Responsible Business

At Key, our core values of teamwork, respect, accountability, integrity, and leadership guide our daily actions and decisions. Strong corporate governance and high standards of ethical business practices are the foundation of our company, and we uphold these standards for ourselves and for the third-party suppliers with whom we collaborate. Continuous improvement and robust risk management continue as strategic priorities. We consistently invest in new tools, technology, and processes to effectively manage the evolving risk landscape and regulatory changes.

Governance philosophy

Strong corporate governance by company leaders, a commitment to ethical business practices, and living our corporate values enable Key to manage all types of risks and opportunities for the benefit of our shareholders and other stakeholders.

Board of Directors

At Key, our Board of Directors (the Board) is the top governing body of the organization. The Board oversees corporate governance, enterprise risk management, and compliance. The Board sets our company goals and establishes expectations for ethical business practices. The Board also works with management through the Board committee structure to ensure clear decision-making and accountability.

We benefit from our Board's experience, independent leadership, 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 of our directors, other than Christopher Gorman, are independent under the New York Stock Exchange's and KeyCorp's standards of independence.

> Additional information about KeyCorp's Board of Directors can be found in the latest Proxy Statement.

The Board oversees our corporate strategies and holds management responsible for current and long-term performance. Our Board focuses on ensuring our actions align with shareholder expectations.

Standing committees of the Board

Our standing Board committees — Risk; Nominating and Corporate Governance; Audit; Compensation and Organization; and Technology — consist entirely of independent directors, and they regularly evaluate CR-related risks.

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 Enterprise Risk Management 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 for 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.

This committee oversees KeyCorp's policies and practices on significant corporate responsibility issues, including sustainability, community and governmental relations, charitable and political contributions, community investment strategy and 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 report to the Audit Committee.

KeyCorp Board of Directors

Christopher M. Gorman
Chairman and Chief Executive Officer
KeyCorp

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

Jacqueline L. Allard
Group Head, Global Wealth Management
Scotiabank

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
Chairman and CEO
Airbus of North America

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

Richard J. Hipple
Executive Chairman (Retired)
Materion Corporation

Somesh Khanna
Co-Executive Chairman
Apexon, Inc.

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

Barbara R. Snyder
President
Association of American Universities

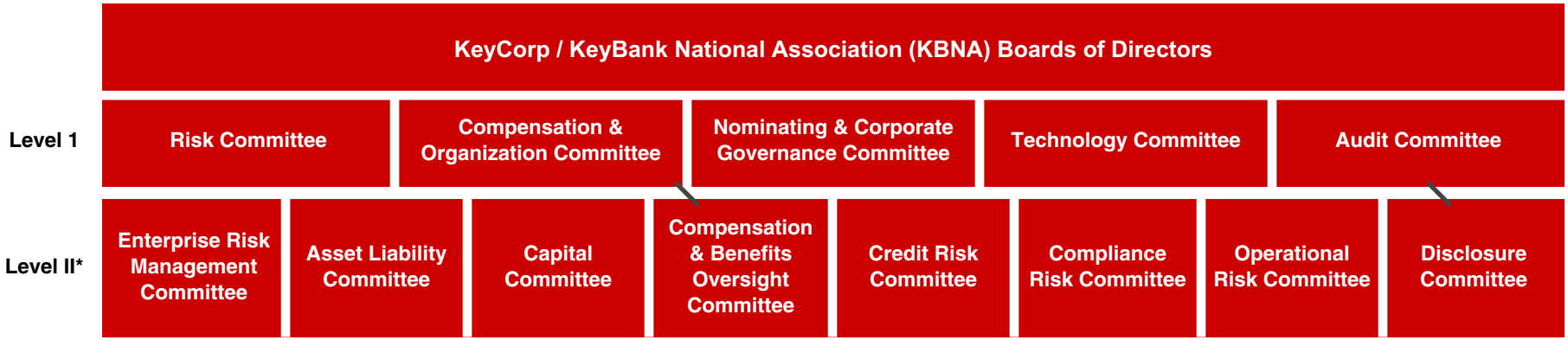
Richard J. Tobin
President and CEO
Dover Corporation

Todd J. Vasos
CEO
Dollar General Corporation

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

Risk Governance Committee Structure

The following table depicts our risk governance hierarchy.



