at any time, with or without cause. For employees outside of the U.S., local laws may apply to the employment relationship.

1.1 Our Commitment to Ethics & Values

This Code generally defines what is appropriate behavior, how we act collectively as a Company, and what we expect of ourselves as individuals. Our Code reinforces our core Values and helps us make ethical business decisions. Every employee is responsible for living up to the highest standards of ethical behavior, complying with the Code, and being accountable in all we do.

The Discover Chief Executive Officer, Chief Financial Officer, Chief Accounting Officer, Controller, and all other individuals performing similar functions (collectively, the "Senior Financial Officers") are also bound by a separate Code of Ethics for Senior Financial Officers, a copy of which is included as a Supplement to this Code. The provisions of the Code of Ethics for Senior Financial Officers supplement, but do not replace, this Code.

Personal integrity and ethical decision-making

The Company's reputation for integrity and excellence depends upon your conduct and actions. In addition to the responsibilities outlined in this Code, you are also responsible to:

- Learn and understand the details of policies, standards, and procedures, as well as the performance expectations, that are applicable to your role and business unit.
- Complete assigned training, including annual Code training, and certify that you have read and understand the Code. This is required of all employees and members of the Board of Directors. Anyone who fails to complete this training (or any mandatory annual training) is subject to corrective action, up to and including separation from the Company.
- Avoid conduct, whether on or off Company premises or on or off duty, that violates a law or regulation, this Code, or Company policies; negatively affects or may negatively affect the reputation of the Company; or negatively affects the work environment, another employee, a vendor's work performance, or the ability of the Company to manage its operations and employees.
- Escalate any potential (or actual) legal, regulatory, and ethical misconduct to the proper channels as detailed in the "When We See Something, We Say & Do Something" section of this Code. Escalation is required whether the conduct is a violation of the law, regulation, or a Company policy or committed by you, another employee, manager, consultant, or a supplier.
- Report if you identify a conflict between a provision of this Code and a law or regulation. You are required to report such discrepancy to the primary coverage attorney for your business function. If you do not know who your coverage attorney is, ask your management or contact the Legal Organization.

Additional responsibility of Managers & Officers

If you are a manager or an Officer (collectively, "Managers"), you play a critical role in fostering an environment where others feel comfortable raising concerns and helping to communicate to all employees under your supervision that they are expected to comply with this Code. In addition to the responsibilities previously outlined, Managers are also expected to:

- Escalate (i.e., report) concerns regarding possible violations of the Code, laws, regulations, or other policies to their managers or executive leadership and ensure that the concerns are addressed.
- Foster a work environment that encourages and supports honesty and open communication, where employees feel empowered to raise questions and concerns regarding possible violations of law, regulation, the Code, or other Company policies.
- Supervise employees' activities for compliance with applicable laws, regulations, and Company policies.
- Encourage discussion of the Code with employees and reinforce (as well as monitor) that the principles of the Code are consistently applied.
- Respond promptly and properly to employee concerns, including reporting necessary matters to Employee Relations and ensuring they are addressed promptly.
- Ensure each employee timely completes assigned training.
- Uphold the principle that employee reporting is protected against retaliation. Promptly report any potential or actual retaliation to Employee Relations or the Legal Organization.
- Take appropriate steps, in consultation with Employee Relations, the Legal Organization, Corporate Compliance, and Business Risk, to stop any misconduct and to prevent its occurrence or re-occurrence.

Managers who do not take appropriate action may subject the Company to legal or regulatory fines, even if they have delegated their supervisory responsibilities. As a result, such Managers may be held responsible for failure to supervise risk and compliance properly or take prompt action.

Relationship between the Code & other policies

In regards to the expectations provided in this Code, the Code should also be read together with applicable country-specific supplements and Company policies referred to or related to the Code. These policies can be accessed under the **Company Policies and Standards section of the Work Resources tab on our DLife site.** In addition, employees must comply with all lawful individual business unit, department, and regional policies, standards, and procedures.

Our Code is administered by the Legal Organization in partnership with Corporate Risk Management and Human Resources. The Company may amend the contents of the Code or its supplements at any time. Any substantive amendments will be communicated to you. As a general matter, when there is a conflict between this Code and any policies of your individual business unit or department, the more restrictive policy applies.

Lastly, the fact that an issue, principle, or responsibility is not specifically addressed in this Code does not relieve you of your obligation to maintain the highest professional and ethical standards under all circumstances. As mentioned previously, if you have any concern about whether your action or inaction could violate a law, regulation, or a Company policy, you have a responsibility to discuss this with your management or escalate it within any of the channels outlined in the "When We See Something, We Say & Do Something" section of this Code.

1.2 Raising concerns, reporting violations, & seeking help without fear of retaliation

What to do when you believe you or others have engaged in misconduct

All employees and Directors have a responsibility to promptly report knowledge of or information regarding any violation or suspected violation of the law, any provision of the Code, or Company policies or procedures. Always use good judgment and common sense. You are expected to do more than simply follow the applicable rules–you are required to promptly escalate potential legal, regulatory, and ethical misconduct. If something seems unethical or improper to you, it may very well be. We will accept all reports of misconduct, including reports of misconduct you believe is likely to occur.

If you observe or become aware of any such conduct–whether by another employee, manager, contractor, consultant, business partner, or supplier, or if you believe you may have violated the law, a regulation, or a Company policy–you have a responsibility to promptly discuss the concerns with your manager or escalate it within any of the channels outlined in the "When We See Something, We Say & Do Something" section of the Code.

Our Commitment to Non-Retaliation

Discover strictly prohibits intimidation or retaliation—in any form—against anyone for reporting concerns or complaints in good faith regarding misconduct. If you witness, or are asked to engage in, actions you believe are retaliatory due to an individual reporting concerns or complaints in good faith regarding misconduct, you must report it. Any retaliatory behavior will be treated as a violation of this Code, and the Company will take corrective action against individuals who engage in retaliation, up to, and including, separation from the Company.

In addition, while we encourage you to raise issues with Discover first, we appreciate that it is not always possible. Nothing in this Code prohibits or restricts you from testifying in or providing information, including confidential information, or assisting in an investigation or proceeding brought by any federal, state, or local governmental or regulatory body or official(s), or from testifying, participating in, or otherwise assisting in a proceeding relating to an alleged violation of any federal law relating to fraud or any rule or regulation of the Securities and Exchange Commission ("SEC") or any regulatory organization. Further, nothing in this Code prohibits you from reporting (and disclosing confidential information in the course of reporting) possible violations of federal, state, or local law or regulation to any governmental agency or entity, including but not limited to the Department of Justice ("DOJ"), the SEC, Congress, and any agency Inspector General, or making other disclosures that are protected under the whistleblower provisions of federal law or regulation, and you are not required to notify the Company that you have made such reports or disclosures.

Further, this Code does not (i) prohibit or restrict you from communicating, providing relevant information to, or otherwise cooperating with the Equal Employment Opportunity Commission ("EEOC") or any other federal, state, or local governmental authority with responsibility for the administration of fair employment practices laws regarding a possible violation of such laws or responding to any inquiry from such authority; (ii) prohibit you from discussing or disclosing information about unlawful acts in the workplace or at Company-sponsored activities, such as harassment, discrimination, retaliation, wage and hour violations, sexual assault, an unfair labor practice, or any other conduct that you have reason to believe is unlawful or unethical; (iii) require you to notify the Company of such communications or inquiry; or (iv) preclude you from benefiting from class-wide injunctive relief awarded in any fair employment practices case brought by any governmental agency. Nothing in this Code shall be construed to prohibit you from filing or proceeding with a charge or participating in any investigation or proceeding conducted by the EEOC, the National Labor Relations Board, or any other comparable federal, state, or local agency charged with the investigation and enforcement of any employment laws.

Confidential information and trade secrets are protected by U.S. laws and regulations, such as the U.S. Defend Trade Secrets Act; however, there are certain exceptions, such as disclosure of trade secrets under seal to a government official or to an attorney. Please note that nothing in this Code prevents such disclosure when the purpose is the reporting or investigation of a suspected violation of law or a complaint made under seal where the context is a whistleblowing or an anti-retaliation lawsuit.

1.3 Violations of the Code

To maintain the highest standards of integrity, you must comply with the Code (including supplements), Company policies, standards, procedures, and applicable laws and regulations. In addition to complying with Company policies, you are assigned to perform duties at, or for, the Company and expected to satisfactorily meet the requirements of your position. Failure to do so may result in corrective action, including disciplinary actions, up to and including immediate separation from the Company. Violations of certain laws and regulations may also result in civil and criminal penalties, which may include significant fines and imprisonment.

The Company reserves the right to investigate matters and to otherwise ensure compliance with this policy, and you are expected to cooperate fully and not interfere with personnel authorized to conduct investigations on the Company's behalf, which may include requesting that you exit the work environment in order to address an alleged violation.

