



Responsible Business

Teamwork, respect, accountability, integrity, and leadership are core values at Key, driving our daily actions and decisions. We hold ourselves — and the third-party suppliers with whom we work — to high standards of ethical business practices. Our culture of continuous improvement and our strong risk management are strategic priorities. We continuously invest in new tools, technology, and processes that enable us to better manage the changing risk environment, from data security to anti-money laundering to evolving regulations.

<u>19</u>	<u>KeyCorp Board of Directors</u>
<u>22</u>	<u>Risk and oversight</u>
<u>25</u>	<u>Business conduct and ethics</u>
<u>27</u>	<u>Anti-money laundering</u>
<u>28</u>	<u>Fair and responsible banking practices</u>
<u>30</u>	<u>Data privacy and security</u>
<u>33</u>	<u>Political involvement and activity</u>



KeyCorp Board of Directors

Key is committed to meeting high standards of corporate governance, ethical behavior, and business conduct. Our corporate governance practices are longstanding strengths of our company.

We benefit from our Board's tremendous experience, independent leadership, diverse expertise, and commitment to Key. Independent leadership and oversight responsibilities are driven through our robust independent lead director role, independent Board committee chairs, and the full involvement of each of our independent directors. All directors elected at the 2023 Annual Meeting of Shareholders, other than Chris Gorman, are independent under the New York Stock Exchange's and KeyCorp's standards of independence. Our standing Board committees (Audit, Compensation and Organization, Nominating and Corporate Governance, Risk, and Technology) consist solely of independent directors. When searching for new directors, the Board considers whether the candidate would enhance the diversity of the Board in terms of gender, race, experience, and/or geography. The Nominating and Corporate Governance Committee (NCGC) utilizes a matrix approach that tracks each director's and director nominee's qualities and qualifications to assist the committee in maintaining a well-rounded, diverse, and effective Board.

Our Board is actively involved in the oversight of our strategies and in holding management accountable, both for the current year and the long-term performance of our company. The Board is focused on and dedicated to ensuring we execute in a manner that is aligned with shareholder expectations. Each year, the NCGC, led by the lead independent director, conducts a thorough evaluation process to assess the effectiveness of each of our directors.

Key also has a strong Executive Leadership Team that brings a wide breadth of knowledge and experience to the organization. The diversity of our team, coupled with extensive industry expertise, has driven sound, profitable growth at Key. Members of the team are dedicated to holding one another accountable while delivering on our commitments and maximizing long-term value.

Additional information about KeyCorp's Board of Directors can be found in the latest [Proxy Statement](#).

KeyCorp Board of Directors Demographics

46%

DIVERSE IN GENDER OR ETHNICITY

31%

WOMEN

23%

RACIALLY OR ETHNICALLY DIVERSE



A message from the Board of Directors

We are pleased to share Key's continued progress in advancing our corporate responsibility and sustainability priorities in 2023, including deepening our impact on financial inclusion and climate stewardship, implementing a more holistic climate risk framework, maturing information security and privacy programs, and strengthening diversity within our senior leadership ranks.

The achievements we've made can be attributed, in part, to making corporate responsibility and sustainability oversight and governance a board priority. These topics are integrated into the entire organization's governance structure, from the Board of Directors to the lines of business, improving Key's ability to manage risks and opportunities and drive operational excellence. In early 2022, we updated Board committee charters to include certain corporate responsibility and sustainability topics, reflecting a more contemporary structure for governance.

The Board plays an active role in ensuring risks and opportunities are integrated into Key's long-term business strategy, the company is measuring and monitoring progress against our commitments set as part of the strategy, and risks are well managed. Corporate responsibility and sustainability policies and practices are monitored closely by the Board's Nominating and Corporate Governance Committee, which oversees significant corporate responsibility issues.

Our annual Board of Directors' education day has included corporate responsibility, sustainability, and fair and responsible banking as featured topics over the past few years. We leverage industry experts to share best practices and an "outside-in" view of our progress and opportunities; this has been formative in shaping our corporate responsibility priorities and the path ahead.

We are proud of the investments we have made to become a more sustainable company and to support financial access and inclusion in the communities we serve. We recognize the significant work ahead to deliver the outcomes we aspire to achieve and look forward to sharing our progress.

Thank you for your interest in our efforts to support thriving communities and a more sustainable environment.