*Level II Committees align to Risk Committee unless otherwise noted

Board oversight of risk

The Board oversees that KeyCorp's risks are managed in a manner that is effective and balanced and adds value for KeyCorp's shareholders. The Board understands KeyCorp's risk philosophy, approves KeyCorp's risk appetite, inquires about risk practices, reviews portfolio of risks, compares actual risks to the risk appetite, and is apprised of significant risks, both current and emerging — and determines whether management is responding appropriately. The Board actively challenges management and promotes accountability in all areas it oversees, including risk management.

Enterprise Risk Management Policy

The Board approves 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 managing risks throughout 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.

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

In addition, there are a comprehensive set of other management-level committees that are a vital part of our governance framework.

Managing risk at Key

Key remains disciplined in managing our risk and capital. We continue to maintain our moderate risk appetite — including strong underwriting standards — and we continually take steps to position the company to perform through any business cycle.

The foundation for risk management

At Key, effective risk management begins with a thorough understanding of our business. This includes a nuanced understanding of the inherent risks within our operations, systems, and processes, and a clear understanding of the external risks that may affect our business from end to end. Everyone at Key is a risk manager, and we continue to focus on driving active risk identification and management by integrating these activities into business processes and training employees on risk awareness.

Key Impact |

How GenAI is Helping Key Manage Compliance Risk

Generative AI (GenAI) is a new technology whose popularity and use have grown rapidly worldwide over the past two years. At Key, we are managing GenAI risk while starting to take advantage of the benefits that the technology can provide. GenAI use cases are evaluated for value and risk through established bank processes. In addition, Key provides training to teammates so they understand GenAI's risks and benefits as they learn to use it effectively and appropriately. Related to Key's use of GenAI in the Compliance Risk space, one of the first approved uses of GenAI at Key is a tool that monitors applicable regulatory and statutory changes. This tool enables our compliance and legal teams to quickly and comprehensively identify and track legal changes efficiently, with appropriate human oversight and input.

Three lines of defense

Key's risk management framework employs "three lines of defense" to manage and govern risk across the organization.

First Line of Defense — Lines of Business and Support Groups
With daily client interactions and other "frontline" and support activities, the LOBs and support groups, along with their management teams, are the First Line of Defense from a risk management perspective at Key. They are also expected to operate within Key's overall Risk Management Framework, and adhere to policies, procedures, and (if applicable) designated limits. Through the First Line of Defense role, managers and employees are responsible to identify, manage, and escalate risk. They acquire and maintain a business understanding of current and emerging laws, regulations, and industry practices. They make decisions about the risk-rewards of their daily activities based on their departments' policies and procedures. LOBs and support groups manage and oversee their own risk profiles for the different types of risk.

Second Line of Defense — Risk Management
Risk Management provides independent, centralized oversight of risk-taking activities at Key. Risk Management aggregates, analyzes, and reports risk information on all risk categories across the enterprise.

The team regularly reviews and challenges conclusions that the LOBs and support groups make about their risk levels. Risk Management also administers the Enterprise Risk Management Policy that ensures the consistent management and reporting of risks across the organization.

Third Line of Defense — Risk Review Group
The Risk Review Group functions independently from the LOBs, support groups, and Risk Management. It conducts independent reviews of the first and second lines of defense and decides on the effectiveness of the control environments in those areas.

The three lines of defense 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 'Moderate Risk Appetite'

Key's Moderate Risk Appetite is designed to allow the company to remain profitable through various business cycles and to support soundness, profitability, and growth.