1.4 Questions about the Code

If you have questions about the Code, please consult your manager. If your manager cannot answer your questions, you are expected to contact Human Resources, Corporate Risk Management, or the Legal Organization.

Before you act, you should ask yourself the questions on the following page. If any answers are "Yes," you should not proceed and should seek additional guidance as detailed in the "When We See Something, We Say & Do Something" section of this document.

1.5 Waivers

Any waiver of this Code for executive officers or directors may be granted only in exceptional circumstances by the Company's Board of Directors, or an authorized committee thereof, and will be promptly disclosed to the Company's shareholders if required by the rules of either the Securities and Exchange Commission or the New York Stock Exchange.

Before you act

Is this (or could this be) prohibited by the Code or other Company policies?

Does this violate the Company's core Values or Discover Behaviors?

Is this illegal, or could this be illegal?

Would this cause loss or harm to the Company, shareholders, customers, business partners, employees, or suppliers?

Would it be of concern if somebody were to see this reported in the news or social media?

We provide everyone with equal employment opportunities & treat them with dignity & respect

Key Principle:

Treat all individuals equally and with respect; do not discriminate or harass anyone. Ensure relationships in the workplace (in-office or remote/virtual) are business-like and free of discrimination, including racism, biased or prejudicial behavior, harassment, violence, bullying, or unfair treatment.

Q

Should I report that my manager has not been treating all of our team members the same (e.g., favoritism to some)?

A

Yes, if you feel your manager is not treating team members equally, you should report this to Employee Relations. If Employee Relations is unavailable or the circumstances make such contact impracticable, you can make an anonymous report through the Integrity Hotline.

We treat everyone equally & with respect

In support of our **Equal Employment Opportunity** policies, the Company is committed to fostering and maintaining a work environment in which all individuals are treated with dignity and respect. It is the Company's policy and your responsibility to ensure everyone is offered equal employment-related opportunities without discrimination or harassment on the basis of race, color, religion, sex, sexual orientation, gender identity, pregnancy, national origin, age, marital status, disability status, protected veteran status, genetic information, or any other characteristics protected by federal, state, or local law. The Company expects all relationships among persons in the workplace to be business-like and free of bias, favoritism, harassment, prejudice, discrimination, violence, and bullying.

To enforce our commitment to this principle, we will not tolerate misconduct (including discrimination, harassment, retaliation, or other forms of unprofessional behavior), whether it is conducted verbally or physically (including via written communication). Such behavior, even if not unlawful, will be considered a violation of this Code and subject you to corrective action, up to and including separation from the Company.

There are several ways you can report knowledge of or information regarding any violation or suspected violation of the law, any provisions of the Code, or other Company policies or procedures, as described further in the "When We See Something, We Say & Do Something" section of the Code.

We are trustworthy

We are trustworthy

3.1 Keeping confidential/private information safe & secure

Proprietary, private, and confidential information generated and gathered as part of performing work for the Company is a valuable information asset. Protecting private and confidential information is critical to the Company's reputation for integrity and its relationship with its consumers, business partners, and employees, and is an important component of compliance with laws and regulations governing the financial services industry. All confidential information, regardless of its form, format, or medium, must be protected from the time of its creation or receipt until its appropriate disposal. Unauthorized access, use, distribution, or disposal of confidential information violates Company policy and could be illegal.

Confidential (or non-public information) can be defined as information that you learn, create, or develop in the course of your employment with the Company where there is an expectation of confidentiality. It includes information that is not generally known to the public about the Company, our consumers, employees, and/or other parties with which the Company has a relationship. It includes personal information that identifies individuals, including, but not limited to, name, address, email address, phone number, Social Security number, account numbers, and information belonging to third parties. If an individual has applied for, currently has, or once had an account with the Company (e.g., credit card, deposit product, etc.), this is also considered to be confidential information.

Additionally, you are not to store confidential information, including, but not limited to, pictures, electronic images, or other copies of confidential information on personal devices (unless the confidential information is stored and secured using Company-mandated physical and electronic methods and with the appropriate pre-approvals according to the **Acceptable Use Policy**). You must only access information that you are authorized to use to perform your responsibilities on behalf of the Company.

For further guidance on your responsibilities around confidential information, reference the Company's **Information Security Policy**, **Acceptable Use Policy**, **Privacy Policy**, **Human Resources Global Data Protection Policy**, and all other **related policies, standards, and guidelines.** In addition, you are responsible for following any other applicable policies and pre-clearance procedures of your business unit or department.

Safeguarding documents

All of us have a responsibility to handle Company records and information assets with care and maintain them according to the law, regulation, and Company policies. You should familiarize yourself with the Company's **Records and Information Management Policy**, **Data Classification & Handling Information Security Standard,** and all other **related standards and applicable retention schedules.**

Key Principles:

- Protect and secure Company, consumer, business partner, and employee information generated (or gathered) by the Company. Avoid unauthorized use, distribution, or disposal of confidential information.
- Use Company systems and information appropriately for Company business purposes only, and not for personal use, anything unrelated to your job responsibilities, or contrary to a policy.

Q

I am working on an important document, and I need to work at home to get it done. Can I email the document to my personal email address and save it to my home computer so I do not need to bring my laptop home?

A

No. Pursuant to the **Information Security Policy** and **Acceptable Use Policy,** you are prohibited from sending Company information to personal email accounts, including your own personal email account, without prior authorization. You should use a Company-issued laptop, approved Bring Your Own Device ("BYOD"), or log in to the Discover secure system using your remote access token when working remotely.

Q

A former employee asked me to send her a copy of a presentation that she worked on before she left. May I send it to her?

A

No. This presentation is Company property, and you cannot release it outside the Company—not even to the person who created it.

Q

A number of years ago, I was contacted by the Legal Organization regarding some documents I had that were subject to a Legal Hold. I am cleaning out my files; do I need to keep these documents?

A

You must retain all documents that are under a Legal Hold notice until the Legal Organization instructs that they no longer need to be retained. Questions regarding legal hold retention can be directed to the Legal Organization.

To support our responsibilities, you are to retain originals of documents (hard copy and electronic) that your business unit or department policy requires to be retained, in the manner specified by the policy or approved retention schedules applicable to your business unit. Any notice from the Legal Organization to hold documents or records (i.e., "Legal Hold") must be complied with as requested.

As a general note, if you become aware of any actual, threatened, or reasonably anticipated investigation, subpoena, warrant, court order, lawsuit, administrative proceeding, or regulatory inquiry for which a Legal Hold has not been issued, you are to notify the Legal Organization immediately.

Treatment of privileged communications & documents

All communications and documents seeking or providing legal advice and prepared for, or in anticipation of, litigation should be treated as confidential and subject to the Company's attorney-client and work-product privileges. This includes communications with and documents created for/by the Legal Organization or the Company's outside counsel.

Such information and documents should only be communicated within the Company at the direction of the Legal Organization and on a strict need-to-know basis, subject to the following two exceptions:

(1) The Company's Board of Directors; and

(2) Bank Regulators.

For the Company's Board of Directors, privileged information can be shared directly with the Board without waiving the attorney-client and work-product privileges. As to Banking Regulators, a federal statute, 12 U.S.C. § 1828(x), permits the sharing of privileged information with Bank Regulators without waiving the privilege. Privilege should not prevent employees from raising issues, including issues related to ethics and compliance, with the Company's Board of Directors or Bank Regulators. Other than these two exceptions, you should not disclose privileged information to anyone outside of the Company unless specifically approved to do so in advance by the Legal Organization. Absent prior approval by the Legal Organization, only the Company's senior officers, in consultation with the Chief Legal Officer, have the authority to waive the Company's attorney-client or work-product privileges.

In addition, you have a responsibility to mark all documents that are prepared for (or at the direction of) the Legal Organization or the Company's outside counsel as "Privileged & Confidential—Prepared at the Request of Counsel." Note, however, that marking documents "Privileged" or "Confidential" does not necessarily provide legal protection from disclosure to a regulatory authority or a litigation adversary unless the document satisfies the legal requirements for the applicable privilege (including appropriate limited sharing and the related purpose for such documents), as recognized in the relevant jurisdiction.

It is also important to keep in mind that documents are not protected from disclosure merely because the author copies someone in the Legal Organization, or because the author believes the documents are personal and private. Documents that are not prepared for (or at the

direction of) the Legal Organization or the Company's outside counsel should be treated in a manner consistent with the applicable **Data Classification & Handling Information Security Standard.**

Regardless of whether any particular document is privileged, employees are still required to comply with the **Issue Management Standard.** Employees should also escalate issues to Senior Management, Corporate Risk Management, and the Board, as they believe is necessary and appropriate. If employees have a question about privilege in connection with an issue that they believe should be escalated, they should promptly consult the Chief Legal Officer or someone on the Litigation team of the Legal Organization.

