BANK OF AMERICA

2023 Code of Conduct

Driving Responsible Growth

Code of Conduct: Core to how we drive Responsible Growth

To my teammates:

Every day, we work hard to drive Responsible Growth — this means growing and winning in the marketplace, focusing on the client in everything we do, managing risk well and making sure our growth is sustainable.

Our Code of Conduct guides us in how we do these things, living our values and delivering on our purpose to help make financial lives better.

To keep all of this top of mind, we are each required annually to review, acknowledge and understand our Code of Conduct. Thank you for doing so, and for upholding our ethical standards and commitment to our values in all you do every day for our clients, teammates and communities.

Brian Moynihan
Chief Executive Officer Bank of America

What would you like the power to do?®

At Bank of America, we ask the question every day of all those we serve. It is at the core of how we live our values, deliver our purpose and achieve Responsible Growth.

Our values

- Deliver together
- Act responsibly
- Realize the power of our people
- Trust the team

Our purpose

To help make financial lives better, through the power of every connection.

Responsible Growth

- We must grow and win in the market—no excuses
- We must grow with our customer-focused strategy
- We must grow within our risk framework
- We must grow in a sustainable manner

Eight lines of business

Serving the core financial needs of people, companies and institutional investors through eight lines of business

Our values

Deliver together

We believe in the importance of treating each customer, client and teammate as an individual and treating every moment as one that matters. We strive to go the distance to deliver with discipline and passion. We believe in connecting with people person-to-person with empathy and understanding. We believe everything we do for customers, clients, teammates and the communities we serve is built on a solid business foundation that delivers for shareholders.

Act responsibly

We believe that integrity and the disciplined management of risk form the foundation of our business. We are aware that our decisions and actions affect people's lives every day. We believe in making decisions that are clear, fair and grounded in the principles of shared success, responsible citizenship and community building.

Realize the power of our people

We strive to help all employees reach their full potential. We believe that diverse backgrounds and experiences make us stronger. We respect every individual and value our differences — in thought, style, cultures, ethnicity and experience.

Trust the team

We believe that the best outcomes are achieved when people work together across the entire company. We believe great teams are built on mutual trust, shared ownership and accountability. We act as one company and believe when we work together, we best meet the full needs of our customers and clients.

Our purpose

We are guided by our purpose to help make financial lives better through the power of every connection. We deliver on our purpose through a focus on Responsible Growth. By investing in the success of our employees, helping to create jobs, develop communities, foster economic mobility and address society's biggest challenges — while managing risk well and providing a return to our clients and our business — we are driving growth and ensuring our long-term success.

Our culture

Our culture comes from how we run the company every day — by acting responsibly and managing risk well — which includes our commitments to honest and ethical behavior, acting with integrity, and complying with applicable laws, rules, regulations and policies. We recognize that cultivating a strong culture is an ongoing effort, fostered day after day in both formal and informal ways. Building a unified culture requires thoughtful, purposeful action, and we do this by ensuring all of our employees — across all our lines of business and in every country and location we operate — are aligned to our purpose of making financial lives better through the power of every connection.

Driving Responsible Growth

We deliver on our purpose through a focus on Responsible Growth. By investing in the success of our employees, helping to create jobs, develop communities, foster economic mobility and address society's biggest challenges — while managing risk well and providing a return to our clients and our business — we are driving growth and ensuring our long-term success.

Human rights

Bank of America is committed to respecting human rights and demonstrating leadership in responsible workplace practices across our enterprise and in all regions where we conduct business. We aim to align our company's policies and practices with international standards. Our commitment to fair, ethical and responsible business practices, as we engage with our employees, clients, vendors and communities around the world, is embodied in our values and Code of Conduct. For additional information, please read our Human Rights Statement.

We focus on growing responsibly

Environmental, social and governance

At Bank of America, we are driving Responsible Growth with a strong focus on ESG leadership. This enables us to serve clients, deliver long-term value through sustainable results to our shareholders, and address some of society's greatest challenges. Also, our focus on ESG helps to drive opportunities and manage risks across our company, helps us define how we mobilize our capital and resources, and inform our business practices and how and when we use our voice in support of our values. Through our commitment to ESG principles, we strive to build trust and credibility as a company people want to work for, invest in and do business with.

Integrated across our eight lines of business, our ESG focus reflects our values, ensures we are holding ourselves accountable, presents tremendous business opportunity, and allows us to create shared success with our clients and communities.

We encourage our employees to be active in our communities through volunteerism, giving and being better environmental stewards. Visit HR Connect and Environmental, Social and Governance on Flagscape for more on opportunities and guidelines, including volunteer time off (for eligible employees), how to record volunteer hours, tips for being sustainable at home and at work, and how to get involved with a My Environment® chapter.

For more information:

- Environmental and Social Risk Policy Framework
- Investor Relations — Making an impact
- Investor Relations — Annual Report and Proxy Statement
- Environmental, Social and Governance Flagscape site

Our Code of Conduct

Bank of America is committed to the highest standards of ethical and professional conduct. The Code of Conduct (the "Code of Conduct" or the "Code") provides basic guidelines of business practice and professional and personal conduct that we are expected to adopt and uphold as Bank of America employees. The Code of Conduct contains the following key themes consistent with our values:

Notice to employees

Nothing in this Code prohibits or limits any employees or their counsel from initiating communications directly with, responding to any inquiry from, volunteering information to, or providing testimony before, the U. S. Securities and Exchange Commission (SEC), the Department of Justice, Financial Industry Regulatory Authority, Inc., any other self-regulatory organization or any other governmental, law enforcement, or regulatory authority, in connection with any reporting of, investigation into, or proceeding regarding suspected violations of law, and no employee is required to advise or seek permission from the company before engaging in any such activity. In connection with any such activity permitted above, employees should identify any information that is confidential and ask the government agency for confidential treatment of such information. Despite the foregoing, employees are not permitted to reveal to any third party, including any governmental, law enforcement or regulatory authority, information employee came to learn during the course of employee's employment with the company that is protected from disclosure by any applicable privilege, including but not limited to the attorney-client privilege, attorney work product doctrine and/or other applicable legal privileges. The company does not waive any applicable privileges or the right to continue to protect its privileged attorney-client information, attorney work product and other privileged information. Additionally, employees recognize that employees' ability to disclose information may be limited or prohibited by applicable law and the Company does not consent to disclosures that would violate applicable law. Such applicable laws include, without limitation, laws and regulations restricting disclosure of confidential supervisory information or disclosures subject to the Bank Secrecy Act (31 U.S.C. §§ 5311-5330), including information that would reveal the existence or contemplated filing of a suspicious activity report.

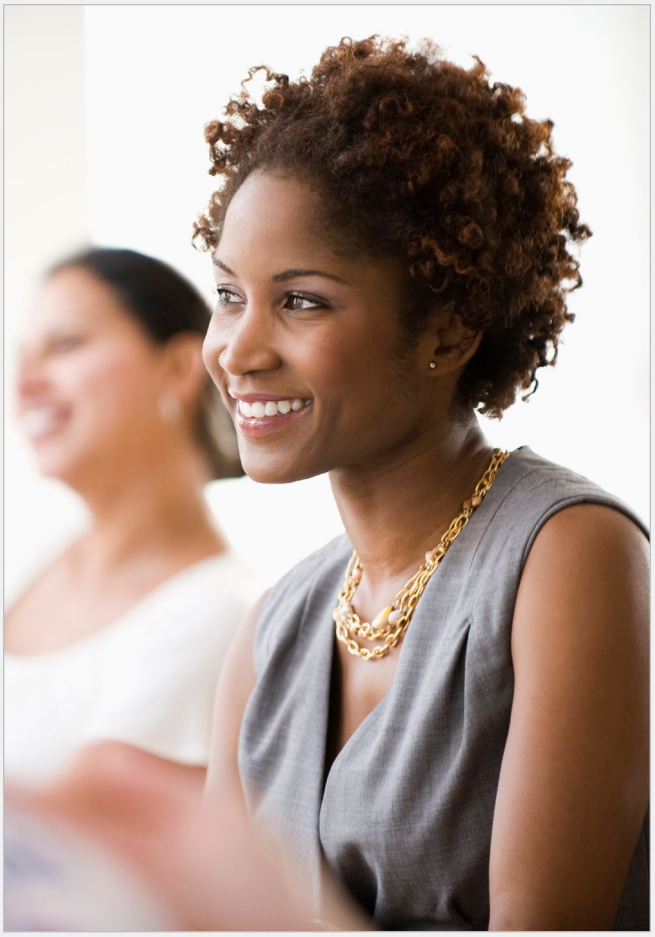
Confidential supervisory information includes any information or materials relating to the examination and supervision of the company by applicable bank regulatory agencies, company materials responding to or referencing nonpublic information relating to examinations or supervision by bank regulatory agencies and correspondence to or from applicable banking regulators.