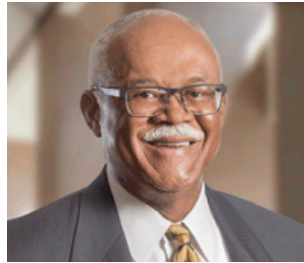
KeyCorp Board of Directors



Christopher M. Gorman
Chairman and Chief Executive Officer
KeyCorp



Alexander M. Cutler
Chairman and CEO (Retired)
Eaton Corporation



H. James Dallas
SVP, Quality and Operations (Retired)
Medtronic, Inc.



Elizabeth R. Gile
Managing Director (Retired)
Deutsche Bank AG



Ruth Ann M. Gillis
EVP and Chief Administrative Officer (Retired)
Exelon Corporation



Robin N. Hayes
CEO (Retired)
JetBlue Airways Corporation



Carlton L. Highsmith
Chairman, President, and CEO (Retired)
Specialized Packaging Group, Inc.



Richard J. Hipple
Executive Chairman (Retired)
Materion Corporation



Devina A. Rankin
EVP and CFO
Waste Management, Inc.



Barbara R. Snyder
President
Association of American Universities



Richard J. Tobin
President and CEO
Dover Corporation



Todd J. Vasos
CEO
Dollar General Corporation



David K. Wilson
Examiner-in-Charge (Retired)
Office of the Comptroller of the Currency



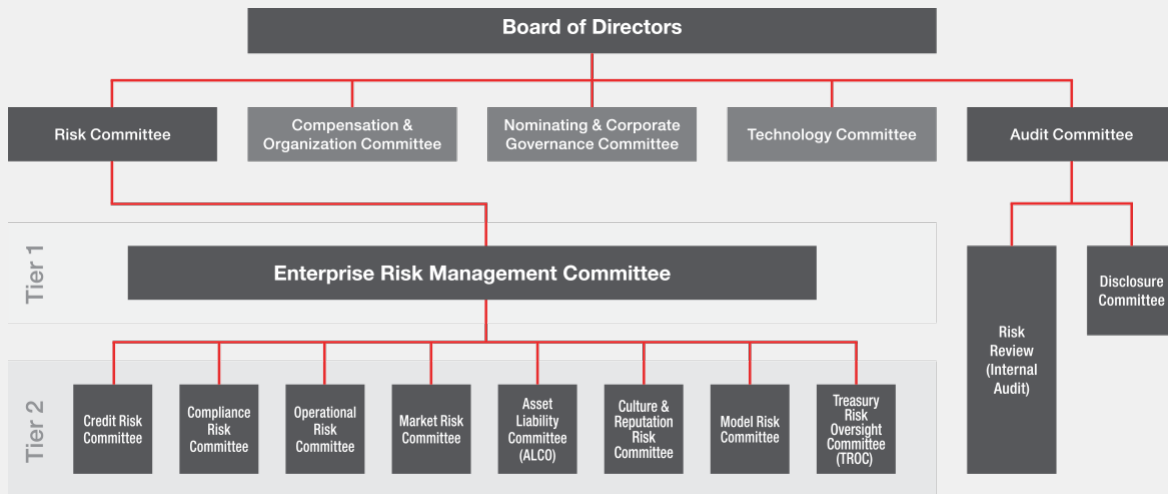
Risk and oversight

KeyCorp risk governance

Teamwork, respect, accountability, integrity, and leadership are core values at Key, driving our daily actions and decisions. We hold ourselves to high standards of corporate governance and ethical business practices. Effective governance is at the core of our company and its ability to manage all types of risks and opportunities for the benefit of our shareholders and other stakeholders.

Risk management responsibility

The table below depicts our risk management hierarchy.



Board of Directors oversight

Our Board of Directors approve our Enterprise Risk Management (ERM) Policy and sets the overall level of risk Key is willing to accept and manage in pursuit of our strategic objectives. The ERM Policy encompasses our risk philosophy, policy framework, and governance structure for the management of risks across the company. The ERM Policy also provides a framework for effective governance and regular review and challenge across our three lines of defense, as described in the [Managing risk at Key](#) section of this report.



Our standing Board committees (Audit, Compensation and Organization, Nominating and Corporate Governance, Risk, and Technology) consist solely of independent directors, and the committees regularly consider CR-related risks. For example:

Risk Committee

The Risk Committee oversees Key's risk management program and is responsible for strategies, policies, procedures, and practices related to the assessment and management of enterprise-wide risk. The Risk Committee reviews the ERM Policy at least annually.

The Committee also meets with senior leadership to review significant policies related to risk and opportunity assessment, identification, management, and compliance. KeyCorp and its officers maintain responsibility for designing, implementing, and managing programs and policies with respect to risk management.

Nominating & Corporate Governance Committee

CR topics are brought to the Nominating and Corporate Governance Committee of the Board at least once annually and are presented by the Chief Corporate Responsibility Officer.