Confidential Supervisory Information

Information requested by or provided to regulatory agency supervisory staff, including examination dates, and internal institution documents addressing supervisory matters, are considered Confidential Supervisory Information ("CSI"). You may not disclose CSI to anyone outside of the Company without express written consent from the Legal Organization and the regulator to whom the CSI belongs. Never remove CSI from Company premises. There are very limited exceptions for certain officers, directors, and staff only to the extent the CSI is relevant to perform assigned job duties, for legal counsel, and certain contractors or service providers.

If an employee or Board member must access confidential and/or proprietary information, including CSI, remotely for business purposes, then such access must be solely through a secure Company-provided platform (e.g., approved VPN).

Q

I overheard two members of senior management talking in the hallway about how the Company's write-offs are going to be higher than expected. Can I share that information with my roommate?

A

No. You have an obligation to protect the Company's confidential information that is not generally known to the public.

Protecting inside information

Misuse of non-public information erodes the Company's trustworthiness and places our business and reputation at risk. While working for the Company, you may become aware of material, non-public information about the Company or another entity. Material, non-public information (also known as "inside information") is information that may have an impact on the price of common stock or another financial instrument the Company, another company, or an investor would be likely to consider important in making an investment decision. Information becomes public when it has been effectively disclosed to the public, and a reasonable waiting period has passed to allow the information to be absorbed by the marketplace.

Keeping that in mind, buying or selling securities of the Company while you possess material, non-public information or encouraging others to do so (otherwise known as "insider trading") is a criminal offense and is prohibited by the Company. Such an offense is considered a violation of this Code and may lead to disciplinary action, up to and including your separation from the Company, as well as civil and criminal penalties. In particular, this applies to stocks, bonds, or any other securities of the Company, as well as derivatives thereof. You may be subject to additional requirements and restrictions on your personal trading due to your job responsibilities and will be notified of such requirements and restrictions, if applicable.

Q

I'm taking PTO next month, and I want another team member to respond to my email while I'm out. Is it okay to give the team member my passwords?

A

No, you should never share your password with anyone, including your team members. Your password is confidential and should remain so. Use your out-of-office message to alert people you are out of the office and direct them to a colleague for help while you are out.

Note, too, that there may be similar insider trading restrictions on information about third parties (such as merchants or suppliers) that is learned in the course of working at the Company.

It is also prohibited to disclose material, non-public information about the Company or other publicly traded companies (including the Company's vendors, suppliers, and customers) to others when that information is obtained in the course of employment with the Company or the performance of services on behalf of the Company before its public disclosure and dissemination by the Company or such other respective company.

If clarification is needed about material, non-public information and trading restrictions, contact the Legal Organization prior to conducting any transactions in Company securities. Additional details about trading in Company securities can be found in the **Insider Trading Policy**.

3.2 Using our assets sensibly

Q

Can I load tax preparation software on my Company laptop to prepare my tax return and remove the software immediately after I am finished?

A

No. Personal software on the Company's computers threatens the security and integrity of the Company's assets.

Information Assets, Computer Resources, and Corporate funds (together "assets") are the property of the Company and should be used for Company business only. Limited personal use of computer assets may be permitted as long as it does not interfere with your daily work and follows all Company policies. You are prohibited from accessing Company-owned Information Assets that are not related to your job responsibilities. For definitions of Computer Resources and Information Assets, see below. For additional guidance, please review the **Acceptable Use Policy**, **Information Asset Protection Policy**, and **Corporate Expense Policy**.

- Computer Resources: Any computer or electronic resource used to maintain, transmit, download, view, post, distribute, or otherwise access or make available Information Assets (collectively, "Computer Resources").
- Information Assets: Information owned or managed by the Company. An asset may qualify as an Information Asset regardless of its form or medium (e.g., typed, handwritten, electronically generated or stored, printed, or filmed), and regardless of how it was acquired (e.g., purchased, leased, licensed, or independently developed).

A few key reminders as it relates to conduct and using Company assets:

- Treat email and instant messages as professional written communications, and avoid colorful, careless slang, or shorthand language that might be misconstrued as unprofessional and/or hostile.
- Never send, store, or forward via email, chat, or instant messages that include any threatening, unlawful, discriminatory, harassing, defamatory, inappropriate, or violence-inciting messages or jokes.
- Never use personal external email accounts (e.g., external Outlook accounts, Gmail), unapproved personal social media accounts, or external instant messaging to conduct Company business.
- Never share your passwords or passcodes.
- Understand and comply with all Company information security policies and standards as well as all applicable laws.
- Do not download, store, load, operate, or execute any unauthorized software onto any Company Computer Resources.
- Return all Company equipment and property promptly upon your separation from the Company.

Lastly, in the event you suspect any misuse or theft of any Company assets, you must immediately alert the Security & Intelligence Operations Center ("SIOC").

Monitoring communications

To ensure both the Company and all employees are safe and sensibly using our assets, it is important to note that your communications using the Company's Computer Resources are not private, and by using such resources, including remote access solutions, you consent to the monitoring of your communications to the extent permitted by law. This monitoring includes your use of Company networks to access the internet from personal devices. In most jurisdictions, electronic communications (including attachments) are retained by the Company and may be produced to regulators and other third parties.

The Company may monitor, record, and review the following (subject to applicable law):

- All written and electronic communications that personnel send or receive at work or while using the Company's Computer Resources, including email, internet access (for example, secure internet websites), instant messages, voicemail, third-party systems, envelopes, packages, or messages marked "Personal and Confidential."
- All conversations on Company communication channels, such as telephone and Voice Over Internet Protocol ("VOIP").
- All communications regarding the Company on social media sites, including those written off duty, using personal equipment, and using anonymous postings and blogs. Please review the **Social Media Risk Management Policy** and the **Social Media Employee Use Standard** for more information.

Q

I heard my email and internet access could be monitored. Is that true?

A

Yes. It is true that the Company may monitor communications through Company systems, networks, and equipment for compliance with Company policy. The guidelines for acceptable internet usage, including access to your personal email accounts, may allow for "limited" personal use, depending on your job function.

Protecting intellectual property

The Company prides itself on creating, developing, and marketing new and innovative products, services, and ideas. Therefore, the Company needs to protect its intellectual property rights in such products, services, or ideas created by its employees.

As a condition of your employment, you are bound by the **Proprietary Rights Supplement**, which sets forth additional details on the Company's intellectual property rights. Specifically, the Company owns all intellectual property that you create or develop while employed by the Company:

- While using equipment, supplies, facilities, confidential information (including trade secrets), Information Assets, Computer Resources, or other resources of the Company.
- Resulting from work performed by you for the Company.
- Relating to the Company's business, anticipated business, or actual or anticipated research or development.

You also have an obligation to disclose to the Company all such intellectual property you create. The **Proprietary Rights Supplement** is contractually enforceable between you and the Company.

Preventing fraud

We put trust in our Company to protect employees and our consumers from fraud. It is our aim and responsibility as employees of the Company to effectively identify, assess, monitor, manage, mitigate, and ultimately prevent fraud. The **Enterprise Fraud Risk Management Policy** outlines the requirements for employees if fraud is suspected or identified. Fraud is defined as intentionally providing a false representation of a material fact, knowingly deceiving another, or deliberately withholding information for personal or financial gain.

Like any other form of misconduct, in the event that the Company becomes aware of actual or suspected fraud, the Company reserves the right to investigate such activity, monitor, collect evidence, take immediate action as appropriate, and cooperate with legal authorities and third parties in investigating any actual or suspected fraud. Conducting fraud is a violation of this Code, and all offenders will be prosecuted. The Company will work with legal authorities to assist in investigations, as required.

At any point, if you suspect or identify potential fraud by Company personnel or a Board member of the Company, you should discuss this with your management or escalate it within any of the channels outlined in the "When We See Something, We Say & Do Something" section of this document.

We are transparent & fair

Key Principles:

- Protect the Company's reputation and deal fairly with consumers, consultants, suppliers, business partners, employees, and competitors. Never take advantage through manipulation, concealment, abuse of privileged information, or misrepresentation of facts.
- Do not trade, encourage others to trade, or recommend securities or other financial instruments based on material, non-public ("inside") information obtained through your job responsibilities.
- Maintain accurate books and records, and be candid in your communications with the public. Ensure all business transactions are recorded accurately and in a timely manner.

We are transparent & fair

The Company seeks to outperform its competition fairly and honestly through superior performance. You are expected to protect the Company's reputation by dealing fairly with consumers, suppliers, and competitors. You are never to take advantage of anyone through manipulation, concealment, abuse of privileged information, or misrepresentation of facts.