The terms "Bank of America," "the Bank," "the Company," "corporation" and "company" refer to Bank of America Corporation and each of its direct and indirect subsidiaries. For convenience, we use these terms because various companies within Bank of America use this document. The use of these terms here or in other publications does not mean you are an employee of Bank of America Corporation. The use of these terms or issuance of this document does not change your existing at-will employee status. Employees remain employed at will, and the at-will employment relationship can only be changed by an authorized company representative in writing. Similarly, the use of these terms or the requirement to read and adhere to this Code does not change the employment status of the employees of the company's third parties or contractors. The term "associate," "employee," "teammate" or "you" refers to any Bank of America director, officer and employee. The 2023 Code of Conduct supersedes and replaces any prior communications, policies, rules, practices, standards and/or guidelines that are less restrictive or to the contrary, whether written or oral. To the extent there are any conflicts with the Employee Handbook in the U.S. and in countries with an Employee Handbook, the language of this Code supersedes the Employee Handbook in the U.S. and in countries with an Employee Handbook. If any provision of this Code conflicts with your local law, the provisions of your local law apply.

Our Code of Conduct

Our Code applies to all employees of Bank of America. In addition to employees, this Code defines our expectations of everyone who acts on our behalf, including, but not limited to, consultants, third parties and contractors. All who act on our behalf are expected to embrace the spirit of this document and to behave with the highest level of integrity.

Your manager or Compliance and Operational Risk officer will provide you with access to any manuals, policies, procedures and training related to your specific job. You should refer to the Employee Handbook in the U.S. and in countries with their own Employee Handbook for additional information on employee conduct. The company may publish additional policies as deemed necessary or appropriate. You are expected to follow this Code, other policies referred to in the Code, additional policies that apply to your specific job and the spirit and letter of all applicable laws and regulations. Violations of the Code of Conduct or other policies, procedures, laws and regulations will be dealt with promptly and may constitute grounds for disciplinary action, including termination of employment and possible legal action.



We honor our Code

Making good, responsible decisions

Every decision we make as an institution and as employees has the potential to impact not only the company and our teammates, but our customers, clients, shareholders and communities as well. We all strive to make good, responsible decisions and to do the right thing. However, making decisions is not always easy. Keep the following in mind to help you make informed, thoughtful decisions:

- Ensure you have the relevant facts.
- Take into account relevant laws, rules, regulations and policies.
- Consider competing interests.
- Identify potential options and their consequences.
- Uphold Bank of America values.

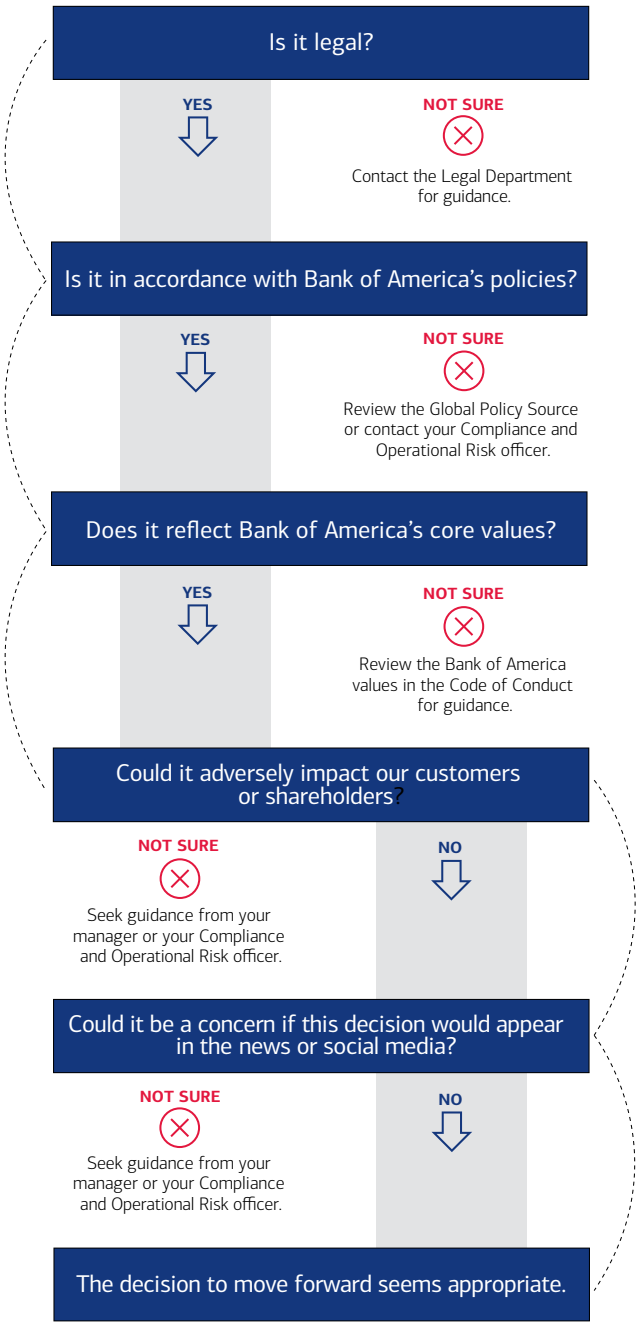
Observing the Code of Conduct and annual training

As a Bank of America employee or contractor, you are required to adhere to the Code of Conduct and take Code of Conduct training, which includes an acknowledgment, on an annual basis.

For more information:

- Code of Conduct Flagscape site
- Compliance Training Policy
- Employee Handbook

Ethical decision-making tree



Fair Dealing and Employee Responsibilities

At Bank of America, we are expected to deal fairly with our employees, customers, vendors, competitors and other third parties:

- You must not take unfair advantage of any employee, customer, vendor, competitor or other third party through manipulation, concealment, misuse of proprietary and/or confidential information, known misrepresentation of facts or any other unfair business practice.
- You must not give or accept bribes, kickbacks, unauthorized promises or preferential extensions of credit.
- You must approve or award orders, contracts and commitments based on objective business standards to avoid favoritism or perceived favoritism.
- You must not conspire or collude in any way with competitors.
- You must not access a customer's account except for appropriate business purposes.

For more information, please see the policies and resources reference in each section in this Code of Conduct and consolidated in the resources starting on page 38.

Key obligations of managers

As a manager, you have key obligations to help create a work environment where conduct issues are actively discussed. These obligations include:

- Lead by example: "Set the tone at the top," actively practice ethical behavior, manage risks in accordance with the company's Risk Framework and the Conduct Risk Management Program and live the standards of our Code and our values.
- Hold others accountable for acting in accordance with our values, our Code, Risk Framework and our Conduct Risk Management Program.
- Ensure that individuals under your supervision are aware of our Code and related policies and procedures.
- Maintain a workplace environment that encourages candid discussions about ethics issues with no fear of retaliation.
- Refrain from conduct that could be considered an abuse of your position or influence (such as improperly pressuring teammates for personal benefit).
- Treat all escalations and complaints confidentially and consistently, following company policies and procedures for handling them.
- Report and/or escalate concerns of misconduct to the Ethics and Compliance Hotline or Employee Relations.

For more information:

- Code of Conduct Flagscape site

Q: As a manager, how can I promote ethical behavior?

A: First and foremost, lead by example. Include discussions about workplace ethics in team meetings. Make team members feel comfortable asking questions when they have concerns. Remind employees that they will not be retaliated against for reporting information in good faith and in accordance with this Code.

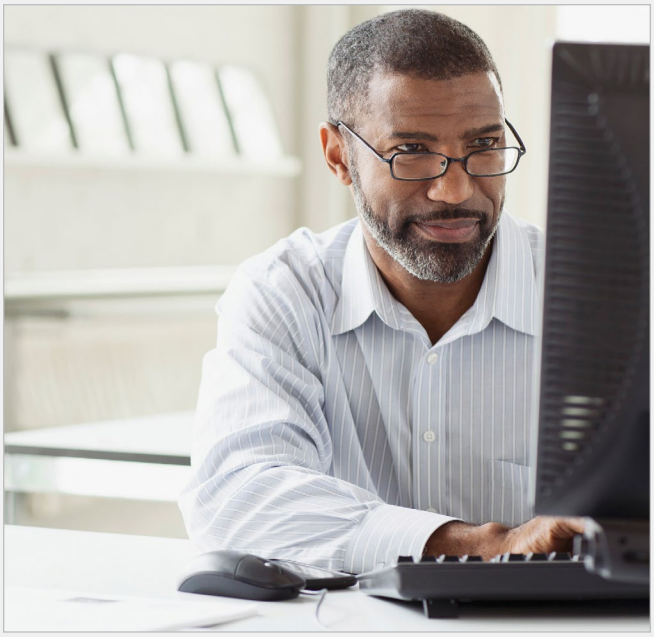
Conduct management

Bank of America recognizes the importance of complying with the legal and regulatory requirements in the jurisdictions where it does business and the risks of improper and unethical conduct. The Conduct Risk Management Program document provides an overview of Bank of America's approach to managing conduct risk.

The Ethics Oversight Committee is responsible for providing oversight of the Bank of America Code of Conduct. This includes reviewing and assisting with the resolution of issues, including strategies to prevent violations and certain exceptions, and reviewing information from the Ethics and Compliance Hotline. The committee includes the company's Chief Audit Executive, global general counsel, chief risk officer, global compliance and operational risk executives, and Chief Human Resource Officer.