Major risk categories

Key has identified nine major risk categories. These different risk types are often interrelated and affect various parts of the company.

Business conduct and ethics

At Key, we uphold the highest standards of ethical behavior in all 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. The Code is reviewed and updated annually by our Ethics Office, with updates vetted by the Enterprise Risk Management Committee. The Code is then reviewed and recommended for approval by the Audit Committee of the KeyCorp Board of Directors, and reviewed and approved by the KeyCorp Board of Directors.

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.

Ethics and compliance training

All Key teammates and directors are required to 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 2024, 96%[1] of employees and 100% of directors completed this requirement. In addition, teammates are required to complete annual core compliance training, and role-specific training. Training topics include, but are not limited to:

- Fair and Responsible Banking
- Fraud Awareness and Escalation
- Protecting Key's Assets
- Managing Risk at Key
- Anti-Money Laundering
- Culture, Conduct, and Ethics

In 2024, our teammates completed more than 534,000 hours of formal learning programs and courses, demonstrating our ongoing commitment to continuous improvement and ethical conduct.

Report a concern

Key employees and members of the KeyCorp Board of Directors are obligated to comply with the Code and to speak up when they suspect or witness a potential violation. 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. This helpline provides a safe and confidential way for teammates to report potential Code violations, with the option for callers to remain anonymous. We do not permit retaliation against individuals for reports of suspicious activity in good faith, nor will disciplinary action be taken for such reports.

Human rights

Key supports the fundamental principles of human rights set forth in the United Nations' Universal Declaration of Human Rights and the Guiding Principles on Business and Human Rights. Consistent with these principles and Key's purpose and values, we seek to build an intentional and dedicated workplace environment where all people are engaged, valued, supported, respected, affirmed, and encouraged to bring their best, authentic selves to work. Read Key's Human Rights Statement.

Key believes that responsible practices related to anti-bribery, anti-corruption, labor, human rights, and safety are essential to fostering a corporate culture of respect, accountability, and integrity. Key is committed to complying with all applicable laws and regulations.

[1] 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.

Business conduct

Key operates in a highly regulated environment and is obligated to comply with all applicable country, federal, state, and local laws, rules, and regulations. This includes all applicable securities laws, accounting standards, controls, and auditing practices.

Anti-bribery and anti-corruption

We remain steadfast in our adherence to all applicable anti-bribery and anti-corruption laws, such as the U.S. Bank Bribery Act, U.K. Bribery Act, and guidelines as provided by Key's Anti-Bribery & Corruption Policy. All Key employees, directors, service providers, and agents must act with transparency and integrity in all business dealings and follow all government requirements. 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 obtained. Any offers or receipts of value from clients or third-party service providers that exceed the allowable limits of the Code must be disclosed to the Ethics Office promptly.

Anti-Money Laundering

KeyCorp fully supports the U.S. government's efforts to combat terrorism and money laundering. We maintain a comprehensive program of financial crimes governance policies, procedures, and guidelines designed to comply with all applicable U.S. Anti-Money Laundering (AML) and countering the financing of terrorism (CFT) laws. These policies apply to our domestic and international operations and are designed to prevent illegal activity and protect our customers from fraud and other illicit finance activities.

Key's Financial Crimes Governance policy is reviewed and approved annually by the Joint Risk Committee of the KeyCorp and KeyBank National Association Boards of Directors.

As part of its AML program, Key maintains reasonable procedures to verify 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 when initiating a business relationship. We maintain record retention policies that comply with applicable laws and perform risk-based customer due diligence to identify potentially high-risk customers.

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

Read Key's Statement of Compliance with Anti-Money Laundering Laws.

Fair and responsible banking

At Key, fair and responsible banking (FARB) is a top priority, demonstrating our commitment to treating each client with integrity and respect. Our mission is to remove barriers to financial wellness and empower our clients to make informed decisions. FARB principles are embedded in all our business functions, policies, and practices, and apply to all employees and third parties.