4.1 Delivering complete & truthful statements about products & services

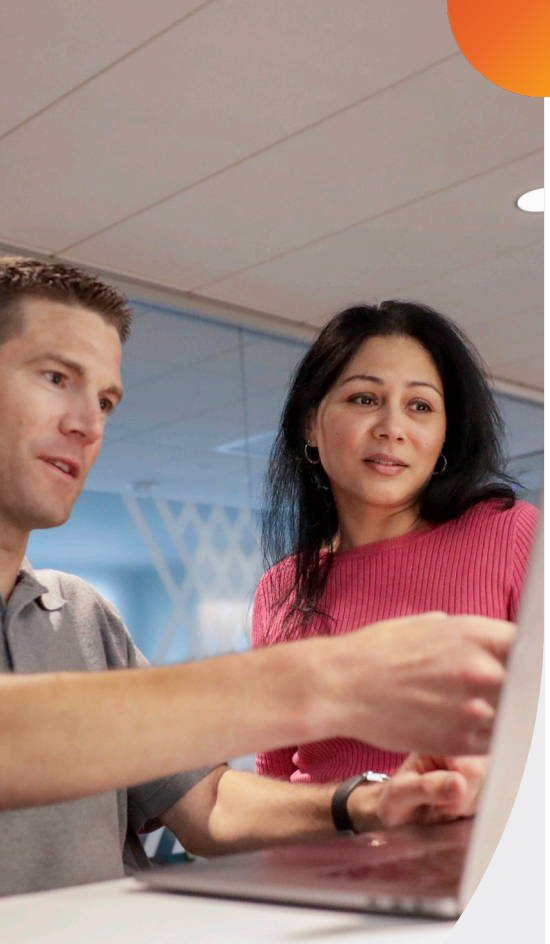
You are expected to make complete and truthful claims about our products and services. Making false or misleading statements about our products or services, or those of our competitors, violates the Code and the Company's commitment to fair dealing and could potentially violate the law. If you are unsure of the proper response to a consumer inquiry regarding a product or service, you must seek assistance from your management and/or your Business Risk office.

4.2 Acting on behalf of the Company

You are not to commit the Company to any obligations unless you have the authority to do so, nor may you commit the Company beyond the scope of your authority. Prior to hiring a lawyer or law firm on behalf of the Company, you must obtain clearance from the Legal Organization.

4.3 Creating & maintaining accurate books & records

Maintaining accurate and complete books and records is not only a requirement of the Company and the Code, but also vital for us to be able to measure our successes. Every business transaction undertaken by the Company must be recorded on its books accurately and in a timely manner. When providing information for these documents, you are responsible for being candid and accurate and will be held responsible for any false or misleading entries made.



4.4 How we communicate with the public

Fair Disclosures

The Company is committed to providing timely, transparent, consistent, accurate, and complete financial and other information to the investment community and the Company's shareholders on a nonselective basis. To the extent that you are involved in the preparation of materials for dissemination to the public, you must make sure that the information is accurate and complete in all material aspects. In particular, the Company's senior financial officers and executive officers must provide accurate, complete, fair, timely, and understandable disclosures.

In addition, only specifically designated individuals are authorized to speak on behalf of the Company. For additional guidance, refer to the Company's **Regulation FD (Fair Disclosure) Policy.** Consult your business unit, department, or regional policy for standards that apply to verbal and written communications with the public, as well as the circumstances under which communications must be reviewed by the Legal Organization and others. If you become aware of a materially inaccurate or misleading statement in a public communication, you are expected to promptly report it to the Chief Legal Officer, Chief Audit Executive, or Chief Risk Officer. Alternatively, you may always report such inaccurate or misleading statements via the Integrity Hotline.

External speaking engagements

The Company interacts with third parties (suppliers, trade associations, etc.) in a variety of ways. Often, these relationships provide us the opportunity to share our experiences and expertise through an external speaking engagement. If you are contacted and/or interested in taking part in an external speaking event (i.e., conference speaker, panelist, online webinar, podcast, analyst event, etc.), prior to engaging, you must take the following steps:

- Review and ensure you comply with the **Supplier Endorsement Policy**.
- Review the total cost and time involved.
- Obtain manager approval.
- Submit the planned presentation and speaker release form (if required) to your department coverage attorney and obtain the required approval for both, if applicable.
- Confirm with conference organizers if the event is open to the media and if the media will attend.
- Forward the presentation to Corporate Communications for additional guidance.

Q

If a local newspaper contacts me because they want to write a story on working women, can I respond?

A

You may respond on your own behalf, but not on the Company's behalf. For the reasons explained on the right, only designated individuals within Discover may speak on behalf of the Company. Therefore, if the story requires that someone speak on behalf of Discover, refer the newspaper representative to Corporate Communications.

Communications with the media

The Company maintains regular contact with the media as a means of communicating Company information to external audiences. Corporate Communications designates certain individuals who may speak on behalf of the Company as official spokespersons. If you have been designated as one of these spokespersons, you will receive notice of this designation by the Corporate Communications department.

Before responding to media inquiries, consult Corporate Communications. We also encourage you to refer to the Company's **Media Relations Policy** for additional guidance.

Communications via social media

The Company understands that employees use social media platforms (e.g., networks, blogs, and forums). With the use of social media comes a responsibility that is important for you, as an employee of Discover, to understand and follow.

All employees should be aware that anything they communicate about their work or the Company via social media can affect the Company's reputation and its relationships with consumers, shareholders, regulators, other important affiliates, and members of the public. Just as with traditional media (e.g., newspapers, radio, and television), the Company must effectively manage its corporate reputation online. For this reason, only designated individuals within the Company may speak on behalf of the Company via social media platforms.

Q

I want to blog about financial services on my own computer after work. I will post without reference to the Company. Can I do this?

A

Yes, but remember to speak only for yourself. Do not represent yourself as a spokesperson for Discover. If Discover is the subject of the content you are creating, be clear and open about the fact that you are an employee of Discover and that your views do not represent the views of Discover, fellow employees, consumers, suppliers, or other people who work for Discover.

The Company requires that all employees conduct their social media communications in accordance with the **Social Media Risk Management Policy,** the **Social Media Employee Use Standard,** and other policies/standards related to employee conduct. A few key reminders to be aware of as you engage in social media include:

- You are expected to avoid any conduct that may discredit our Company, either directly or by association.
- When you use social media, you are responsible for your actions; you should never post inappropriate/unprofessional content towards other individuals, including members of the public, that is inconsistent with this Code and other Company policies.
- You may not disclose confidential information, and you may not use copyrights, trademarks, or any intellectual property rights of a third party without their permission.
- If you speak about the Company, you must always disclose the fact that you are an employee of the Company and that your views do not represent the views of the Company.
- Use good judgment prior to posting on social media. Remember our Values and Discover Behaviors before posting and the impact that your post may have on the Company's reputation.

For additional guidance, please refer to the **Social Media Risk Management Policy** as well as the **Social Media Employee Use Standard.**

We conduct business legally & ethically

Key Principles:

- Understand the laws and regulations applicable to your job, comply with both the letter and the spirit of the law, and avoid actual or perceived misconduct.
- Avoid any investment, activity, interest, or relationship outside the Company that appears to (or could) compromise your judgment or interfere with your job responsibilities. Never engage in conduct that compromises the Company's interest or take personal advantage of your position or authority with the Company.
- Do not accept/give gifts greater than that of nominal value from/to any person or organization with which the Company has a current (or potential) business relationship. Avoid misconduct, the appearance of misconduct, or creating an inappropriate expectation or obligation on the part of the recipient.

We conduct business legally & ethically

5.1 Following both the spirit & letter of the law

The banking industry is highly regulated, and we must comply with numerous laws, rules, and regulations in jurisdictions at both the federal and state levels. As a financial services company with multiple operational subsidiaries and affiliates, we are subject to comprehensive, consolidated supervision and regulation by the U.S. Securities and Exchange Commission ("SEC"), the Federal Deposit Insurance Corporation ("FDIC"), the Federal Reserve Board ("FRB"), the Department of Labor ("DOL"), the Department of Justice ("DOJ"), the Equal Employment Opportunity Commission ("EEOC"), and other federal and state law enforcement agencies.

All employees and Directors must abide by the laws and regulations impacting the financial services industry, as well as federal and state laws and regulations such as employment laws, antitrust laws, privacy laws, insider trading laws, and criminal laws governing fraud, theft, money laundering, anti-corruption, anti-bribery, embezzlement, conversion, and conflicts of interest. Improper and/or wrongful actions or inaction by employees or Directors, which could subject the Company to civil or criminal liability or jeopardize the Company's regulatory compliance efforts, are prohibited and may subject the person to corrective action, including immediate separation from the Company. Additionally, alleged violations of laws applicable to the Company's business may be reported to the appropriate authorities for individual prosecution. The Company expects you to be knowledgeable about—and comply with—the letter and spirit of laws applicable to your job responsibilities.