For more information:

- Code of Conduct Flagscape site
- Bank of America programs, policies and procedures
- Employee Handbook



Reporting conduct complaints and possible violations

Subject to applicable laws and the Notice to Employees in this Code, you must promptly report any knowledge or information about conduct by anyone in the company that you reasonably believe to be:

- A crime or illegal act.
- A violation of law, regulation or policy including this Code.
- A dishonest act or unethical act, including misappropriation of funds or anything of value from Bank of America, or the improper recording of the company's assets or liabilities.

You also must report any other circumstances or activities that may conflict with the Code of Conduct. If you have any questions or concerns regarding the Code of Conduct:

- Consult your manager or Compliance and Operational Risk officer.
- Refer to Risk Management on Flagscape for additional information and contacts.
- Contact Employee Relations.

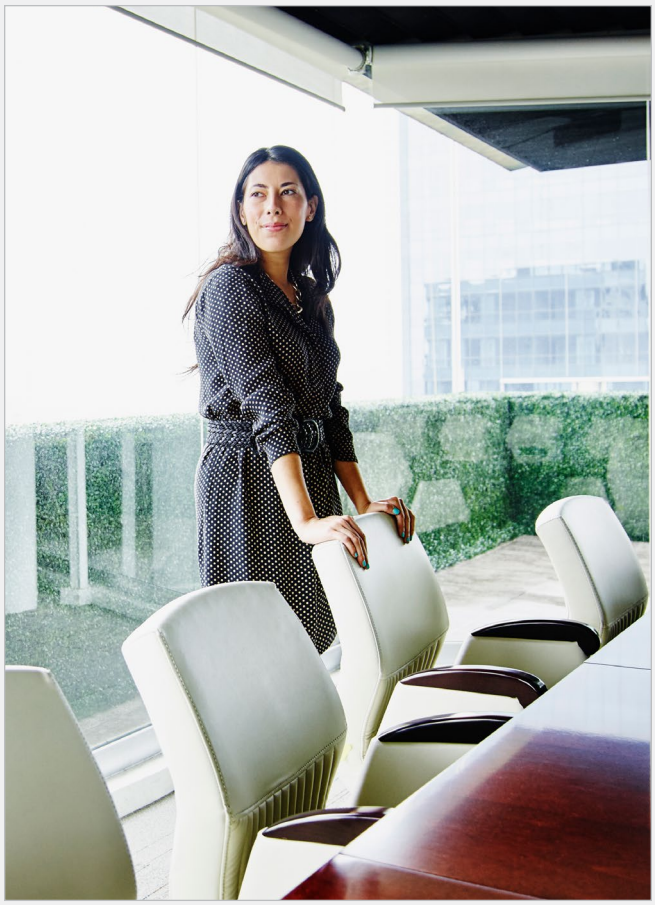
To report complaints or possible violations regarding ethical issues or other inappropriate activity, promptly call the Ethics and Compliance Hotline at the numbers below, or submit a report online at bankofamerica.ethicspoint.com:

- Employees in the U.S., Puerto Rico and U.S. Virgin Islands call toll-free 888.411.1744.
- For other international employees, toll-free dialing instructions will vary by location. Please see the International Ethics and Compliance Hotline dialing instructions.

Please note that complaints or possible violations can be submitted anonymously and in complete confidence.

If reporting suspicions of a financial crime, these must be reported via The Referral Management System. This can be done instead of or in addition to reporting them to the Ethics and Compliance Hotline.

Individuals outside the U.S. should click on this link for further information about reporting their concerns.



Non-retaliation

Bank of America values clear and open communications and respects the contributions of all employees.

You will not be retaliated against for reporting in good faith and in accordance with this Code information that you believe relates to possible misconduct, unethical acts and/or violations of laws, rules, regulations and this Code.

Retaliatory conduct includes discharge, demotion, suspension, threats, harassment and any other manner of discrimination in the terms and conditions of employment because of any lawful act performed in connection with such reporting.

Bank of America takes seriously claims of retaliation against those who report possible misconduct. We will investigate allegations of retaliation, and any individual found responsible for retaliating against any individual who reported possible misconduct to the Ethics and Compliance Hotline or any other channel is subject to disciplinary action, up to and including termination of employment and possible legal action.

Duty to report arrests

Subject to local applicable laws and guidelines, all Bank of America applicants are required to pass a criminal background check as a condition of employment. Background checks are conducted only after an applicant receives a conditional offer of employment. As a federally regulated financial institution, Bank of America is prohibited from employing individuals whose criminal history does not meet applicable legal and financial industry rules. Bank of America also conducts an individualized review of criminal history focused on maintaining the safety and soundness of the company. To ensure continuing compliance with these laws and standards, Bank of America may conduct additional criminal background checks at any time during employment. In addition to complying with any line-of-business-specific guidelines or industry requirements, unless prohibited by law, you are required to inform the company of any arrest or criminal investigation that arises during your employment, for any offense other than a minor traffic violation (e.g., speeding, running a red light, failing to yield and failure to obey a traffic device) by email addressed to codeofconduct@bofa.com. Arrests and charges will be considered only as required or permitted by applicable law, and disclosure of a pending arrest or charge or resulting conviction will not necessarily disqualify you from employment. If you have any questions regarding compliance with this requirement, you should contact Employee Relations.

For more information:

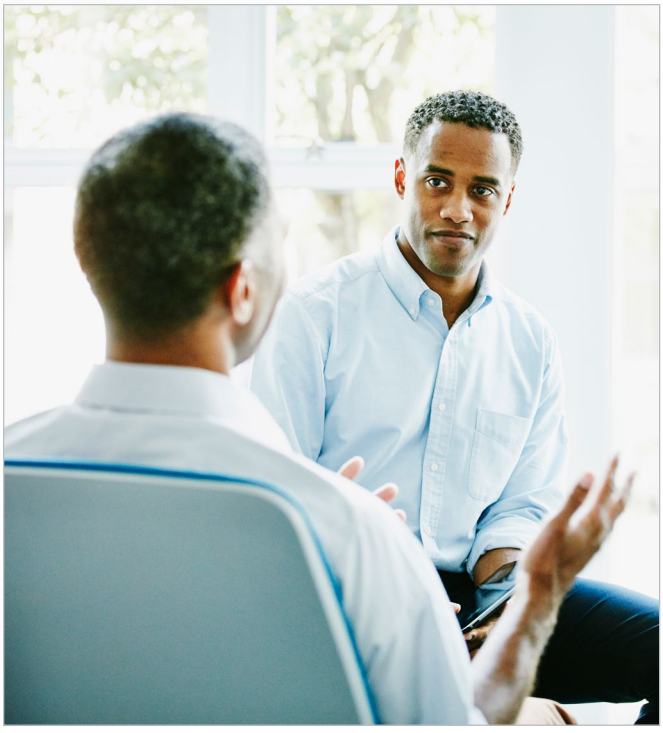
- Global Background Check Policy
- Conduct Risk Management Program
- Employee Handbook
- Employee Relations on HR Connect
- Compliance and Operational Risk officer
- Applicable local and line-of-business-specific guidelines

Duty to cooperate

You must fully and truthfully cooperate with any internal or external investigation or audit, or any regulatory examination or request for information subject to legal protections. You need to be aware of and comply with any applicable business-specific policies and procedures regarding contact with regulators, which, among other things, may require you to report such contact to either your manager and/or Compliance and Operational Risk officer and/or Global Regulatory Relations. Additionally, you must immediately inform your manager if you are the subject of an external investigation unless laws, regulations or the investigating authority prohibit you from doing so.

For more information:

- Code of Conduct Flagscape site
- Employee Handbook
- Employee Relations on HR Connect
- Risk Management Flagscape site
- Global Regulatory Relations Flagscape site



We manage risk well

Managing risk is central to everything we do. That is why, no matter where we work in the organization, managing risk well is foundational to fulfilling our purpose and values — and delivering Responsible Growth.

Our Risk Framework provides an understanding of our approach to risk management and each employee's responsibilities for managing risk. A culture of managing risk well:

- Requires us to focus on risk in all activities
- Encourages the necessary mindset and behavior to enable effective risk management
- Promotes sound risk-taking within our risk appetite

To live our culture of managing risk well:

Take ownership

Hold yourself and each other accountable to live our values, act responsibly and be proactive in finding and fixing issues. Make decisions as if your own reputation were on the line.

Use your voice

Speak up and foster an environment where others feel comfortable sharing their concerns. Encourage and recognize those who bring attention to potential risks.

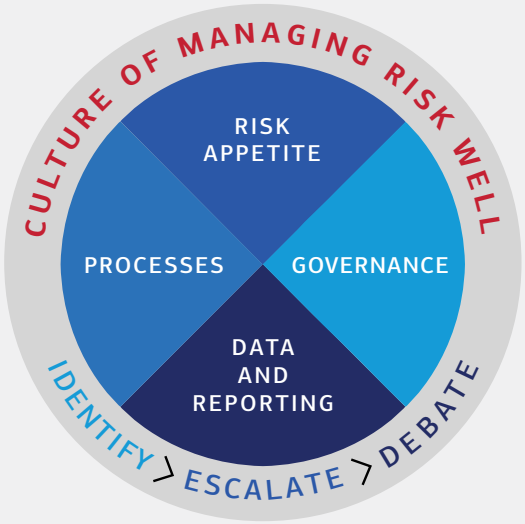
Be intellectually curious

Openly and regularly engage colleagues in conversations about risks. Challenge one another, think objectively and work together to make smart decisions.