The NCGC oversees KeyCorp's policies and practices on significant corporate responsibility issues, including ESG and sustainability, community and government relations, charitable and political contributions, community development, Community Reinvestment Act activities, and the fair and responsible treatment of clients.

Audit Committee

The Audit Committee of the Board considers climate-related issues through its oversight of the integrity of KeyCorp's financial statements, including reviewing disclosures made in our SEC filings.

Our Risk Review Group and Disclosure Committee fall under the Audit Committee.

Reporting to the Risk Committee of the Board is our Enterprise Risk Management Committee (ERMC), which is chaired by our CEO and provides governance, direction, oversight, and high-level management of risk, including the management of emerging and top risks. The committee meets regularly and ensures that the corporate risk profile is managed in a manner consistent with our risk appetite and assists in the ability to create sustainable value for our stakeholders.

In addition, there are management-level committees that report to the ERMC, which are a vital part of our governance framework and serve a critical purpose in enacting the appropriate governance for key initiatives. For example, the Culture and Reputation Risk Committee, chaired by the CEO, serves as the governance body providing oversight of risks related to risk culture, conduct, ethics, ESG, climate, brand, and reputation.



Managing risk at Key

Key remains disciplined in managing our risk and capital. We have maintained our moderate risk profile, including strong underwriting standards, and we have taken steps to position the company to perform through any business cycle.

To further align with the moderate risk appetite, Key employs “three lines of defense” for risk governance.

1	2	3
1st Line of Defense:	2nd Line of Defense:	3rd Line of Defense:
Lines of business and support areas	Risk Management	Risk Review (Internal Audit)
<ul style="list-style-type: none"> • Primary responsibility to accept, own, and proactively identify, monitor, and manage risk • Oversee line of business risk profile and report on status relative to desired risk profile • Manage within risk tolerances and partner with them in establishing and periodically refining tolerances • Integrate risk considerations into strategic decisions and management activities • Make informed decisions to optimize risk-adjusted returns and mitigate potential and actual risk issues • Primary accountability to escalate material risk issues or trends in a timely manner • Establish procedures and processes as necessary to ensure compliance with policies • Adhere to Key’s risk management policies, practices, and controls 	<ul style="list-style-type: none"> • Provide independent, centralized oversight over all risk categories by aggregating, analyzing, and reporting risk information • Provide holistic, integrated view of the corporate risk profile and report on status relative to desired corporate risk profile • Design and maintain the ERM Policy and Program • Create robust review and challenge processes and ensure an understanding of risk interdependencies • Provide the appropriate risk infrastructure to support the lines of business, including policies and subject matter expertise • Act as a trusted advisor to the lines of business in managing acceptable levels of risk, anticipating a range of business conditions, and optimizing revenue • Exercise authority as needed to ensure risks are managed at acceptable levels, including escalation of material risk issues 	<ul style="list-style-type: none"> • Primary responsibility to accept, own, and proactively identify, monitor, and manage risk • Provide independent assessment and testing of effectiveness, appropriateness, and adherence to KeyCorp’s risk management policies, practices, and controls • Provide an independent, aggregate view of risk • Validate the ERM Policy and Program design and evaluate its effectiveness • Recommend improvements for ERM and other risk practices • Provide objective review of accountabilities, escalation activities, and quality/timeliness of issues resolution • Interface with external auditors

The three lines are balanced in importance and stature, and they must all operate effectively across the enterprise to sustain strong risk management. Risk appetite is considered as strategic alternatives are evaluated, performance objectives are established, and mechanisms are strengthened to manage risks.

Key maintains a strong risk culture through proactive risk management activities integrated into business processes as well as employee risk awareness training.



Living our values through the Code

Key maintains the highest standards of ethical behavior throughout our operations. Our Code of Business Conduct and Ethics (the Code) is critical to how we fulfill our purpose and create the type of environment we promise to our employees. Our five core values — teamwork, respect, accountability, integrity, and leadership — guide and inspire our daily actions. These are explained in more detail on page 10. Together, the Code and our values reinforce our responsibility to make good choices and to act according to the highest professional and ethical standards in everything we do.

Administration of the Code

The Chief Ethics Officer leads Key's Corporate Ethics Office, which is responsible for the administration of the Code, Key's ethics program, and oversight of conduct investigations. The ethics program is designed to deter and detect unethical or illegal employee conduct and to provide guidance and review of outside business and professional activities. The Code is the foundation for the ethics program. We continually monitor the efficacy of the ethics program, including risk and control testing. These results are reported to the Culture and Reputation Risk Committee as well as the Audit Committee of the Board.