If you are unsure about the legality or integrity of a particular course of action, you are expected to seek the advice of your management, the Legal Organization, Corporate Compliance, Internal Audit, or Business Risk. Any improper or illegal acts committed (or known about) during your employment are treated as misconduct and a violation of this Code.

5.2 Preventing money laundering & ensuring compliance with sanctions

The Discover Financial Services **Anti-Money Laundering, Counter-Terrorist Financing, and Sanctions Compliance Policy (the "AML Policy")** requires you to comply fully with all applicable anti-money laundering and anti-terrorism laws and regulations as well as all applicable economic and trade sanctions ("Sanctions Programs") administered and enforced by the U.S. Department of the Treasury's Office of Foreign Assets Control and those of equivalent authority in non-U.S. jurisdictions (e.g., the Office of the Superintendent of Financial Institutions in Canada).

To add further context, Sanctions Programs restrict trade and other economic activity with designated governments, individuals (e.g., suspected terrorists and narcotics traffickers), and entities, as well as with individuals and entities that are located in, or are nationals or agents of, particular countries. For further information, see the **AML Policy**.

It is important to understand your responsibilities as they relate to this topic. In summary, you must not participate, assist in, or turn a blind eye to money laundering, terrorist financing, or any transaction in violation of Sanctions Programs. Additionally, you are required to:

- Follow the Company's and your business unit's policies and procedures designed to prevent money laundering and terrorist financing and to detect possible transactions that may violate Sanctions Programs, including those procedures relating to obtaining and, in some cases, verifying information of prospective consumers and business partners.
- Be alert and refer to your manager or Corporate Compliance (for referral to AML Compliance within Corporate Risk Management) questionable or unusual activity about a consumer, the source of their funds, or their transactions.
- Refer any money laundering, terrorist financing, or Sanctions Programs inquiries to AML Compliance within Corporate Risk Management in accordance with your business unit's procedures.

Any involvement in money laundering activity or transactions is in violation of the Sanctions Programs and this Code.

5.3 Prohibiting bribery & corruption

The Company prohibits corruption in all forms and has zero tolerance for it in our business and by those with whom we do business. It is your responsibility not to make, offer, promise, authorize, demand, solicit, or accept a bribe.

Most countries in which the Company does business have laws and regulations that:

- Prohibit corruption of government officials and/or private-sector parties [i.e., Foreign Corrupt Practices Act ("FCPA"), UK Bribery Act 2010 (the "Bribery Act"), etc.].
- Prohibit soliciting or accepting anything of value from any third party with whom the Company does or contemplates doing business (the "Bank Bribery Act").

The Company has created an Anti-Bribery and Anti-Corruption (ABAC) Program to ensure compliance with all applicable bribery and corruption laws. ABAC Program requirements can be found in the Company's **Anti-Bribery and Anti-Corruption (ABAC) Policy,** and it is your responsibility to know and comply with those requirements.

The Company may be held liable under such ABAC laws not only for actions taken by you, but also for actions taken by external parties (e.g., conducting business on behalf of the Company). Whenever you engage an external party, you are responsible for ensuring their actions comply with the Company's ABAC Policy. The ABAC Policy details ABAC due diligence requirements and your responsibilities prior to engaging an external party. ABAC due diligence may also be appropriate with respect to certain joint ventures, mergers and acquisitions, and other similar investment activities.

In support of our efforts to prevent bribery and corruption, the Company's ABAC Program imposes:

- Strict limitations when you provide anything of value to or receive anything of value from an external party. If the recipient is affiliated with a foreign government (including employees of entities owned and/or controlled by non-U.S. governments), Compliance preapproval may be required (see the **ABAC Policy** and the Company's **Corporate Expense Policy** for specific requirements).
- Restrictions on the use of Company funds to finance contributions to, or events for, foreign political parties or candidates (see the ABAC Policy for specific requirements).
- Requirements that you maintain accurate books and records in support of the Company's compliance with the FCPA. It is expected that all business expenses you incur will be properly authorized and accurate details of the transaction recorded in the books and records of the relevant Company entity.
- Restrictions when you utilize company funds as charitable contributions, for corporate sponsorships, and to host meetings and events attended by external parties (see the ABAC Policy for specific requirements). Note that external parties you conduct business with are subject to ABAC laws and regulations of their home country. If you are unsure of these requirements, you should contact the ABAC team or Legal Organization.

Q

In reviewing an account, I see unusual transactions, but I am not sure if they constitute money laundering. Given my doubts, what should I do?

A

Promptly report the unusual activity in accordance with your business unit's procedures or report your concerns to your manager or Corporate Compliance (for referral to AML Compliance within Corporate Risk Management).

Q

I have an international trip planned next month with a foreign corporation to explore opportunities for a possible business relationship. I am unsure whether the corporation is owned by a foreign government. I am planning on bringing Discover-branded pens for the members of the corporation. Is that okay?

A

If you are unsure, you should reach out to the Anti-Bribery and Anti-Corruption (ABAC) team for assistance in determining the status of the foreign entity. Gifts and entertainment outside of thresholds listed in the ABAC Standard that you intend to provide to a Foreign Official, including representatives of a foreign government-owned or controlled entity, must be reviewed and preapproved prior to their provision.

If you suspect another employee or external third party is misusing funds from the Company in violation of ABAC requirements, report your suspicions through the Integrity Hotline or to the ABAC team or the Legal Organization.

5.4 Exchanging only appropriate gifts & entertainment

A small gift or reasonable entertainment can help to strengthen a business relationship but should never be used to improperly influence an external party. Gifts and entertainment, given to or received from an external party with which the Company has a business relationship, may create an appearance of impropriety or an inappropriate expectation or obligation on the part of the recipient. In general, you as well as any member of your family are prohibited from:

- Giving gifts or special favors to any person or organization with which the Company has a current or potential business relationship, unless the gifts are of Nominal Value as defined by the **Corporate Expense Policy**.
- Receiving a gift or special favor from any person or organization with which the Company has a current or potential business relationship, unless the gift is of Nominal Value.
- Offering anything of value, including business entertainment, which would negatively impact the Company's reputation, be illegal under any applicable law, or expose the Company or third party to any civil or criminal liability to any governmental authority or agency.

For further guidance, see the Company's **Corporate Expense Policy** and **ABAC Policy**, which provide additional definitions, guidance, and limitations with respect to business entertainment and gifts given by or to employees.

A few key reminders:

- If the gift is given/received for obvious family or personal relationships, where it is clear those relationships, rather than the business of the Company, are the basis for the gift, then the gift may be permissible. However, even if a gift is permissible, you should be mindful of how the gift may be perceived.
- If the gift exceeds Nominal Value or would otherwise conflict with Company policy, you are expected to decline the gift.
- In particular, you are not permitted to give or receive payment, gift, or hospitality if:
  - The gift or hospitality is associated with an illegal purpose or motive.
  - The gift or hospitality would create an appearance of impropriety.
  - The gift or hospitality is provided with the expectation or hope that an improper business advantage will be received, or to reward an improper business advantage already given.
  - The intention behind entertainment provided must always be considered. Excessive gifts or hospitality could appear

Q

During the holidays, a supplier with whom I do a lot of business sent me a gift card to take my team to dinner. Can I keep the gift?

A

No. You may not accept gifts (other than those of Nominal Value) from any organization with which the Company has a business relationship and may never accept cash or gift cards, regardless of value. You should return the gift to the supplier and explain the Company's policy.

Q

A business partner with whom I do a lot of business offered me two tickets to a national sporting event as a thank you. Can I accept the tickets?

A

No. Accepting tickets to an elaborate event could be perceived as a conflict of interest, unless preapproved as outlined in the **Corporate Expense Policy.**

- For complete guidance on receiving gifts from third parties, please refer to the **Corporate Expense Policy** or contact Corporate Compliance or the Legal Organization.

to be designed to cause an external party to engage in business based on factors other than the merits of the products or services offered.

- Gifts given to other employees should not be given with the intent to influence employment decisions, or to create a feeling of indebtedness or embarrassment.
- Before attending an elaborate event or function, you must obtain approval from Corporate Compliance.
- Providing gifts and/or entertainment to employees, agents, or officials of foreign governments or public international organizations may be subject to additional restrictions (see the ABAC Policy for specific requirements).
- Be mindful of the Bank Bribery Act, which strictly prohibits soliciting or accepting anything of value from any third party with whom the Company does, or contemplates doing, business with.