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 identify, measure, monitor, control, and report FARB-related risks; provide a credible challenge to 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

Established in 2021, the FARB/CRA[2] Risk Committee oversees fair and responsible banking and Community Reinvestment Act (CRA) risk activities. It ensures compliance with regulatory requirements and KeyCorp's Risk Appetite. The Committee monitors risks, trends, and issues across business segments and products, operating under the KeyCorp Enterprise Risk Management Policy.

Responsible sales and lending

Our team members apply FARB principles to all client interactions, ensuring clients are fully informed about product risks and benefits. We make investments in products and services to support communities and clients at all stages of their financial journeys, including ways to save, pay down debt, buy a first home, and start businesses.

Listening to clients

Understanding our varied client base is crucial. We gather feedback through client surveys and a state-of-the-art experience platform. Social media is another key tool, with our Social Customer Care team monitoring and managing follow-up communication. We also use client feedback in the design and development of new products through our client panel called Voices.

Managing complaints

Client feedback helps us improve our services. Our customer service professionals, including the Social Customer Care team, are trained to address complaints effectively. We use multiple channels to monitor feedback and have clear escalation processes for serious concerns. Complaints alleging discrimination are escalated to Enterprise Client Relations (ECR) for thorough investigation, and then to the FARB Complaint Management team for review and investigation prior to resolution being provided by ECR.

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

To apply the FARB principles to client interactions effectively, Key employees receive mandatory training based on their roles. Topics include Fair Lending and UDAAP, AML, consumer advertising compliance, Key's Code of Business Conduct and Ethics, protecting Key's assets, fraud awareness and escalation, and managing risk. Employees are required to report any suspected regulatory violations to their managers or the ethics helpline. Such reports are kept in as confidential a manner as possible, and Key strictly prohibits retaliation against any employee for making a good-faith report.

[2] 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.

Data privacy and security

Safeguarding the personal and financial information of our clients and teammates, as well as other individuals with whom we come into contact, is one of our highest priorities. We are committed to maintaining robust data security and privacy controls, continuously monitoring the threat landscape, and aligning with industry standards to protect information, use it lawfully, and manage threats or incidents effectively.

Our information security and privacy programs are continuously maturing, driven by continual investments in technology and other solutions. We focus on strengthening endpoint protections, event monitoring, and analytics, as well as modernizing our Identity & Access Management processes and controls. Additionally, we are enhancing our fraud detection capabilities and improving the efficiency of case management and disputes resolution. As the demand for a digital-first client experience increases, we are evolving our client access and authentication methods to ensure security and convenience.

Data privacy policy and governance

Key's internal Privacy Policy governs the lawful processing of personally identifiable information (PII) across our entire organization, including affiliates, subsidiaries, and contracted service providers. The policy sets industry best practices as minimum requirements for processing PII, covering the entire data life cycle from collection to destruction. Our privacy practices adhere to applicable state and federal privacy laws and regulations for financial institutions.

Our dedicated Privacy team, led by the Chief Privacy Officer (CPO), is part of the broader Compliance team, which reports to the Compliance Risk Committee (CRC). The CRC, in turn, reports to the Enterprise Risk Management Committee. The CPO and Privacy team have the authority to escalate privacy risks to the Board. The Privacy, Cybersecurity, and other Risk teams work closely to implement appropriate controls and maintain compliance with applicable laws and regulations.

Key's online privacy statement explains how we maintain the privacy and security of PII. It details our practices for collecting, using, sharing, and safeguarding information, as well as the privacy rights afforded to individuals under applicable laws. Our privacy notice for consumers describes how we collect and protect PII, the types of information we share with others, and why. Key does not sell PII and only shares it with contracted third parties for specific, necessary purposes or as required by law.

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 approving the enterprise's technology strategic plan, including cybersecurity technology. The Risk Committee of the Board oversees the Information Security Policy and provides strategic direction for its development and execution. Any risk management issues are escalated to the Risk Committee for review and action.