The Code is our first source of guidance when making decisions in the course of our duties. In addition, Key has Human Resources and line of business policies and standards that set expectations for behavior, including Key's Professional Conduct Policy.

Each teammate and member of our Board of Directors is responsible for understanding, adopting, and upholding all principles and requirements within the Code and protecting and maintaining Key's reputation. The Code is reviewed annually and updated to ensure coverage of new ethical issues that arise.

Understanding and complying with the Code are also part of Key's risk management program. New employees are provided, and are required to complete, the Culture, Conduct and Ethics training and certification upon joining Key. In addition, all Key teammates and directors are required to successfully complete mandatory ethics training in a timely manner and are required to review and certify their understanding of the Code annually. At the end of 2023, 95%⁴ of employees and 100% of directors completed this requirement.

In 2023, Key updated the Code by streamlining guidance about where to seek help while reminding teammates that they should feel comfortable speaking up whenever they have concerns.

Code of Ethics Officer

Each line of business and support area has a dedicated Code of Ethics officer who is specially trained to respond professionally and as confidentially as possible to ethics and other potential violations.

The dedicated Code of Ethics Officer is an expert for any Code-related questions (either general or specific), such as those concerning limits on gifts and entertainment, running for political office, or other business-related ethical concerns, and is supported by the Corporate Ethics Office.

⁴ Our goal is for 95% of employees to complete annual Code training; this allows us to accommodate new hires and employees who may be on extended leave.



Report a concern

Key's employees and Board of Directors are obligated both to comply with the members of Code and to speak up when they suspect or witness a potential violation of the Code. Individuals can report concerns to a Code of Ethics Officer, contact the Ethics Office, call Key's Ethics Helpline, or complete an online form on Key's intranet or from their personal computer.

Key's Ethics Helpline (administered by an independent third party) is available toll-free 24 hours a day, seven days a week. The Ethics Helpline allows teammates to report a possible Code violation without necessarily revealing their identity, if they choose to remain anonymous.

Non-retaliation

Key is committed to supporting and sustaining the integrity of our company.

Teammates are encouraged to speak up if they suspect any unethical activity or behavior at Key. We do not permit any retaliation against employees for reports of suspicious activity made in good faith, and reporters will not be subject to disciplinary action for making a report in good faith.

All investigations of employee misconduct concerning the Code will be handled promptly and in as confidential a manner as possible. If the investigation results in disciplinary action for an employee, documentation of the action will be placed in their employment file.

Business conduct

We conduct our business in a highly regulated environment. We are obligated to comply with all applicable country, federal, state, and local laws, rules, and regulations. This includes all applicable securities laws and regulations, accounting standards, accounting controls, and auditing practices.

Anti-tying

We provide a choice of financial products and services designed to meet our clients' needs; however, certain products and services may not be "tied" to other products and services to complete the transaction.

"Tying" occurs when the "sale" or delivery of a service or product is contingent on the purchase or delivery of another service or product. An employee may not require a client to purchase or engage in a nontraditional product or service as a condition for that client receiving certain terms and conditions for another product or service. Avoiding the improper tying of services and products will ensure we remain in compliance with anti-tying laws and maintain our clients' trust.

Anti-bribery and anti-corruption

We are committed to compliance with all applicable anti-bribery and anti-corruption laws, including, but not limited to, the U.S. Bank Bribery Act, the Anti-Bribery & Corruption Policy, and the U.K. Bribery Act. Key employees, directors, service providers, and agents acting on Key's behalf must act with transparency and integrity in all business dealings. We follow all government requirements. Bribery comes with severe civil and criminal penalties, so it is important that employees are aware of anti-bribery and anti-corruption laws to avoid inadvertent violations and be able to quickly recognize concerns so they can be addressed in a timely manner. Bribes include actions taken to influence others or to be influenced to gain an improper business advantage for Key. Employees may never offer, provide, solicit, demand, authorize, promise, or accept a bribe.

Anti-bribery and anti-corruption training is included in the annual mandatory Code training.

Key's Public Entities Policy strictly prohibits gifts and entertainment for public officials unless prior approval is received. If employees are offered or receive something of value from a client or third-party service provider outside of the allowable limits of the Code, it must be disclosed to the Ethics Office in a timely manner.

In order to ensure transparency and comply with applicable anti-bribery and anti-corruption requirements, teammates must accurately, and in a timely manner, document expenses related to gifts, entertainment, monetary payments, and other things of value in compliance with Key's finance and expenditure policies.