5.5 Competing legitimately

The Company is committed to honest competition in compliance with antitrust and competition laws, which prohibit:

- Price-fixing and other anti-competitive agreements like boycotts, market allocations, and bid-rigging
- Monopolization (and attempts to monopolize)
- Certain exclusive dealing and "tying" arrangements
- Deceptive acts and unfair competitive methods
- Improper participation in trade association, benchmarking, or other collaborative activities
- Overlapping boards of directors in certain cases
- Exchanges of competitively sensitive information between competitors

Q

At an industry conference, a representative from a competing company approaches me and begins to discuss the competitor's plans to increase prices. The competitor's representative then asks me about our Company's pricing plans. What should I do?

A

You should indicate to the competitor's representative, (1) to stop disclosing their pricing plans to you and (2) that you are not authorized to discuss the Company's pricing plans. You should then reach out to the Legal Organization for any additional guidance.

Accordingly, under no circumstances should you acquire or divulge information in contravention of this policy. Specifically, unless you have received the prior approval of the Legal Organization, you are not permitted to:

- Discuss with competitors any competitively sensitive matters or items such as price, product, service arrangements, or market shares.
- Divulge the identity of, or the terms on which the Company deals with, the Company's consumers or potential consumers.
- Enter any agreement obligating any consumer or merchant to deal exclusively with the Company or not to deal with a competitor.
- Enter any agreement with a third party that involves pricing restrictions, restrictions on hiring, or wage setting.
- Participate in any unsanctioned or unapproved trade association, information-sharing, or benchmarking activity that involves interactions with competitors.

If you find yourself in any situation that could involve any of the above circumstances, you should immediately cease your participation.

For further guidance about any antitrust or trade regulation issue, you should contact the Legal Organization.

Q

I observed a colleague reviewing the credit reports of his friends and family. Is that appropriate?

A

Only specific employees are authorized to access credit reports, and even those employees may only access credit reports for specific business reasons. You should report this inappropriate action to your management, as it violates Company policies and may be harmful to the Company's reputation.

5.6 Protecting our consumers

The Company has a strong commitment to making financial services available to consumers and prospective consumers on a fair and consistent basis. With that, similar to the expectations the Company seeks around how we treat each other, you are required to also treat all consumers equally and with respect in the way we conduct business.

Furthermore, this commitment means that activities are conducted in a manner consistent with applicable fair and responsible banking laws and regulations and the standards outlined in the **Fair and Responsible Banking Policy**.

All Discover products and services are to be offered and extended following these standards:

- Serving any qualified applicant regardless of race, color, religion, national origin, sex (including gender identity or sexual orientation), marital status, familial status, handicap, age (provided the applicant has the legal capacity to enter into a binding contract), the fact that all or part of a consumer's or prospective consumer's income is derived from any public assistance program, or the fact that a consumer or prospective consumer has—in good faith—exercised any rights under the Consumer Credit Protection Act (each, a "prohibited basis").
- Making all Discover products (deposit and credit) and services throughout the lifecycle of the product available to consumers without discrimination on any prohibited basis.
- Encouraging all consumers (prospective or current) to complete and/or submit an application for credit or deposit product, without regard to any prohibited basis.
- Treating and servicing consumers (prospective or current) in a fair and consistent manner in all aspects of the product lifecycle.
- Assessing a consumer's ability to repay a loan in accordance with its terms, based on one or more reasonable methods appropriate to the type of loan, prior to granting credit.
- Pricing credit products and services consistent with factors that take into consideration the risk and cost of making loans, competition and marketplace strategy, and safety and soundness, and without regard to any prohibited basis.

In addition, the Company complies with federal and state laws that prohibit unfair, deceptive, or abusive acts or practices. Specifically, we are all to be committed to:

- Communicating with consumers clearly and in plain language
- Being transparent with consumers about our products and services
- Meeting all customer commitments
- Ensuring all claims are substantiated
- Monitoring complaints and taking action as necessary

- Promptly responding to any consumer complaints alleging potential fair and responsible banking concerns
- Prohibiting any unfair, deceptive, or abusive practices

Incentive Programs

The intent of the Company's incentive compensation programs is to justly reward high-performing employees. All employees are prohibited from using business and sales practices that abuse the intent and spirit of the Company's incentive programs. Any employee, including managers, who manipulates or attempts to manipulate incentive results for personal gain at the expense of customers, other employees, or Company objectives will be subject to corrective action, up to and including separation from the Company. Employees are expressly prohibited from establishing incentive plans or practices or from otherwise offering incentives of any type whatsoever, other than those specifically allowed by the Company's incentive programs. If you become aware of unethical incentive program practices, you are expected to report any such activity to Employee Relations, or you may always report it via the Integrity Hotline.

Lastly, the Fair Credit Reporting Act contains very explicit requirements and prohibitions concerning the use of and access to consumer credit reports. Access to consumer credit reports is limited to employees specifically authorized who have a permissible purpose, and who are thoroughly trained in the proper access and use of credit reports. Any questions about the use of and access to credit bureau information should be directed to the Legal Organization or Corporate Compliance.

5.7 Avoiding conflicts of interest

The way we conduct ourselves in business impacts our reputation and the trust we maintain with our consumers as well as each other. By recognizing and taking preemptive steps to prevent conflicts of interest, we are demonstrating our loyalty to the Company's integrity and our determination to "Do the right thing."

With that, you are responsible for:

- Avoiding any activities, interests, or relationships that do (or may) interfere with your ability to act in the best interest of the Company.
- Not taking personal advantage of your position or authority with the Company (e.g., approving personal lending transactions or accessing personal information or credit history for oneself or a relative).
- Not engaging in conduct that is detrimental to the Company's interests or reputation in any way.
- Identifying and managing conflicts or potential conflicts in accordance with regulatory requirements and Company policies.
- Notifying Employee Relations of all outside personal or business interests ("outside activity"), which may create a conflict of interest and request approval before engaging in any such outside activities from Employee Relations.

Q

I work full-time for Discover as a Vice President, and I have a paid part-time role consulting for a local Fin-tech company. Is this a problem?

A

Yes, this is most likely a conflict of interest. You should have a discussion with Management and escalate for further review by Employee Relations.

Once an outside activity has been assessed and deemed permissible, if the nature or scope of that business or your participation changes, you are to request an assessment (e.g., a privately held company becomes publicly traded or any change in ownership).

Lastly, you may not engage in an approved outside activity during Company hours or use Company assets to further those activities.

The following sections provide greater detail around the different types of conflicts that should be avoided. Managers who identify conflicts of interest in the business or to whom conflicts are raised by employees should manage those conflicts in accordance with Company policies and refer the conflict to Employee Relations for further review.

Potential business conflicts

A business conflict of interest may arise as a consequence of the Company's interests and its relationship with third parties. It would be considered a conflict when your interests or those of third parties do not align with the Company's overall values or best interests. Business conflicts can occur:

- Between different suppliers or third parties.
- Between suppliers, third parties, and the Company itself.
- Across different business units.

While it is not possible to describe every situation, the above examples (or of the like) must be disclosed to Employee Relations for further review and approval. Employee Relations and/or the Legal Organization are also available for additional guidance, if needed.

Outside positions

You cannot accept or hold an outside position if that position would interfere with your ability to perform work for the Company. While it is not possible to describe every situation, the following are examples of situations that may raise a conflict and therefore must be disclosed to Employee Relations:

- Taking an outside position with a company or entity that is a supplier, third party, or competitor of the Company.
- Serving as a director, trustee, officer, or affiliate in a paid or unpaid position for a for-profit corporation, other than with the Company.
- Serving as a director, trustee, officer, or affiliate of a not-for-profit or charitable organization in the financial services industry (see the **Charitable Giving Policy** for complete guidance).
- Accepting employment or compensation from any organization engaged in the business of financial services.
- Engaging in unauthorized employment elsewhere while on an approved leave of absence.

Employee Relations is available for further guidance on Outside Positions.

Business & personal opportunities

Business and personal opportunities that could (or may) impair your judgment or interfere with your responsibilities to the Company or our consumers should be avoided. If a business opportunity arises, either

Q

My sister works for a company that specializes in designing training modules for financial services corporations. Can I help her get business from Discover?

A

No. You can introduce her to the group that handles training, but you should then remove yourself from the conversation. She will have to be evaluated along with other competing suppliers and selected based on the price and quality of service. It is a conflict of interest to select a supplier purely based on a personal relationship.

because of your position with the Company or by using corporate property/information, that opportunity belongs to the Company.