When we all take personal ownership of risk management, it contributes to the strength and sustainability of our company and supports the work we do to serve our customers, clients, communities, shareholders and employees.

For more information, please refer to the Risk Framework.

Risk Framework components



We act ethically

Sustaining our culture of managing risk well throughout the company is critical to our success and our efforts to drive Responsible Growth. Growing responsibly is supported by our commitment to act responsibly, which means that as we help make financial lives better for our customers and clients, we must always conduct ourselves with fairness, honesty and integrity.

Conflicts of Interest

Bank of America's employees face actual, potential and perceived conflicts of interest on a regular basis during the normal course of business. A conflict of interest may occur when your personal interests, or the activities you perform on behalf of the company, interfere or appear to interfere with the company's, shareholder's or a client's best interest. A conflict of interest can arise when you take action or have interests that make it difficult to perform your company work objectively. We must take reasonable steps to identify, mitigate, disclose or restrict business activities or practices that may pose a conflict. Some of the potential conflicts of interest that you must be aware of are:

- Personal relationships among employees
- Gifts among employees
- Corporate opportunities
- Charitable contributions and solicitations
- Outside business activities
- Activities outside of work
- Bribery and Corruption
- Gifts and Entertainment
- U.S. political contributions and activities
- Interactions with government employees (federal, state and municipal)
- Interactions with third parties

Considerations for identifying potential conflicts of interest:

You are responsible for identifying, managing and escalating (to your manager or Compliance and Operational Risk officer) actual, potential or perceived conflict in accordance with applicable regulatory requirements and Bank of America policies, including this Code. Some general considerations for identifying potential conflicts of interest:

- **Perception:** Could the activity or transaction be perceived as a potential conflict by others?
- **Intent:** Is the offer or request an attempt to influence the recipient's or your judgment?
- **Impact:** Will the company, its employees, its shareholders or its customers be disadvantaged or negatively impacted if you participate in the activity?
- **Objectivity:** Will your participation in the activity affect a customer's or your judgment or your ability to be objective with regard to any business decision?
- **Time considerations:** Will the time required by an outside business activity or outside interest interfere with your ability to effectively carry out your job responsibilities to the company, its shareholders or its customers?

For additional information, refer to the Conflicts of Interest — Enterprise Policy.

Personal relationships among employees

While you may have a personal relationship with someone who also works at Bank of America, it is important that hiring decisions, reporting relationships and other terms and conditions of employment (e.g., granting time off, adjusting schedules or other potentially favorable work arrangements) avoid any conflict of interest, or the appearance of a conflict of interest.

A real or perceived conflict of interest may arise if you have a personal relationship with another employee where either party has direct or indirect influence over the other party's employment, compensation, approval authority, chain of custody or work conditions. Examples of personal relationships include, but are not limited to, those of a family member,[1] close friend, intimate or romantic partner, roommate, babysitter and/or renter/landlord. Further, you must avoid workplace relationships that would create a conflict of interest. For example, managers are prohibited from dating or having a sexual relationship with subordinates or anyone in their chain of command. Escalate to your manager and HR or Employee Relations if you have a personal relationship that could create such a conflict or if you are unsure whether a particular personal relationship creates a conflict.

Note: Merrill Lynch Wealth Management follows line-of business-specific guidelines regarding employment of relatives. Please contact your manager, Employee Relations or Advisory Online for additional information.

Gifts among employees

A conflict of interest may arise when you provide or receive gifts to or from another employee, and especially when gifts are exchanged among employees in the same reporting line or in positions of influence. Employees must exercise good judgment to ensure that any gift is reasonable for the occasion, and is not lavish or so frequent to create any appearance of a conflict of interest or be perceived as compensation or reward for job performance.

Note that you may provide gifts in connection with life events or holidays (e.g., weddings, birthdays, births) where the circumstances make it clear that it is the life events — rather than Bank of America's employment relationships — that are the motivating factors for giving the gifts.

For more information:

- Conflicts of Interest — Enterprise Policy
- Anti-Bribery Anti-Corruption — Enterprise Policy
- ABAC Gifts and Entertainment — Enterprise Policy
- Gifts and Entertainment FAQ
- ABAC U.S. Political Activities — Enterprise Policy
- U.S. Political Activities FAQ
- Outside Business Activities — Enterprise Policy
- Employee Handbook
- Compliance and Operational Risk officer
- Applicable line-of-business-specific guidelines

[1]For the purposes of this Code, "family member" includes a spouse or domestic partner, child (including by adoption), parent, grandparent, grandchild, cousin, aunt, uncle, niece, nephew, sibling, parent-in-law, brother-in-law or sister-in-law of the employee or the employee's spouse or domestic partner, step relationships of the aforementioned or individuals residing in an employee's home.

Corporate opportunities

You also have a duty to the company to advance its legitimate interests when the opportunity to do so arises. Accordingly, you must not deprive the company of an opportunity by:

- Competing with the company or using corporate property, information or your position for personal gain.
- Taking for yourself an opportunity that is discovered using corporate property or belongs to the company, or helping others do so, if they are in a position to divert a corporate opportunity for their own benefit.

Charitable contributions and solicitations

A conflict of interest may arise from a contribution made to a charitable organization at the request of a client or vendor as a means to maintain or induce business, or when an employee asks a client or vendor to give to a charitable organization in exchange for reduced fees, favorable terms, products or services. A perceived conflict can also occur when a contribution is made by an employee to a charitable organization that is a direct client and/or a charity board member who is a direct client of the employee, or a charitable organization that is associated with a government employee.

For more information:

- Conflicts of Interest Flagscape page
- Compliance and Operational Risk officer
- Applicable line-of-business-specific guidelines
- ABAC Enterprise Policy

Q: I have given a yearly donation to the local chapter of my favorite charity for the past five years. I just learned that one of my clients has been asked to join the board of directors. Can I continue to give to this charity?

A: Yes. You have a history of giving to this charity prior to your client's joining the board of directors; however, you should review any future decisions to significantly increase your giving with your manager and/or Compliance and Operational Risk officer.

Q: My daughter is currently working on her undergraduate degree in finance. Can I send her resume to the recruiter for an open internship on our team?

A: No, you may not use your influence and position at the bank for the personal benefit of yourself or a family member. However, your daughter is welcome to follow normal standard hiring practices to become an intern with the company. If selected for a position based on her merits, placement of a family member on the same team would not be permitted.

Outside business activities

A conflict of interest or other risk may arise from activities, employment or other relationships conducted outside your role with Bank of America. You must not act on behalf of or appear to represent the company in any business transaction outside your role and responsibilities with Bank of America. For activities requiring approval, you must obtain all required approvals prior to engaging in an outside business activity by disclosing the activity within the Associate Investment Monitoring (AIM) system.

You are permitted limited use of Bank of America resources while pursuing such outside business activities and relationships (including but not limited to physical space, supplies, communication methods or time). However, you must not allow any outside business, civic or charitable activities to interfere with your job performance, must not use Bank of America resources to develop inventions related to an outside business activity, and you must not store any material, nonpublic information (MNPI) or other sensitive data related to an Outside Business Activity on bank property. With few exceptions, Bank of America generally discourages employees from serving on a board of a for-profit organization in a personal capacity, particularly, the board of a public company, and additional approvals are required.

For more information:

- Outside Business Activities — Enterprise Policy
- Business interests outside of primary employment
- Compliance and Operational Risk officer
- Applicable line-of-business-specific guidelines

Activities outside of work

We are all expected to act in a manner consistent with high standards of professional conduct that merits public trust and confidence.

You must be aware that your actions outside of work have the potential to impact Bank of America's reputation/brand, customer relationships, co-worker relationships or your role. If your actions outside of work are associated with Bank of America, even if the association is unintended, a real or perceived conflict of interest or conduct issue may arise, especially if the actions conflict with our values or this Code of Conduct.

Actions outside of work that create a real or perceived conflict of interest, excluding protected speech involving terms and conditions of employment, could lead to disciplinary action up to and including termination.

Q: I've been asked to serve on a board of local nonprofit organization. Do I need to get approval?

A: Yes, you must obtain approval before serving on a board of an organization, whether a for-profit or a nonprofit entity. For additional guidance, please visit Outside Business Activities on Flagscape.

Q: How do I disclose an outside business activity?

A: All activities requiring approval must be disclosed within the AIM system. This disclosure will facilitate obtaining approval from your supervisor and any additional approvals that may be required for the activity. For additional guidance, please visit Business interests outside of primary employment on Flagscape.

Q: If an outside business activity was previously approved, is there any further action?

A: Yes, if details of previously disclosed outside business activities change, you must update your disclosure within the AIM system. Bank of America may deny or rescind approval at any time, and participation must cease within the agreed-upon time determined by the Company. For additional guidance, please visit Business interests outside of primary employment on Flagscape.