> **Additional details** about our risk governance structure can be found in the Risk and oversight section.

Cybersecurity audits and assessments

We conduct regular internal and external penetration tests to ensure the robustness of our security environment. We maintain a comprehensive third-party security program to affirm our cybersecurity posture. Annually, we benchmark ourselves against industry-leading frameworks, such as 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 security programs.

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

Our Risk Review Group conducts independent internal audits to evaluate and improve the effectiveness of our risk management, control, and governance processes. Any identified gaps are rated, assigned a due date for remediation, and tracked to completion. The Risk Review Group verifies the remediation to ensure thoroughness.

Incident management

When an incident is identified, we follow established processes outlined in our enterprise privacy and cyber incident response plans. These plans provide a framework for the Enterprise Cyber Response team to effectively recover operations in the event of a cyberattack and manage incidents impacting bank information, including clients' and employees' data.

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

Our Privacy team assesses all incidents involving PII to ensure compliance with applicable laws and regulations, including notifying affected individuals and regulators when necessary.

To safeguard client data, we employ robust security measures for online accounts, leveraging advanced data protection, strong encryption, and continuous monitoring to protect our clients' accounts. Our online banking platform has strong sign-on requirements to safeguard sensitive information. We also regularly share security and fraud alerts with clients to help them protect their financial accounts.

Privacy and security education

Key remains committed to providing information security and privacy education to our employees, clients, and the communities we serve. We execute robust cybersecurity, privacy, and fraud education and awareness programs for our employees, including annual mandatory training and ongoing campaigns on topics such as reporting threats, phishing, fraud scams, and security best practices.

We provide clients with information and standard industry practices to keep individuals and businesses safe in a digital world. In 2024, we created more than 40 educational assets focusing on cybersecurity and privacy best practices, which were promoted through client emails, account alerts, social media posts, newsletters, webinars, and information on Key's website.

Corporate Political Activity

Corporate political activity principles statement

For the fifth consecutive year, KeyCorp has been recognized as a Trendsetter for our political policies and related disclosures by the CPA-Zicklin Index of Corporate Political Disclosure and Accountability.

At Key, we believe that active participation in public policy advocacy is essential to shaping the future of our industry and positively impacting the communities we serve. While corporations and national banks are legally limited or prohibited from making political contributions, we strive to play a constructive role in the political process. Our Government Relations department is dedicated to ensuring all political activities are conducted in full compliance with applicable laws and regulations. We follow approved policies and procedures, which are rigorously monitored by our Law Group and Compliance department. Additionally, our Chief Ethics Officer oversees the enforcement of conflict provisions within our Code of Business Conduct and Ethics.

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 surrounding political contributions. This includes Key's policies about 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 is managed by a team of in-house government relations professionals and contract lobbyists. We are committed to complying with all lobbying and disclosure laws. In 2024, our reportable federal lobbying expenditures totaled $1 million.

Trade association membership

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

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

Corporate political spending

It is important to note that 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.

As referenced on the previous page, 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 for final approval to the executive leader of Key's Corporate Center. Contributions for approved ballot issues are reviewed annually by the Nominating and Corporate Governance Committee of the KeyCorp Board of Directors and are disclosed semiannually on the Corporate Governance page of key.com.

Political action committees

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

> **Information** about contributions by the KeyCorp Advocates Fund and the KeyCorp Advocates Fund – Federal is publicly disclosed and accessible at fec.gov.

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

Voting Time-Off

We support our teammates' right to participate in the democratic process. We provide internal communications guidance, host regular training, review compliance protocols, and conduct internal audits to ensure all political and lobbying activities follow the law and the KeyCorp Code of Business Conduct and Ethics.

To assist teammates in casting their votes and making their voices heard, we offer Voting Time-Off for all primaries and general elections. This policy applies to all employees (except those on call or on commission only). Eligibility varies by state, but employees can take up to two to three hours of Voting Time-Off per year.