In addition, the Bank Bribery Act prohibits self-dealing. Self-dealing occurs when an employee conducts business in a manner that places their interests above those of the Company. While it is not possible to describe every situation, the following are examples of situations that may raise a conflict and therefore must be disclosed to Employee Relations for review:

- Taking personal advantage of any business or investment opportunity that you find out about through your work for the Company (e.g., the purchase or sale of property, services, or other interests).
- Making any personal investment in an enterprise if the investment might (or may appear to) affect your ability to make unbiased business decisions on behalf of the Company.
- Acquiring an interest in a transaction involving the Company, a consumer, third party, or supplier (not including routine investments in publicly traded companies, mutual funds, and employee investment funds managed by the Company).
- Receiving a personal loan or guarantee of an obligation as a result of your position with the Company.
- Granting personal loans to other employees that could make, or might be perceived as making, the recipient beholden to you (over and above the need to repay the loan).
- Accepting (for personal use) any special favors, business opportunities, or purchasing goods and services not available to other persons as a result of your position with the Company and from any person or organization with which the Company has a current (or potential) business relationship.
- Seeking to engage a "relative," or their company, to provide goods or services to the Company. See **Employment Eligibility Policy** for complete guidance, including the definition of "relative."

Employee Relations is available for further guidance on Business and Personal Opportunities.

Employment of relatives

The Company permits the employment of an employee's relative under certain circumstances. If you become aware that we are considering one of your relatives for employment, those circumstances must be disclosed to Employee Relations as soon as this is known, and it will be handled in accordance with the **Employment Eligibility Policy**.

In order to avoid potential conflicts of interest, including even the appearance of favoritism, you may not supervise, work directly for, work in the same chain of command as, or make employment decisions about a relative. Additionally, relatives of employees are not to work any position in which Employee Relations believes may create an inherent or perceived conflict. For additional information related to the Company's rules regarding hiring of relatives, you should refer to the **Employment Eligibility Policy** or contact Employee Relations.

Self-Dealing

Self-dealing occurs when an employee or Director appears to put their own personal or financial interest, or the interest of immediate family members or others with whom they have a close personal or familial relationship, above the interests of our Company. All employees and Directors must avoid engaging in these activities because they are or give the appearance of a conflict of interest.

Examples of activities that our Company considers to be prohibited self-dealing are as follows:

- Personally extending credit to a Company customer or any person (other than an immediate family member) who has applied for and was denied credit by the Company.
- Representing the Company in any activity requiring the employee's judgment or discretion that affects a person or entity with which the employee has a material family, financial, or other close personal relationship.
- Signing a customer's account, acting as a customer's power of attorney, or otherwise representing customers. This prohibition does not include immediate family members.
- Accessing customer account information without a valid business need to do so. You may not use the Company's internal systems to access information regarding accounts on which you are a signatory or accounts for entities in which you have a material management ownership or personal financial interest. Never use the Company's internal systems to access information regarding accounts of immediate family members and other persons with whom you have a close personal or familial relationship, or other accounts in which you have a personal interest. Employees should use the same methods available to the Company's customers (including online, mobile banking, and ATMs) to access information regarding their personal accounts.
- Improperly influencing an employee over whom a supervisor has managerial responsibility to perform any action that would otherwise be prohibited by this Code.
- Processing bank transactions or conducting service or maintenance for your own personal accounts, the accounts of immediate family members and other persons with whom you have a close personal or familial relationship, or other accounts in which you have a personal interest or on which you are an authorized signer or have a material management, ownership or personal financial interest. Specifically, this includes, but is not limited to, opening accounts, accepting deposits, withdrawal of deposits, refunding, reversing or waiving fees, transferring funds, ordering debit or credit cards, entering loan or credit applications, approving or increasing credit lines or loans, and cashing checks. Employees must conduct transactions for their personal accounts using the same methods available to other Company customers (including online or mobile banking, ATMs or having the transaction processed by an impartial agent).

Q

A friend of mine is running for local office. Can I help her advance the campaign?

A

Yes. You must ensure that you do not use Company resources (i.e., letterhead, office space, dining facilities, supplies, computers, or copiers) to support the campaign.

5.8 Abstaining from unethical political contributions & lobbying activities

Under U.S. federal law, the Company may not contribute corporate funds or make in-kind contributions to a candidate for a federal office or to a federal political party. Similar restrictions apply in many U.S. states. In addition, there are also state and local legal restrictions on corporate or personal political contributions made to public officials whose decisions may impact companies that do business with the state.

In compliance with these laws and our **Political Contributions and Activities Policy**, you are not to do the following without clearance from Government Relations:

- Make a political contribution in the name of the Company.
- Use Company resources (or staff in the form of a delegate) in connection with any political event or political contribution.

The following explains further your responsibilities as it relates to this topic:

- If you make personal contributions, you will not be reimbursed by the Company.
- If you wish to seek political office or serve on a public board or similar public body, you must request and receive preapproval from your designated manager and the Legal Organization.

In addition, communication or interaction with any government official may be broadly defined to include legislative and regulatory lobbying, which can trigger reporting and/or registration requirements. Therefore, if you, on behalf of the Company, or anyone who could be perceived to be acting on behalf of the Company, communicate with a government official, take part in a trade association visit with a government official, or participate in a government-sponsored event, you must ensure these actions are conducted under the direction of the Company's Government Relations staff and the **Legislative and Regulatory Lobbying Policy**.

Please note that the Company's policy does not restrict the Company's right to support our Political Action Committee (Discover PAC), or the right of Discover and its employees to engage in lawful political activities.

We keep our work environment safe & professional

Key Principles:

- Maintain a safe and professional work environment free of distraction, disruption, or threatening behavior within the office or while remote/ virtual working.
- Commit to our responsibility in prohibiting forced labor and human trafficking within our business and supply chains. Report any suspicion of forced labor and/or human trafficking.

We keep our work environment safe & professional

At Discover, we are committed to providing a safe and professional work environment for the Company and our visitors. It is the Company's policy, and all of our responsibility, to expressly prohibit disruptive or threatening, intimidating behavior, or any acts or threats of "acts of violence," which involve or affect any employee, consumer, supplier, visitor, or other third party in the work environment.

6.1 Prohibiting disruptive behavior, threats, and/or acts of violence

The Company will not tolerate disruptive behavior or any threats or acts of violence against its employees, consumers, suppliers, visitors, third parties, or property by any individual on the Company's premises, or while an individual is engaged in business with or on behalf of the Company. In addition, such behavior is not to be conducted whether on or off the Company's premises or at a Company-sponsored event.

"Threats or acts of violence" could be defined as conduct against persons or property that is sufficiently severe, offensive, or threatening as to give an individual reasonable cause to believe that they or others are at risk of injury, or creates a hostile, abusive, or intimidating work environment. If you feel threatened, you should call the SIOC (24 hours) at 844-405-7462 and/or Employee Relations. If immediate assistance is needed and an individual's safety is or may be at risk, you should call 911.

The following is prohibited whenever you or non-employees (such as contractors) are conducting Company-related business, operating any Company vehicle, or are present on Company premises:

- Using, purchasing, possessing (even residual amounts), selling, manufacturing, or distributing any illegal substances or purchasing, using, or possessing legally authorized controlled substances without proper medical authorization. Additionally, manufacturing, selling, or distributing legally authorized controlled substances is prohibited at Discover.
- Being under the influence of alcohol or drugs, as defined in the Company's Drug-Free Workplace Policy.
- Consuming alcohol, except when Company management (an officer-level employee for the department) authorizes the consumption of alcohol while on premises or during a work-related function. Note: No work is to be performed, and no Company vehicle may be operated, during or after such event.

- Possession of firearms or other weapons while on Company premises, or while on Company business or at Company events, subject to applicable law; or threatening the personal safety of fellow employees, consumers, suppliers, visitors, or third parties, on or off Company premises.
- Engaging in gambling activities involving wagering/betting (risking money on the outcome of an event) while working, on Company property, or while using Company-provided equipment.
- Vandalism or theft of Company property, assets, or another's personal belongings.
- Smoking or using tobacco products (including e-cigarettes) inside the building or anywhere on Discover-owned or leased property, unless otherwise designated. For additional guidance on building usage, see the **Facilities Building Policy.**

Contact Employee Relations with any questions concerning such expectations.

Global safety efforts

At Discover, in addition to and beyond just our work environment, we are committed to enhancing our global safety efforts and prohibiting forced labor and human trafficking within our business and supply chain. If you have any reason to suspect forced labor or human trafficking is occurring either within our business or in connection with it, you are to immediately report your concerns to Employee Relations or the Integrity Hotline.

6.2 Preventing distracting solicitation

To avoid unwanted distractions, disruption of business operations, or disturbance of employees, visitors, and suppliers, you are not to solicit, distribute, and/or post any unapproved materials or requests for money on or at Company property or any area visible where (or while) work is being conducted.