Anti-money laundering

KeyCorp fully supports the U.S. federal government's efforts to combat terrorism and money laundering.

Key maintains a program of financial crimes governance policies, procedures, and guidelines specifically designed to comply with all U.S. Anti-Money Laundering (AML) and counter-terrorist financing laws. These policies, procedures, and guidelines apply equally to both Key's domestic operations and international activity. Key's policies are designed to reduce the likelihood that the corporation, any subsidiary, or any employee will become the victim of, or unknowingly participate in, any illegal activity. These policies help fight terrorism and money laundering and protect customers from losses from fraud and other illegal activity.

Key's Financial Crimes Governance policy is reviewed and approved annually by the Risk Committee of the KeyCorp Board and the KeyBank National Association Board of Directors. Key also maintains an Anti-Corruption compliance program, including a Foreign Corrupt Practices Act policy and Code of Business Conduct and Ethics.

As part of its AML program, Key maintains reasonable procedures to determine the identity of each prospective customer and ascertain whether they are on the Office of Foreign Assets Control (OFAC) list or a similar list provided by a U.S. governmental or regulatory body prior to initiating a business relationship. Key maintains record retention policies compliant with applicable laws. In addition, Key performs risk-based customer due diligence in order to assist Key in the identification of potentially high-risk customers.

Key takes its regulatory obligations seriously and is committed to meeting all applicable compliance requirements.

Key's customer due diligence program includes, but is not limited to, the following:

- Establishment and maintenance of written procedures that are reasonably designed to identify and verify beneficial owners of legal entity customers, as mandated by federal regulations, as well as collection of beneficial ownership at lower equity thresholds for higher risk customers and periodic screening of all beneficial owners for OFAC, as well as periodic political exposure screening for foreign beneficial owners and/or beneficial owners of foreign associated legal entity customers
- Policies and procedures covering relationships with senior foreign political figures, their families, and close associates (collectively known as politically exposed persons or PEPs), and periodic PEP screening of Key's foreign-affiliated customer base using a risk-based methodology
- Risk rating of the customer base
- Collection of documents, such as the customer's AML program and business license, as applicable, and other due diligence information using a risk-based methodology
- Ongoing/periodic enhanced due diligence, including transaction review and negative media screening for high-risk customers
- Certain high-risk customer types, such as PEPs, Money Services Businesses, and Foreign Correspondent Banks, are subject to approval of the Chief Anti-Money Laundering Officer
- Policies prohibiting accounts/relationships with certain customer/business types, including but not limited to, shell banks and payable-through accounts to cannabis-related businesses
- Key also has implemented other reasonable controls, including monitoring of our customer base and their transactions to aid in the identification of potentially suspicious activity. Key requires AML training at onboarding for new employees and annual AML training for employees, directors, and applicable third parties. An annual independent testing review is conducted of Key's AML program. Key's AML program applies a risk-based approach to all activities and operations.



Our commitment to fair and responsible banking

Fair and responsible banking (FARB) is the right thing to do for our clients and communities and is a high priority for Key. FARB is also an ongoing focus of our regulators and community organizations. Key provides comprehensive financial solutions to help clients achieve their goals of financial wellness, and we strive to create lasting positive impact in the communities we serve. Our mission is to remove, or empower people to remove, the barriers between themselves and financial wellness.

Key is committed to treating each client with integrity and respect and to providing quality service that is prompt, competent, diligent, and courteous. Moreover, Key's goal is to help every client understand available products and services so that they can make informed financial decisions that are the most appropriate for their circumstances. Integral to this vision is a commitment to fair, consistent, and responsible treatment of consumers and customers.

FARB laws, regulations, and regulatory guidance apply to all of Key's business functions, employees, and third parties acting on Key's behalf and are implemented throughout Key and its subsidiaries. The same principles of anti-discrimination and fairness apply to all employees, including customer relations, through Key's [Code of Business Conduct and Ethics and the Professional Conduct Policy](#). Our FARB policies, programs, and practices are designed to proactively identify, measure, monitor, control, and report FARB-related risks; provide a credible challenge of business activities across products and services; and support effective risk management activities related to fair lending and unfair, deceptive, abusive acts or practices (UDAAP).

FARB/CRA Risk Committee

The FARB/CRA⁵ Risk Committee was formed in 2021 to oversee fair and responsible banking and Community Reinvestment Act risk activities and assure conformance with regulatory requirements, bank policies and procedures, and the KeyCorp Board-approved Risk Appetite. The FARB/CRA Risk Committee monitors reporting. It provides oversight and guidance to the organization's management of fair and responsible banking and CRA risks, trends, and issues across business segments, products, and functional areas. The Committee operates as a subcommittee of the KeyCorp Compliance Risk Committee under the KeyCorp Enterprise Risk Management Policy which is managed and overseen by the KeyCorp ERM Committee.