Bribery and Corruption

You may not give, promise or offer money or anything of value to any customer, government employee or any other person for the purpose of improperly influencing a decision, securing an advantage or obtaining or retaining business. If you engage in such behavior, you expose yourself and the company to potential regulatory, civil and/or criminal liability and significant reputational harm, and you undermine the trust of our customers, shareholders and communities.

For more information:

- Anti-Bribery Anti-Corruption Flagscape site
- Compliance and Operational Risk officer

Gifts and Entertainment

Providing gifts and entertainment, including promotional items, is often customary in the financial services industry; however, many countries have rules that regulate these activities. You must adhere to such rules to avoid impropriety or the appearance of impropriety that could expose Bank of America to civil or criminal liability or threaten the public's trust in Bank of America.

A conflict of interest may arise when you give or receive gifts or entertainment to or from clients, prospects or third parties. You must ensure that the exchange of gifts or entertainment is reasonable and for a legitimate business purpose (unless personal in nature), and is in compliance with our enterprise and local policies.

You are prohibited from providing or receiving gifts or entertainment that are so lavish, frequent or excessive that they could be perceived as improper. Your gift and entertainment activities may be restricted to specific dollar limits (or local currency equivalents) and/or subject to certain preapproval thresholds.

For more information:

- Conflicts of Interest — Enterprise Policy
- Personal relationships among employees (Employee Handbook)
- ABAC Gifts and Entertainment — Enterprise Policy
- Compliance and Operational Risk officer

U.S. political contributions and activities

In general, you may make personal political contributions, within applicable legal limits, to candidates, parties and committees. Because of industry regulations and federal, state or local laws, employees of particular businesses, or who have certain coverage responsibilities, may be restricted from making some political contributions or engaging in certain political activities.

Under no circumstance may you coerce or pressure other employees to make political contributions. Employees may not make use of any company assets or personnel to engage in political fundraising or solicitation activities on company premises.

For more information:

- Anti-Bribery Anti-Corruption Flagscape site
- ABAC U.S. Political Activities — Enterprise Policy
- U.S. Political Activities FAQ
- Compliance and Operational Risk officer

Interactions with government employees

You must not offer, give or promise to give money or anything of value to any employee of any government, agency, state-owned or controlled enterprise, political party or candidate for political office if it could be perceived as a conflict of interest or suggestion of a quid pro quo. Interactions with government entities and their employees may expose the company and its employees to various public policy, legal and compliance risks. You must obtain preapproval from your manager and Compliance and Operational Risk officer for any gifts and entertainment provided to government officials.

Please review the ABAC Gifts and Entertainment — Enterprise Policy for additional information including types of government entities/employees covered under the policy. You are expected to be particularly vigilant when interacting with government employees and must not engage in behavior that could be seen as being intended to improperly influence a Bank of America business relationship.

Nothing in this section is intended to prohibit employees from filing a complaint with governmental agencies such as the SEC, the Financial Industry Regulatory Authority, Inc., the National Labor Relations Board, the Occupational Safety and Health Administration, and similar regulatory entities.

For more information:

- ABAC Gifts and Entertainment — Enterprise Policy
- ABAC U.S. Political Activities — Enterprise Policy
- U.S. Political Activities FAQ
- Notice to Employees

Interactions with third parties

Bank of America uses third parties across many processes, operations and products while ensuring that such outsourced activities are conducted in a safe and sound manner and in compliance with all applicable policies, laws and regulations. Our work to engage third parties throughout our supply chain is intended to support the environmental, social and governance (ESG) work we're doing around the globe. We are committed to increasing our company's use of diverse third parties and driving impactful environmental and social change throughout our supply chain to improve the communities in which we do business. Learn more about our ESG expectations of third parties in our Supplier Code of Conduct.

Third parties are critical in helping each of our eight lines of business and control functions deliver to their capabilities. A conflict of interest may arise from relationships with third parties or other service providers. If you are authorized to approve or award orders, contracts, commitments or engagements to third parties for goods or services, you must do so based on objective business standards to avoid any real or perceived favoritism. Interactions between employees of Bank of America and third parties, who may also be Bank of America clients, must be conducted in accordance with all applicable Bank of America policies and principles of arm's-length transactions.

Global Procurement is the Bank of America organization that sets the framework for third party risk management. Including requirements for business and risk management activities, the program supports the company goal of maintaining a consistent, sustainable and effective risk-based process for managing the third party engagement and life cycle. Global Procurement must be engaged for all third party interactions.

For more information:

- Third Party — Enterprise Policy
- Third Party Management Flagscape site
- Supplier Code of Conduct

We are fair and honest in our communications

Responding to media inquiries

We work to both advance and protect the Bank of America brand through engagement with the news media as part of our larger marketing, communications, public policy and corporate affairs activities. If you are contacted or approached by a reporter or member of the media and asked to speak on behalf of the company, you should direct them to the Journalist Resources section of the Bank of America newsroom. Only employees designated by Bank of America's Media Relations staff are authorized to speak with the media as spokespersons for and on behalf of the company.

If you anticipate speaking or communicating with the media on behalf of the company, including social media, you must obtain approval from a member of the Media Relations team and comply with applicable line-of-business-specific policies and procedures. This includes requests for information or comments on behalf of the company about company business, plans or strategy, organizational or administrative matters, results of operations or information about the company's performance. This also includes requests for comments or information on behalf of the company either on an "on-the-record," "off-the-record" or "background" basis. Employees acting on behalf of the company are prohibited from giving members of the media access to or a summary of company confidential or proprietary information, such as internal conference calls, webcasts and internal emails or other written materials or presentations, without prior involvement and approval of Media Relations and the Legal Department.

These policies are not intended to infringe upon or violate your rights protected under applicable employment, securities, or other applicable laws, rules and regulations. However, you may not disclose MNPI, proprietary, confidential or private information learned in the course of employment with the company or any confidential customer or client information, except as specifically provided in the company's policies or as described in the Notice to Employees in this Code. If you are contacted by the media regarding non-company issues where the situation could reflect negatively on the company as your employer or result in high-profile media attention, you must alert your manager and Media Relations. While these situations do not directly involve the company, the media could highlight your affiliation with the company, resulting in questions for you and Media Relations, and create reputational risk to the company.

For more information:

- Bank of America newsroom
- Media Relations
- Notice to Employees

Electronic communications and social media

Electronic communications help us improve overall business efficiency and are an important part of how Bank of America does business. Adhering to all applicable electronic communications policies preserves customer trust, protects our brand and minimizes risk.

We are all responsible for utilizing company-approved communication devices, approved applications and approved connecting services for sharing company information, including information that may be material, nonpublic, proprietary, confidential or private.

All electronic communications activities using internal and external systems, devices, tools and applications are, to the fullest extent permissible by law, subject to monitoring and retention by or on behalf of Bank of America.[2] Communication activities may include, but are not limited to, email, SMS text, instant messaging, chat, voice, video, collaboration tools, and web streaming and conferencing, including social media chat and collaboration functions.

Adhering to our written communication principals means that employees may not use non-company-approved applications or devices for business related written electronic communication. Non-approved applications include personal communication's features typically located on personal devices such as personal laptops, tablets and personal phones. These personal communications features frequently include, but are not limited to: personal email, digital and SMS text, instant messaging, chat, iMessage, and audio/video collaboration tools. The Company cannot monitor, secure, produce or retain business-related communications sourced from non-approved applications or personal devices.

You are permitted limited personal use of company-managed devices and applications, the internet and email for personal communications. The use of the resources may be monitored and inspected to ensure productivity is not negatively impacted. In doing so, you must maintain the integrity of the systems (e.g., monitoring for the introduction of malware or inappropriate data transmissions) and avoid activities that may give rise to company liability or risk (e.g., claims of unlawful harassment or conduct).

All electronic communications and social media use (both internal and external) must adhere to the standards of this Code and the Employee Handbook in the U.S. and in countries with an Employee Handbook, as applicable. As with any communication about the Company, you are reminded to act ethically when using social media. Your behavior on social media can not only affect you personally and professionally, but also the Company's brand. Social media posts or other content that includes discriminatory remarks, harassment and threats of violence or similar inappropriate or unlawful conduct will not be tolerated and may subject employees to disciplinary action up to and including termination. Additionally, you should be aware of any line-of-business-specific social media policies and other restrictions that you may be subject to due to regulatory requirements.

For more information:

- Electronic Communications Retention — Enterprise Policy
- Electronic Communications Guide
- Employee Handbook
- Social media at Bank of America Flagscape site
- Line-of-business-specific social media policies and other restrictions

[2] In the United States and other countries, where permissible, based on local laws and regulations, as applicable, employees should have no expectation of privacy with respect to electronic communications that are transmitted or stored on systems, platforms, hardware or software that are controlled by the company or that are publicly available, including any publicly available social media, whether or not controlled by the company. For questions regarding local laws and restrictions, employees should contact their local Compliance and Operational Risk officer or the Legal Department.

We safeguard information

Customer information

We are committed to respecting our customers' right to privacy by keeping their personal and financial information protected and secure through responsible and lawful information collection, processing and use practices. You must not access or use customer information except for appropriate business purposes, and you must protect the confidentiality and security of customer information. Our internal privacy and information security enterprise policies and standards provide additional details on your duty to protect and secure customer information, and reinforce our commitment to the responsible processing of personal data which respects individuals' privacy rights as well as its appropriate use. You should also be familiar with the "Need to Know" principle for all confidential information, including MNPI related to our corporate clients.