If your reason to solicit, distribute, and/or post materials is in support of any of the following scenarios, prior approval would not be required:

- Supporting a Company-sponsored program or event.
- Organizing events for another employee (e.g., employee departures from a business unit, wedding showers, adoption/birth of a child, promotions, death, or mourning).
- Supporting a cause, charity, or fundraising event sponsored, funded, organized, or authorized by the Company (e.g., legal pro bono work, Employee Resource Group (ERG)-approved events, Discover Cares programs).
- Joining a group of employees for an authorized non-business purpose (e.g., recreational or volunteering).
- Participating in employment-related activities or groups, as protected by law (e.g., terms and conditions of employment).

For further context, “Solicitation” means campaigning, requesting contributions, or seeking to obtain membership in, or support for, any unapproved organization. “Distribution” or “Posting” means giving written materials (physically or electronically) such as pamphlets, posters, or petitions of any kind (“Materials”) on Company property or by using Company resources.

Any activity not referenced above, as permissible, will require advanced approval from Employee Relations and must comply with all applicable laws and Company policies.

6.3 Professional dress code & workspace expectations

Professional dress code

You should always represent the Company well and are expected to dress in a manner consistent with the **Dress Code Guidelines** retained within myHR. Beyond these specific guidelines, employees should always give primary consideration to the kind of professional interactions they expect for the day. For example, if there are “meetings” (in person or virtually) with clients, suppliers, regulators, or other third parties, employees should wear attire that reflects the professionalism of our Company.

Workspace expectations

Regardless of work location, you are expected to maintain a professional and neutral workspace that is free of anything that could be considered or interpreted as offensive and/or discriminatory via methods such as pictures or posters, including that which may be viewed in the background of a video conference call. To help avoid such issues, employees should consider using one of the video conference features that allows you to blur the background or to use an approved virtual background.

When we see something, we Say & Do something

When we see something, we Say & Do something

7.1 Reporting illegal, unethical, or improper conduct

Key Principle:

Notify appropriate parties and request action pursuant to this Code or other Company policies if you observe or become aware of any illegal, unethical, or improper conduct, litigation, or regulatory investigation relating to the Company.

If at any time you suspect your actions may have violated the law, this Code, or any of the Company's other policies or if you observe or become aware of any illegal, harassing, or discriminatory behaviors, or unethical or improper conduct by another employee, consumer, consultant, supplier, or third party relating to the Company, you are required to promptly notify one of the following:

- Your management
- Employee Relations
- Chief Legal Officer
- Chief Compliance Officer
- Chief Risk Officer
- Chief Audit Executive
- For fraud, you may also email your concerns to internalinvestigationrequests@discover.com.

Just saying something may not be enough. It's important to understand the difference between saying something to someone (e.g., a friend at work, a peer, or a manager) and actually taking action to "do" something and ensuring the matter is escalated and addressed appropriately in accordance with the Code and other Company policies, or applicable laws or regulations.

Managers have a responsibility to address employee concerns promptly. Therefore, we encourage employees to work with their managers to address issues or concerns the employee feels violated the Code or a law, regulation, or other Company policy. However, if your discussion with your manager or promptly notifying one of the above parties does not address your concern, or if you would prefer to report your concern anonymously, you may also always choose to report your concern via the Integrity Hotline (see the next section).

For additional direction, concerns regarding Executive management may also be reported in these ways:

- If it is regarding the Chief Executive Officer, any Senior Vice President, any Executive Vice President, or a member of the Board of Directors:
  - Escalate concern to the Chief Audit Executive and/or Chief Legal Officer
- If regarding the Chief Audit Executive and/or Chief Legal Officer:
  - Escalate concern to the Chairman of the DFS Board of Directors

If you would prefer to report your concerns anonymously or do not feel comfortable raising your concerns through the channels identified above, you may also always choose to report your concerns through the Integrity Hotline.

Q

I believe another employee acted illegally in relation to the Company. Should I confront the employee?

A

If you become aware of another employee's conduct that you suspect may be illegal, unethical, or improper, you must notify the appropriate channels outlined in the Code immediately to discuss your concerns. Regardless of how the report is made, the Company will not tolerate any retaliation against you for reports made in good faith.

In addition, you must promptly notify Employee Relations if you are criminally charged, indicted, or become involved as a defendant in a criminal matter (exclude minor traffic violations), are convicted, enter into a plea, settle the matter, or otherwise enter into a pretrial diversion or similar program in connection with the matter. Employee Relations and the Background Investigations team will partner to assess the information and determine whether a substantial relationship exists between any behavior that occurred and your responsibilities to the Company, or whether any unreasonable risk exists to the safety of the workplace or Company assets.

Integrity Hotline

We encourage you to report concerns related to issues such as violations of the law or if you observe or become aware of any illegal harassing/discriminatory behaviors or unethical or improper conduct by another employee, consumer, consultant, supplier, or third party relating to the Company or its reputation to any of the channels listed in the previous section.

If you feel you are unable to address or resolve a matter using any of those options or would like to report a matter anonymously, please contact the Company's **Integrity Hotline**. The Integrity Hotline is a service you can access from any location by phone or internet. You may choose to identify yourself when you make your report, or you may choose to remain anonymous.

The Integrity Hotline is available 24 hours a day, 7 days a week, and is staffed by a third-party service provider whose employees are trained to receive initial reports of potential misconduct. Reports may be made on a confidential, anonymous basis.

Employees who choose to submit an anonymous report to the Integrity Hotline should provide sufficient detail to allow the Company to conduct a thorough investigation into the matter. Additionally, individuals have the opportunity to communicate with the Discover Integrity Hotline team and provide more information as needed for the investigation. Employees submitting reports are encouraged but never required to make use of this function.

Integrity Hotline contacts:

United States, Canada, and Puerto Rico
Hotline Number: 866-714-1305
Discover.alertline.com

China, PRC - No. Region, Beijing & Vicinity
Direct Access Number: 108-888
Hotline Number: 866-714-1305
Discover.alertline.com

China, PRC - So. Region, Shanghai & Vicinity
Direct Access Number: 108-11
Hotline Number: 866-714-1305
Discover.alertline.com

Hong Kong (Hong Kong Telephone)
Direct Access Number: 800-96-1111
Hotline Number: 866-714-1305
Discover.alertline.com

Hong Kong (New World Telephone)
Direct Access Number: 800-93-2266
Hotline Number: 866-714-1305
Discover.alertline.com

India
Direct Access Number: 000-117
Hotline Number: 866-714-1305
Discover.alertline.com

France
Direct Access Number: 0800-99-1111 or 0805-701-288
Hotline Number: 866-307-9281
Discovereu.alertline.com

United Kingdom
Direct Access Number BT: 0800-89-0011
Hotline Number: 866-307-9281
Discovereu.alertline.com

Q

A government regulator contacted me to inquire about a particular disclosure on one of our solicitations. What should I do?

A

Upon contact, and prior to any response, you should immediately contact Compliance and inform them of the regulator's inquiry.

7.2 Involving the right stakeholders in litigation or a regulatory investigation

Together, we have the responsibility to provide accurate and complete information to government authorities, as well as to cooperate in Company-related litigation, internal investigations, and government inquiries. For this purpose, the Legal Organization and Compliance collaborate to manage the Company's contacts with governmental, regulatory, and administrative authorities, as well as attorneys for private litigants regarding subpoenas, investigations, inquiries, and requests.

Further, the Company maintains regulatory relationship teams for many of our key regulators. Any communications or interactions with regulators should be reported to and coordinated with a member of the appropriate regulatory examination team in Compliance. Information regarding the regulatory relationship teams is available from Compliance.

Cooperation

During litigation, an internal investigation, or a government, regulatory, or administrative examination or inquiry involving the Company, you may be asked to provide information (including documents, testimony, or statements) or meet with Company personnel, its outside counsel, or government, regulatory, or administrative authorities. You must cooperate fully with any such request. Additionally, you must comply with all Legal Holds requesting the preservation of data, documents, or other items.

If at any time you become involved in any litigation, regulatory exam, or investigation that may fall under the following categories, you must notify the Legal Organization:

- Regulatory investigation or proceeding;
- Planned lawsuit or voluntary regulatory filing in connection with a Company-related matter or business;
- Civil litigation or arbitration (excluding personal claims or family law matters that do not concern the Company); or
- Receipt of a subpoena, warrant, court order, inquiry, complaint, or request from a governmental, regulatory, or administrative agency, or a claimant, plaintiff, or outside attorney that involves, or has the potential to involve, the Company.

You may report possible violations of law or regulation to any governmental agency or entity, including but not limited to the Department of Justice, the Securities and Exchange Commission, Congress, any Fair Employment Practices agency, and any agency Inspector General, or make other disclosures that are protected under the whistleblower provisions of federal or state law or regulation. You are also not required to notify the Company that you have made such reports or disclosures. Further, as an employee of the Company, you agree to allow the Company to provide, without notice to you, information about you to the authorities in response to subpoenas, warrants, court orders, or other civil discovery requests.