GOVERNANCE

Accountability, integrity, leadership, respect, and teamwork 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 corporate governance and ethical business practices. Our culture of continuous improvement and 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.

KEYCORP BOARD OF DIRECTORS

Key is committed to meeting high standards of corporate governance, ethical behavior, and business conduct. Our corporate governance practices are long-standing 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 director nominees for election at the 2022 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 long-term performance of our company. They are 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.

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

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. The team is 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.

46%
DIVERSE

31%
WOMEN

23%
RACIALLY
or ethnically diverse

A MESSAGE FROM THE BOARD OF DIRECTORS

We are pleased to share with you Key's continued environmental, social, and governance progress. We remain committed to doing business fairly and responsibly and to advancing environmental, social responsibility, and governance efforts and outcomes.

Key made significant progress on our ESG journey in 2021. Based on feedback from our stakeholders, we updated our ESG focus areas to include: diversity, equity, and inclusion; financial inclusion; climate stewardship; and data privacy and security. These updated areas of focus align with our long-standing and well recognized commitment to economic access and diversity, equity, and inclusion while remaining a national leader in both affordable housing and renewable energy financing.

In 2021, Key also significantly expanded our ESG disclosures to provide more decision-useful information. We expanded our ESG Report, issued our inaugural Taskforce for Climate Related Financial Disclosures report and Sustainability Accounting Standards Board index, and continued disclosure through the Global Reporting Initiative and CDP.

Our Board's Nominating and Corporate Governance Committee is responsible for overseeing ESG matters and is committed to our progress. The Committee focuses on our ESG practices and reporting with respect to environmental topics as well as resourcing, tracking, and progress of other responsible banking initiatives.

We recognize our role in ensuring that ESG risks and opportunities are integrated into long-term strategy; that the company is measuring and monitoring progress against commitments set as part of the strategy; and that ESG risks are well managed. For the second year in a row, ESG was a featured topic at our annual Board of Directors' education day. We have leveraged industry experts to share best practices and 'outside-in' views of our progress and opportunities, which have been formative to our priorities and path ahead. In early 2022, we are updating Board committee charters to include certain ESG matters, reflecting a more contemporary structure for governance.

In 2022, we are committed to continuing our progress, with specific focus on our ESG priorities. We will also continue to monitor ESG trends across the industry and evaluate how those trends apply to Key. We are proud of our enhanced climate and community commitments and recognize the significant work ahead to deliver the outcomes we aspire to achieve. We look forward to sharing our progress.

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

Christopher M. Gorman
Chairman and CEO
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
JetBlue Airways Corporation

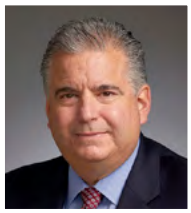
Carlton L. Highsmith
Chairman, President, and CEO (Retired)
Specialized Packaging Group, Inc.

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

Board responsibility for risk management

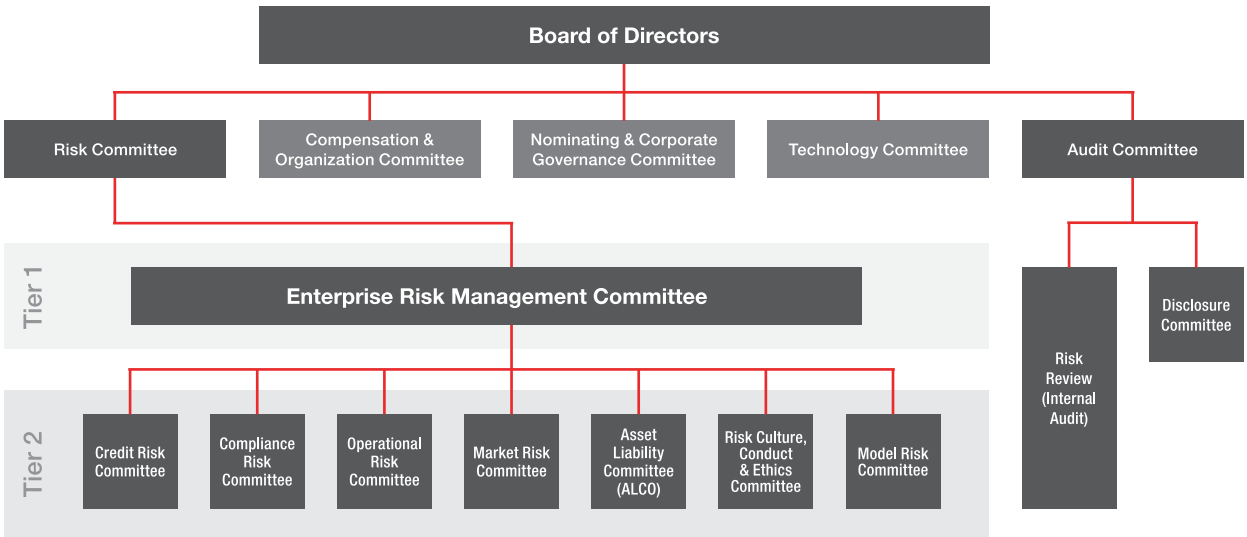
Like all financial services companies, we engage in business activities and assume the related risks. The most significant risks we face are credit, compliance, operational, liquidity, market, reputation, strategic, and model risks.