Responsible sales and lending

Our teammates apply FARB principles to every aspect of a client's interaction and transactions. They are instructed to be consistent, follow their line of business policies and procedures diligently, and escalate any potential violations or concerns to their manager. Teammates strive to make sure our clients are fully informed about a product's risks and benefits before a client makes a product decision.

Our commitment to fairness and equity is demonstrated in the investments Key has made to help under-resourced communities and low- and moderate-income clients with ways to save money, pay down debt, buy a first home, start a business, and empower them to pursue other financial goals.

Other actions in 2023 include Key's launching of a targeted marketing outreach campaign to reach historically under-resourced neighbors and neighborhoods, including direct mail, radio spots, bus wraps, billboards, and social media posts.

⁵ The Community Reinvestment Act of 1977 (CRA) encourages certain insured depository institutions to help meet the credit needs of the communities in which they are chartered, including LMI neighborhoods, consistent with the safe and sound operation of such institutions. <https://www.occ.gov/topics/consumers-and-communities/cra/index-cra.html>



Listening to clients

We have a diverse client base. Understanding their evolving needs and experiences is critical to our success. That's why we employ a variety of methods to gather feedback from clients. We recently redesigned our client surveys to gather more meaningful insights and launched them from a new, state-of-the-art experience platform.

We evaluate themes uncovered in client feedback and deploy new approaches to drive action. Social media is another important communication tool; our highly experienced Social Customer Care team closely monitors social media channels and manages follow-up communication as appropriate. We also solicit client feedback in the design and development of new products via our client panel called Voices.

Managing complaints

Client feedback provides us with an equally important opportunity to make improvements to the way we conduct business. Key's dedicated customer service professionals, including our Social Customer Care team, are trained to appropriately respond to complaints and ensure issues impacting our clients are thoroughly addressed. A variety of channels are available to Key's clients to make us aware of their concerns, and Key uses a number of monitoring systems to scan for critical feedback via client surveys and digital channels. Our Customer Service and Social Customer Care teams resolve most complaints directly. For those that require additional support or raise more serious concerns, there are clear escalation processes in place. Complaints alleging discrimination or similar unfair treatment, for example, are escalated to the Fair and Responsible Banking Complaint Management team to ensure timely, thorough, and appropriate investigation and resolution.

Furthermore, Key uses complaint data to identify trends and areas for enhancement and to inform management of opportunities to improve the customer experience.

Employee training and reporting

Teammates receive mandatory training, based on their role at Key, on a range of topics including FARB (e.g., Fair Lending and UDAAP), anti-money laundering, consumer advertising compliance, Key's Code of Business Conduct and Ethics, managing risk, protecting Key's assets, and fraud awareness and escalation.

We require teammates to report any suspected regulatory violations, including Fair Lending and UDAAP, to their manager or the ethics helpline. These reports remain as confidential as possible, and teammates are protected against retaliation (e.g., termination, demotion, harassment).





Data privacy and security

Maintaining the protection and security of the personal and financial information of our clients and employees, as well as other individuals with whom we come into contact, is one of Key's highest priorities. Strong data safeguards and controls, in conjunction with continuous monitoring of the threat landscape, help protect the security and privacy of the information entrusted to Key. As the information security threat landscape continues to evolve, we will remain focused on our ability to align with industry standards to protect information, use it lawfully, and manage threats or incidents as they arise.



Our information security and privacy programs are continuously maturing. We make ongoing investments in technology and solutions to enable us to better manage the evolving regulatory and security environment.

Critical information security and fraud initiatives include:

- Strengthening endpoint protections, event monitoring and analytics, and modernizing Identity & Access Management processes and controls
- Enhancing fraud detection capabilities and improving efficiency in case management and disputes resolution
- Evolving client access and authentication as the demand for a digital-first client experience continues to increase

Key's security and privacy controls are regularly reviewed to align with industry standard practices, evolving laws, and changing client expectations.

Information security governance and oversight

Our Chief Information Security Officer and Enterprise Security Services Director regularly report to Board-appointed committees on the status of Key's information security program. The Technology Committee of the Board is responsible for approval of the enterprise's technology strategic plan, including cybersecurity technology. Risk management issues are escalated to the Risk Committee of the Board. The Risk Committee is the approving body for our Information Security Policy and provides oversight in its development and execution.

Additional details about our risk governance structure can be found in the [Risk and oversight](#) section.