Supervisory information received from regulatory authorities

Supervisory information[3] received from our regulatory authorities must be treated as confidential. Depending on the agency, such material may be deemed government property that Bank of America is not authorized to share or disseminate without express written consent. Information received from regulatory authorities should be kept secure and not disseminated outside of Bank of America without proper authorization. Such information should only be shared within the company with other employees who "Need to Know" the information. For more information, consult Global Regulatory Relations.

Bank of America information

You must keep secure and not disclose confidential or proprietary information about Bank of America, such as business plans, market conditions that may be of use by competitors or harmful to the company or its customers if disclosed, and third party information. Such information should only be shared within the company with other employees who "Need to Know" the information to perform their duties. Consult your manager if you have questions about sharing information about Bank of America on a "Need to Know" basis.

Employee information

You must not access another employee's information or use another employee's information except for appropriate business purposes, and you must protect the confidentiality and security of such information. The Commitment to Protecting Employee Information — Enterprise Policy establishes requirements for how employees, managers and third parties must treat U.S. employee information. Outside the U.S., country-specific Data Protection Notices are in place, which can be provided by your local Human Resources partner or Compliance and Operational Risk officer.

Third party information

You must keep confidential and secure any information about Bank of America's purchase of products or services or other information received by Bank of America from a third party. Sharing such information could result in competitive harm to Bank of America and the third party, provide an improper advantage to a competitor of Bank of America or of the third party and violate agreements that Bank of America has with a third party. In some instances, it also might violate the "Need to Know" principle for MNPI.

For more information:

- Privacy and Cross Border Data Movement — Enterprise Policy
- Information Security — Enterprise Policy
- Information Wall — Enterprise Policy
- Security and Privacy Flagscape site
- Enterprise Data Management — Enterprise Policy
- Third Party — Enterprise Policy
- Third Party Management Flagscape site

[3] Supervisory information includes any information or materials relating to the examination and supervision of the company by applicable bank regulatory agencies, company materials responding to or referencing nonpublic information relating to examinations or supervision by bank regulatory agencies and correspondence to or from applicable banking regulators.

Bank of America intellectual property

In accordance with the Proprietary Rights and Information Agreement, any and all assets you create for Bank of America or while using Bank of America resources are the company's property, and remain its property even if you leave Bank of America.

We respect the intellectual property rights of others. You must not obtain, use, sell or distribute the intellectual property of others in violation of confidentiality obligations or intellectual property law.

For more information:

- Intellectual Capital & Property Flagscape site
- Proprietary Rights and Information Agreement

Q: Can I leverage materials from my previous employer at Bank of America?

A: You may not use, reference or distribute any materials from prior employers at Bank of America. Examples include, but are not limited to, playbooks, manuals, software code, analytical models and any other nonpublic information. You also cannot leverage Bank of America materials at any future employers. For additional information and guidance, please visit the Proprietary Rights and Information Agreement.

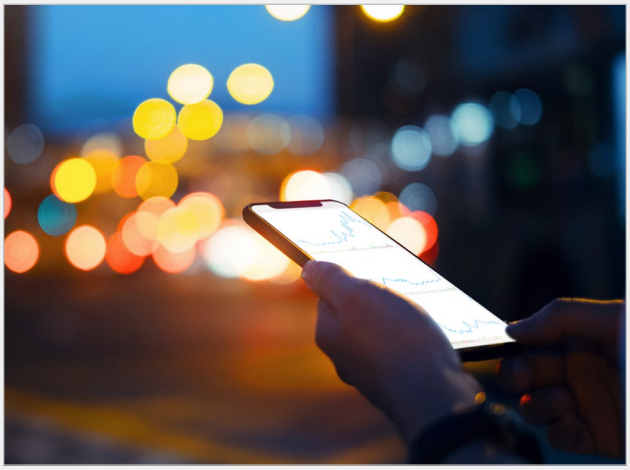
We will not misuse information

Restrictions on trading in securities or financial instruments

If you are in possession of MNPI of any company, including Bank of America, you are prohibited from buying, selling, recommending or trading — either personally or indirectly through someone else — securities or financial instruments of that company. Under the securities laws, such activities may constitute insider trading because they involve fraud on securities markets by illegally permitting an individual or company to profit from information not available to the public.

In addition, you must not communicate or disclose such information to others who may misuse it, including family members.[1] Doing so would not only be a violation of your duty of trust or confidence but also may be a violation of U.S. federal and state laws, as well as the laws of many countries.

You must be familiar with, understand and comply with the Information Wall — Enterprise Policy and all other policies and procedures that relate to your area of responsibility, paying attention to specific guidance relating to restrictions on the trading of securities and other activities, including in the event that MNPI is received.



As an employee, you have additional restrictions on trading in Bank of America securities, including:

- If you are a Bank of America director or executive officer or have been designated as an insider (Designated Insider) by the company, you must obtain approvals before trading in Bank of America securities.
- Bank of America directors, executive officers and Designated Insiders may not engage in hedging, speculative trading or trading in derivative securities with respect to Bank of America securities. This prohibits short sales and trading in puts, calls, prepaid variable forward contracts, equity swaps, collars or exchange funds and other options or derivatives with respect to Bank of America securities.
- Other Bank of America employees must not engage in speculative trading of Bank of America securities. This prohibits short sales and trading in puts, calls and other options or derivatives with respect to such securities, unless such transaction is a bona fide hedge against an existing long position in Bank of America securities (e.g., writing a covered call or purchasing a covered put).

If you have questions regarding the potential speculative nature of your transaction, please talk with your manager, Compliance and Operational Risk officer or Legal department.

For more information:

- Additional Guidance While Trading in Bank of America Securities
- Information Wall — Enterprise Policy
- Compliance and Operational Risk officer

What is MNPI or Material, Nonpublic Information?

The definition of MNPI is broad. You should consider information to be material if a reasonable investor would consider it important in making an investment decision (for example, any information that likely would affect the market price of a security or financial instrument if made public). There is no bright-line standard for assessing materiality. Rather, materiality is based on an assessment of all of the facts and circumstances. Examples can include merger-and-acquisition information, leadership or board-of-director changes, significant cybersecurity breaches and earnings-related and other significant financial information. You should consider information nonpublic if it is not widely disseminated or generally available to the investing public.

In other jurisdictions, MNPI is often referred to as "inside information" or "price-sensitive information." While MNPI and "inside information" or "price-sensitive information" are similar, they are not identical. You should be familiar with applicable business-specific or jurisdiction-specific policies and procedures, and consult with your Compliance and Operational Risk officer with questions.

For more information:

- Information Security — Enterprise Policy
- Information Wall — Enterprise Policy
- Country-specific policy and procedures
- Applicable line-of-business-specific guidelines
- Compliance and Operational Risk officer

Q: Are there any restrictions on voice communications on personal devices?

A: Voice communications on a personal device are permissible provided that the employee is not subject to any voice recording requirements or obligations. Employees subject to any voice recording requirements must be on company-managed devices and should refer to their specific line-of-business requirements. Employees are reminded, however, that it is not permissible to send or receive business-related written communications on personal devices.

We protect Bank of America assets

We must properly care for and protect Bank of America property and assets from theft, loss, carelessness, waste and cybersecurity threats. The Bank's property and assets should be used efficiently and for legitimate business purposes only.

You must not:

- Steal, embezzle or misappropriate money, funds or anything of value from Bank of America. Doing so subjects you to potential legal and/or disciplinary action, according to the law and Bank of America policy.
- Use Bank of America assets for personal gain or advantage. This includes personal use of confidential or proprietary information that you learn through your employment.
- Remove Bank of America assets from the facilities unless you are authorized to do so or have your manager's approval.
- Use official Bank of America stationery, corporate brand, documents, name, trademark or logos for commercial gain.
- Misuse your internet, phone or email privileges. See the Electronic communications and social media section of this Code for additional information.

You are expected to safeguard company-issued hardware, software and devices against theft, loss or unauthorized use. You must protect your login credentials and use caution when opening email attachments or clicking on links as these can introduce significant malware risk to the company. You should promptly report to InfoSafe any of the following incidents, whether suspected or actual:

- Data compromises, misdirected emails or lost documents
- Unauthorized attempts to access our network or workspaces
- Lost or stolen electronic equipment or badges, including permitted personal devices used to conduct business (e.g., smartphone)
- Social engineering, such as impersonation of a customer or employee
- Unauthorized access or upload of confidential or proprietary data
- Unusual database or system log anomalies

For more information:

- Employee Handbook
- Enterprise Fraud Risk Management Standard
- Information Security — Enterprise Policy
- Information Wall — Enterprise Policy
- Proprietary Rights and Information Agreement
- Applicable line-of-business-specific guidelines

Bank of America assets include, but are not limited to:

- Computer hardware and software innovations
- Customer lists or information
- Intellectual property
- Data processing systems
- Money and funds
- Databases
- Records
- Equipment
- Reference materials
- Furnishings
- Reports
- Files
- Supplies
- Ideas
- Technology
- Information about Bank of America's business, including corporate or customer transactions
- The company's information systems and private computer systems, including your email and your internet access

We comply with laws and regulations

You must not take any action, either personally or on behalf of Bank of America that violates any law, rule, regulation or internal company policy or procedure.