Cybersecurity audits and assessments

We regularly conduct internal and external penetration tests of our environment and maintain a robust third-party security program to affirm our cybersecurity posture. We benchmark ourselves at least annually against industry-leading frameworks, including, but not limited to, the National Institute of Standards and Technology Cybersecurity Framework and the Cyber Risk Institute Profile. Lessons learned from these assessments are used to inform and develop our program.

Key is subject to cybersecurity and privacy regulatory exams as required by law for financial institutions operating in the U.S.

Key's Risk Review Group conducts independent internal audits of our lines of business, operations, information systems, and technologies. Internal audits provide an independent perspective on Key's processes and risks by using a systematic, disciplined approach to evaluate, test, and improve the effectiveness of risk management, control, and governance processes. A risk-driven process is used to assess significant categories of risk. Technology risks are evaluated in areas including cyber and information security, data control, acquisition and development, delivery and support, business continuity, and information technology governance. Results of internal audits are shared with line of business management, Key's Operational and Compliance Risk Management groups, Key's Audit Committee, and banking regulators to provide an adequate level of transparency. Any identified gaps are rated, issued a due date for remediation, and tracked through completion of remediation. Remediation is verified by the Risk Review Group.



Incident management

When an incident is identified, we follow established processes in our enterprise privacy and cyber incident response plans, which are supplements to our corporate incident response plan. They provide a framework to enable the Enterprise Cyber Response team to effectively recover operations in the event of a cyberattack and to effectively manage incidents impacting bank information, including our clients' and employees' information.

Our Core Incident Response Rapid Emergency Assessment and Coordination Team (Core IR REACT) is responsible for responding to incidents, including cyberattacks, performing a preliminary assessment, and engaging additional support team members as necessary. The Core IR REACT team is a multidisciplinary team that is empowered to escalate issues, as appropriate, to our Crisis Management Team (CMT), which includes the CEO and the most senior executives from Key's lines of businesses and major support areas. The CMT provides overall strategic direction for incident response and recovery.

Key's Privacy team assesses all incidents that involve or may involve personally identifiable information to drive adherence to applicable laws. This may include notifying impacted individuals, regulators, and other required parties.

How Key safeguards client data and information:

- **Robust security for online accounts:** We leverage advanced data protection, strong encryption, and continuous monitoring to protect our clients' accounts.
- **Online banking security:** Our online banking has strong sign-on requirements to protect clients' sensitive information.
- **Security alerts:** To help protect financial accounts, we regularly share security and fraud alerts with clients.

Data privacy

Key's internal Privacy Policy governs the lawful processing of personally identifiable information across our entire organization, including our affiliates and subsidiaries, and our contracted service providers that are engaged to provide services on our behalf. The policy sets industry best practices as minimum requirements to the processing of personally identifiable information. It encompasses the complete life cycle of data including collecting, using, sharing, accessing, protecting, handling, retaining, and destroying data.

Our privacy practices adhere to applicable state and federal privacy laws and regulations for financial institutions.

Privacy governance and oversight

Key's dedicated Privacy team is led by our Chief Privacy Officer (CPO). The Privacy team is part of the broader Compliance team, which reports into the Compliance Risk Committee (CRC). The CRC reports to the Enterprise Risk Management Committee. Our CPO plays an active role on our governance committees. The CPO and Privacy team have the power to escalate privacy risks up through the Board.

Additional details about Key's risk governance structure can be found in the [Risk and oversight section](#).

The Privacy, Cybersecurity, and other Risk teams work closely together to implement appropriate controls around how personally identifiable information is managed and protected and to maintain Key's compliance with applicable laws and regulations.



Privacy information usage and sharing

Our [online privacy statement](#) explains how we maintain the privacy and security of personally identifiable information (PII). It details how we collect, use, share, and safeguard information and also explains the privacy rights afforded to individuals under applicable laws. Embedded in this statement is our privacy notice to consumers.

Key's [privacy notice for consumers](#) describes how we collect and protect PII about our consumers, the type of information we share with others, and why. It also explains how clients can limit certain types of information sharing. Key does not sell PII and only shares this information with contracted third parties that assist us in servicing accounts and to facilitate our banking relationships with our clients and employees or as otherwise required by law.

Privacy and security training and education

Key remains focused on providing information security and privacy education to our employees, clients, and the communities we serve.