The Referral Management System (TRMS) *is used to report potentially suspicious or fraudulent activities. Learn more about financial crimes and how to report potentially suspicious activity through The Referral Management System (TRMS) on the Financial Crimes site under Risk Management on Flagscape.*

Anti-money laundering and economic sanctions

Money laundering is the process by which criminals attempt to make "dirty" money (derived from unlawful activities) look "clean" (as if from legitimate sources) by moving it through a financial institution.

Economic sanctions are foreign policy tools that impose strict limits on a range of activities, including providing financial services or conducting transactions. They are imposed by governments or international bodies to try to isolate or impede a specified individual, entity or jurisdiction for some specified purpose or activity.

These rules target people such as criminals who engage in activities that harm us and our communities (e.g., human trafficking, corruption, drug trafficking, fraud, wildlife trafficking and financing terrorism), as well as those who threaten national security.

We all have a role to play in helping to prevent criminals and targets of sanctions from using Bank of America's products and services. This includes an obligation to know our customers, identify and escalate suspicious activity, and escalate transactions with sanctioned countries, people or businesses. Learn how to do your part by visiting Financial Crimes under Risk & Compliance on Flagscape.

We must comply with anti-money laundering rules and economic sanctions, as we have an important role in allowing investigators to follow the money and to prevent criminals and sanctions targets from being able to access their funds.

Regulators around the globe have fined financial institutions billions of dollars for failing to meet their obligations under these rules.

For more information:

- Financial Crimes Enterprise Policy
- Financial Crimes Global Standard
- Financial Crimes Flagscape site

Facilitation of tax evasion

Bank of America may be exposed to reputational harm, or potential civil and criminal liability,[4] if those providing services (e.g., employees, agents, service providers and vendors) facilitate the evasion of taxes while working on behalf of the company.

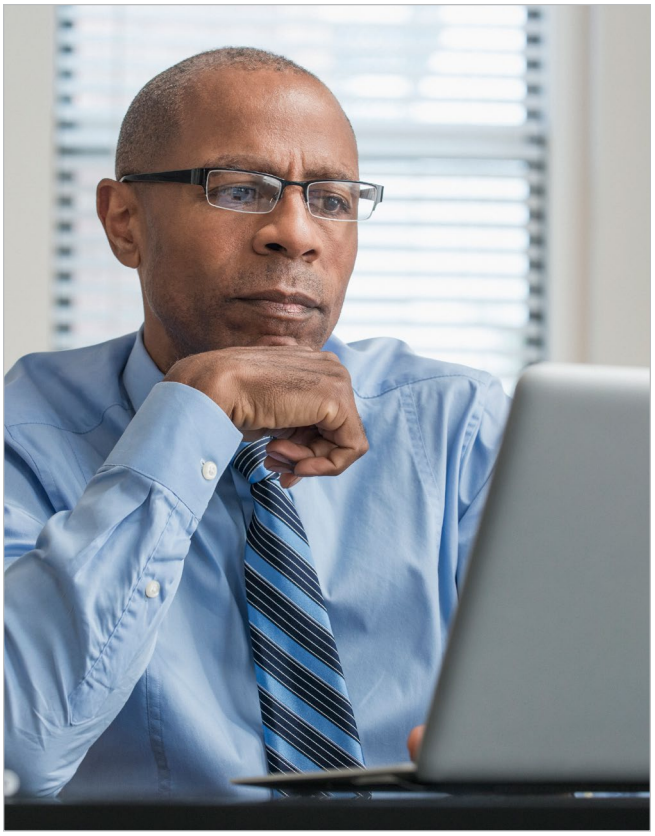
Tax evasion is dishonest non-compliance with tax rules (e.g., intentionally or recklessly not reporting income or capital gains, or not paying taxes owed). This should be distinguished from "tax planning," which involves neither dishonest conduct nor non-compliance.

Facilitation of tax evasion may occur where you become aware that a client (a corporate entity or an individual) dishonestly intends to evade paying the correct amount of tax and, either through your own conduct (such as the advice you give) or by intentionally ignoring dishonest conduct, you knowingly assist the evasion of taxes. This situation could arise in several ways but, as examples: as part of your role in structuring a transaction or setting up accounts you assist someone to evade payment of tax; or you are asked to remit money in an unusual way for the purpose of evading required tax obligations.

You are expected to be informed of and alert to this issue to ensure that you do not knowingly assist the evasion of taxes. Any knowledge or suspicion of tax evasion must be reported to Global Financial Crimes.

For more information:

- Financial Crimes Enterprise Policy
- Financial Crimes Flagscape site
- The Referral Management System (TRMS)
- Global Financial Crimes officer
- Compliance and Operational Risk officer



[4] The U.K. government, for example, has created offenses for corporate entities, such as the Bank and its subsidiaries, which make an entity criminally liable if someone acting on its behalf facilitates the evasion of taxes (wherever globally they may be payable).

Books and records

Accurate record keeping and reporting reflects on our reputation, our integrity and our credibility, each of which promotes the interests of our shareholders. You must maintain accurate books and records including, but not limited to, any system of record for customer transactions, bank financial records, etc., in compliance with legal, regulatory and operational requirements.

All employees responsible for the preparation of the company's financial statements, or who provide information as part of that process, must maintain and adhere to internal accounting and operating controls and procedures so that all underlying transactions, both within Bank of America and with third parties, are properly documented, recorded and reported.

In addition, we all have the responsibility to promote full, fair, accurate, timely and understandable disclosure in reports and documents that Bank of America files with or submits to regulators or other public communications.

For more information:

- Global Records Management — Enterprise Policy
- Global Records Management Standards

We conduct our financial affairs responsibly

You should conduct your personal financial affairs responsibly and keep your business expenses in order. You are responsible for your financial activities in the following areas:

Personal borrowing and lending

To avoid potential conflicts of interest, you may not personally borrow money from or lend money to customers or vendors, unless the loan is a transaction with an institution normally in the business of lending and is obtained on non-preferential terms.

In addition, borrowing money from or lending money to other employees (unless they are family members) is not permitted. The occasional loan of nominal value (such as for lunch, dinner or a social event that is promptly reimbursed) is acceptable, as long as no interest is charged.

For more information:

- Conflicts of Interest — Enterprise Policy
- Employee Handbook

Business expenses

To minimize financial and regulatory risk, you must report your business expenses accurately and in a timely manner in alignment with Enterprise policy requirements. You also must not use business credit cards for any purpose other than appropriate business expenses.

You may not make business purchases directly from or (unless specifically authorized) enter into contracts on behalf of the company with third parties, because the company has established requirements for efficient and compliant purchasing, contracting and payments for products and services acquired from third parties. You must submit and approve vendor invoices for payment promptly to avoid late payments that may result in financial, regulatory or reputational risk.

For more information:

- Employee Initiated Expense — Enterprise Policy
- Enterprise Expense Standard
- Third Party — Enterprise Policy

Personal accounts and fees

Misuse of Bank of America personal accounts and banking services (e.g., personal debit or credit cards issued through the bank), as outlined in the Employee Handbook, is prohibited. Additionally, you may not process transactions (e.g., refunding fees) unless you are permitted under existing policies to do so. Further, accepting personal fees or commissions for any transaction on behalf of Bank of America unless you are specifically authorized to do so is prohibited.

For more information:

- Conflicts of Interest — Enterprise Policy
- ABAC Gifts and Entertainment — Enterprise Policy
- Employee Handbook

We value each and every teammate

Diversity and inclusion

Our commitment to diversity and inclusion helps make our company a great place to work. The diversity of our employees — in thought, style, age, sexual orientation, gender, gender identity and expression, national origins, race, ethnicity, culture, disability, religion, veteran status and experience — makes us stronger, and is essential to our ability to serve our clients, fulfill our purpose and drive Responsible Growth.

Our diversity also provides fresh ideas and perspectives and, when coupled with inclusion, results in an innovative environment where employees can bring their whole selves to work, build careers and contribute to the Responsible Growth of our business.

We are honored to be recognized as a leader in diversity and inclusion, for our representation, progressive workplace practices and initiatives to promote inclusion.

For more information:

- Equal Employment Opportunity and Affirmative Action — Enterprise Policy
- Commitment To Employees With Disabilities
- Employee Handbook
- Diversity and inclusion Flagscape site

Harassment, Discrimination and Retaliation

At Bank of America, we are committed to promoting an inclusive and respectful work environment.

Discrimination, harassment and retaliation are unacceptable and contrary to the company's values. The bank does not tolerate unlawful discrimination or harassment of any kind, including but not limited to verbal, physical, visual, sexual and abusive conduct (bullying) as outlined in our Harassment, Discrimination and Retaliation Prevention — Enterprise Policy.

These expectations apply in the workplace, which includes events sponsored by the company or when you are engaged in business on behalf of the company or at other outside activities with a connection to employment or work (e.g., social activities with teammates, or recognition events), whether during or outside of normal business hours. These activities, including entertainment, must not be conducted at establishments where sexually explicit or other inappropriate entertainment is offered.

You should not tolerate discrimination or harassment and should report any such conduct experienced or observed to your manager, Human Resources/Employee Relations and/or the Ethics and Compliance hotline.

Reported incidents of prohibited behavior and/or retaliation will be investigated. Investigations are conducted thoroughly and in as discreet a manner as is possible based on the situation. If the company finds violations of this policy or other inappropriate conduct of a sexual, discriminatory or retaliatory nature has occurred, disciplinary action up to and including immediate termination from employment may result.

For more information:

- Harassment, Discrimination and Retaliation Prevention — Enterprise Policy

Workplace violence

Bank of America strives to provide a safe work environment in which employees treat each other with courtesy and respect and resolve any differences in a professional, non-abusive and non-threatening manner.

Workplace violence is prohibited and includes acts or threats of physical violence, but it also can include abusive conduct or behavior, such as harassment and bullying.

Possessing weapons, whether licensed or not, in the workplace or while engaged in business on behalf of the company is prohibited. We are all responsible for our behavior and for understanding how our conduct both inside and outside the workplace may affect others. We all have a responsibility to report inappropriate behavior before it escalates to violence in the workplace — if we see something, we say something. Please contact Human Resources if you need assistance.

For more information:

- Violence-Free Workplace — Enterprise Policy
- Violence-Free Workplace Flagscape site
- Employee Handbook
- Human Resources
- Security Operations Analysis Command Center (SOACC)

Domestic violence

Bank of America is committed to supporting employees experiencing difficulties because of domestic violence.

Domestic violence is a pattern of abusive behavior that is used by one partner to gain or maintain power and control of another intimate partner. Employees who require assistance in dealing with the impacts of domestic violence are encouraged to contact Human Resources, including the Life Event Services Domestic Violence Support Team, or Corporate Security. The company also prohibits the misuse of company property, vehicles, telephones, computers or the assistance of another employee to commit acts of domestic violence, including stalking, harassment or threats. Employees may contact the U.S. Life Event Services Domestic Violence team for support at lifeeventsupport@bofa.com.

For more information:

- Violence-Free Workplace — Enterprise Policy
- Violence-Free Workplace Flagscape site
- Employee Handbook
- Life Event Services on HR Connect
- Security Operations Analysis Command Center (SOACC)

Workplace safety

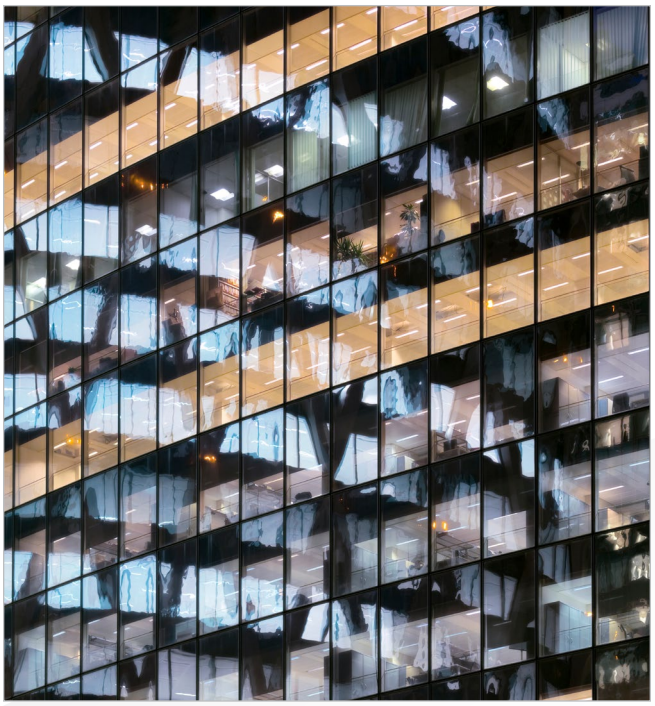
We are committed to the safety and security of our teammates around the globe. In order to avoid risk to yourself or those around you, you must follow all applicable safety and security procedures, as well as applicable laws, rules and regulations. You should report unsafe working conditions to your manager or Compliance and Operational Risk officer.

For more information:

- Safety and Security Flagscape site
- Security Operations Analysis Command Center (SOACC)

Business continuity

Our business continuity program focuses on placing the highest priority on the physical safety and security of our customers and employees, while preparing for loss of facilities and technologies. The goal is to provide uninterrupted service to customers and clients by recovering critical business functions and applications. For additional information, please visit Business continuity on Flagscape.



Safety and business continuity is everyone's responsibility. You must:

- Know the emergency response procedures for your building.
- Keep your personal contact information updated within Workday.
- Talk with your manager before a business interruption occurs so you understand your role in recovery. Stay in contact with your manager during and after disaster events.
- Maintain personal awareness and readiness for disaster events that may affect your area. Follow directions from local authorities during disaster events.
- Keep key contact information readily available at all times.
- Save Emergency Notification and Associate Communication Tool (ENACT) as a contact on your mobile phone(s) and respond appropriately to ENACT messages (you may be asked for your Person Number).
- Call the 24/7 security hotline (SOACC) to report life safety and security incidents, robberies, building security issues or any suspicious activity.

For more information:

- Business Continuity Management — Enterprise Policy
- Business Continuity Flagscape site
- Security Operations Analysis Command Center (SOACC)
- Workday

Resources

See below for an alphabetical list of policies and resources referenced in the Code (access noted)

Global Policy Source (internal)

Anti-Bribery Anti-Corruption (ABAC) — Enterprise Policy

ABAC Gifts and Entertainment — Enterprise Policy

ABAC U.S. Political Activities — Enterprise Policy

Business Continuity Management — Enterprise Policy

Commitment To Employees With Disabilities — Enterprise Policy

Commitment to Protecting Employee Information — Enterprise Policy

Compensation Governance — Enterprise Policy

Complaints — Enterprise Policy

Compliance Training Policy

Conflicts of Interest — Enterprise Policy

Country Whistleblowing Policies:

- Australia Whistleblowing Policy
- France Whistleblowing Policy
- India Whistleblowing Policy
- Ireland Whistleblowing Policy
- MLIQ Whistleblowing Policy
- UK Whistleblowing Policy

Data Management — Enterprise Policy

Drug Free Workplace and Alcohol — Enterprise Policy

Electronic Communications Retention — Enterprise Policy

Employee Initiated Expense — Enterprise Policy

Enterprise Expense Standard

Enterprise Fraud Risk Management Standard

Equal Employment Opportunity and Affirmative Action — Enterprise Policy

Financial Crimes Enterprise Policy

Global Background Check — Enterprise Policy

Global Compliance — Enterprise Policy

Global Records Management — Enterprise Policy

Global Records Management Standards

Harassment, Discrimination and Retaliation Prevention — Enterprise Policy

Information Security — Enterprise Policy

Information Wall — Enterprise Policy

Issues, Risks, Enterprise Sub-issues and Control Enhancements — Enterprise Policy

Outside Business Activities — Enterprise Policy

Privacy and Cross Border Data Movement — Enterprise Policy

Registration and Licensing — Enterprise Policy

Third Party — Enterprise Policy

Unfair, Deceptive, or Abusive Acts or Practices Prevention — Enterprise Policy

Violence Free Workplace — Enterprise Policy

Other resources

Guidance (internal):

Additional Guidance While Trading in Bank of America Securities

Applications with Compliant Retention Solution

Conduct Risk Management Program

Data Protection Notices (DPNs)

Electronic Communications Guide

2022 Bank of America Employee Handbook

2022 Risk Framework

Flagscape sites (internal):

Anti-Bribery Anti-Corruption

Business continuity

Business interests outside of primary employment

Conflicts of Interest

Diversity and inclusion

Environmental, social and governance

Financial crimes

Global Records Management

Global Regulatory Relations

Information Security

Intellectual capital and property, intangible assets

Newsroom

Privacy and cross border data movement

Risk Management

Safety and Security

Social media at Bank of America

Supplier Code of Conduct

Additionally, please note that versions in Spanish and Portuguese are available on our main BAC.com Supplier Management page.

Third Party Program

Contacts and systems:

Bank of America Media Contacts

Code of Conduct Mailbox

Employee relations

HR Connect

InfoSafe

Life Event Services

The Referral Management System (TRMS)

Workday

External websites:

Annual Reports & Proxy Statements

Bank of America newsroom

Central Bank of Ireland (CBI)

Ethics and Compliance Hotline

European Central Bank (ECB)

Financial Conduct Authority (FCA)

Prudential Regulation Authority (PRA)

Human Rights Statement

Whistleblowing Outside of the U.S. (EU directive disclosure)

Environmental and Social Risk Policy Framework

Investor Relations — Making an Impact

Notice

Code waivers

The board of directors must approve any waiver of the Code of Conduct for the chief executive officer, the chief financial officer, the chief accounting officer and any executive officer or director. The company will promptly disclose any such waiver on the Investor Relations portion of its website or through a press release or other public filing as required by applicable law, rule or regulation.

For more information:

- Investor Relations — Code of Conduct