Teammate engagement

Key executes on robust cybersecurity, privacy, and fraud education and awareness programs to educate teammates on identifying and reporting cybersecurity and privacy concerns. Throughout the year, we provide ongoing education and awareness campaigns for teammates that focus on topics such as reporting a suspected cybersecurity threat, phishing and social engineering threats, fraud scams, identity theft, and security best practices. These campaigns are communicated through emails, company intranet articles, webinars, and "lunch and learn" sessions. All employees participate in mandatory enterprise-wide cybersecurity, privacy, and fraud training on an annual basis.

Client engagement

Client security is one of Key's highest priorities. We provide clients with information and standard industry practices to keep individuals and businesses safe in a digital world. We encourage clients to report suspected fraudulent activity and suspicious emails via our dedicated phone line and email address. Throughout 2023, we created 45 educational assets for clients that focused on cybersecurity and privacy best practices, identifying different fraud scams including account takeover, ransomware, business email compromise, and social engineering. Assets were promoted through client emails and account alerts, social media posts, newsletters, webinars, and information on Key's website.

Community engagement

Key engaged with secondary schools, colleges, and universities to provide cybersecurity education and awareness and promote technology and cybersecurity careers. We participated in numerous career day events at local high schools, providing information on the importance of keeping PII secure and promoting careers in cybersecurity.



Corporate Political Activity

Corporate political activity principles statement

For the fourth year in a row, KeyCorp was distinguished as a Trendsetter for our political policies and related disclosures by the CPA-Zicklin Index of Corporate Political Disclosure and Accountability.

An important part of Key's commitment to our communities includes active participation in public policy advocacy and the political process. While corporations and national banks are limited or prohibited by law from making political contributions, we believe it's critically important to take a constructive role in the political process that will shape the future of our industry and its impact on our communities. Based on this premise, KeyCorp, through our Government Relations department, seeks to: 1) conduct political activity in accordance with all laws and regulations; 2) follow approved policies and procedures monitored by our Law Group and Compliance department; and 3) clear potential conflict provisions within our Code of Business Conduct and Ethics overseen by our Chief Ethics Officer.

Board of Directors oversight

The Nominating and Corporate Governance Committee of KeyCorp's Board of Directors meets annually with a member of Key's Government Relations team to review Key's policies and practices regarding political contributions. Policies and practices reviewed by the Committee include Key's policies regarding doing business with public entities; the Government Relations preapproval process for ballot issue support; substantive changes to regulations, if any, affecting Key's sponsored separate, segregated funds; corporate political activity; and confirming that Key does not contribute corporate funds to candidate campaigns for election.

Key's Government Relations program utilizes in-house government relations professionals and contract lobbyists to advocate on our behalf. Key complies with lobbying and disclosure laws. Our reportable federal lobbying expenditures for 2023 totaled \$860,000.

Trade association membership

KeyCorp is a member of several industry trade associations at the national, state, and local levels. These organizations support initiatives that align with our commitment to our communities, which include initiatives that would make a positive impact on our ability to do business, spur economic growth, and enhance the quality of life in the communities we serve, including diverse, equitable, and inclusive policies.



American
Bankers
Association®



CONSUMER
BANKERS
ASSOCIATION



National Association of
Affordable Housing Lenders

These associations work to develop industry consensus and advocacy, enabling us to reach government officials more efficiently and in a coordinated manner with peers in the financial services industry.

\$860,000

REPORTABLE FEDERAL

lobbying expenditures for 2023



Corporate political spending

KeyCorp does not contribute corporate funds for election campaigns. This includes prohibiting supporting candidate committees, political parties or committees, or political action committees (PACs) organized for the advancement of political candidates or Super PACs or the making of independent political expenditures.

Key may make contributions in support of certain ballot issues. These issues support the interests of our businesses, our employees, and/or our communities. Ballot issue requests are reviewed by Key's Law Group and then submitted to the executive leader of Key's Corporate Center for final approval. Contributions for approved ballot issues are reviewed annually by the Nominating and Corporate Governance Committee of the Board of Directors and are disclosed semi-annually on the [Corporate Governance page](#) of key.com.

Political action committees

Eligible officers, managers, and professional employees of KeyCorp can voluntarily participate in the political process by making an individual contribution to the PAC sponsored by KeyCorp.

Information regarding contributions by the KeyCorp Advocates Fund and the KeyCorp Advocates Fund – Federal is publicly disclosed and accessible at [fec.gov](https://www.fec.gov).

Information for the KeyCorp Advocates Fund – New York can be found at elections.ny.gov.

Compliance

Key is committed to complying with all applicable laws and regulations regarding political activity. We publish internal communications guidance for teammates, host regular training, review compliance protocols and systems, and conduct internal audits to ensure all political activity and lobbying activity are followed according to the law and our Code of Business Conduct and Ethics.