Our Board of Directors approves the Enterprise Risk Management (ERM) Policy and sets the overall level of risk KeyCorp 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 Risk Appetite Statement, which is included in our ERM Policy, describes the industries with which Key will not do business, including for socially responsible purposes. The policy also ensures effective oversight is in place for managing risks, enabling regular review and challenge. The Risk Committee of the Board oversees KeyCorp's risk management program and is responsible for strategies, policies, procedures, and practices relating to the assessment and management of the corporation's enterprise-wide risk, including risks related to capital adequacy, capital planning, and capital actions.

The ERM Committee is chaired by the CEO and is comprised of other executive officers including the Chief Risk Officer. This management committee meets regularly and is central to ensuring that the corporate risk profile is managed in a manner consistent with KeyCorp's risk appetite. The Committee supports the management of all risks by providing governance, direction, oversight, and high-level management of risk.

KeyCorp Risk Governance Committee structure

The table below depicts our risk management hierarchy and associated responsibilities and activities of each group.



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.

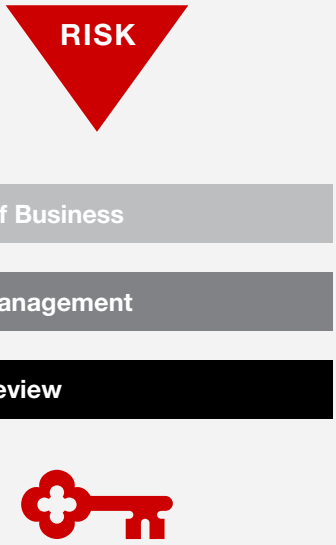
To further align with the moderate risk appetite, Key employs "three lines of defense" for risk governance.

- The lines of business are responsible for acting as the "first line of defense" with primary responsibility to accept, own, and proactively identify, monitor, and manage risk.
- Risk Management, which acts as independent centralized oversight, is the "second line of defense," aggregating, analyzing, and reporting risk information, and driving the establishment of risk policies reflective of Key's risk appetite.
- The "third line of defense" is Risk Review, which provides independent assessment and testing of the effectiveness, appropriateness, and adherence to risk management policies, practices, and controls.

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.

Three Lines of Defense Against Risk



BUSINESS CONDUCT AND ETHICS

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 6). 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.

Employee Promise

Our Employee Promise defines who we are as a company. It describes the partnership between Key teammates and how we create an environment where our teammates, our clients, and our communities thrive. We do this by providing smart solutions and great service to help our clients make confident financial decisions.

- We have a strong sense of community.
- We have the opportunity for personal growth.
- We do work that matters.
- We are accountable, and our results are rewarded.

Business conduct

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 quarterly risk and control testing. These results are reported to the Risk Culture, Conduct, and Ethics Committee as well as the Audit Committee of the Board.

The Code is our first resource for guidance when making decisions in the course of our duties. In addition, Key has other 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. Teammates and directors are required to successfully complete ethics training and certify their understanding of the Code. At the end of 2021, 97%[1] of employees and 100% of directors completed this requirement. Being ethical is part of living our Key values.

[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 inactive status due to leave.

Key's employees and Board of Directors are obligated to both comply with the 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 the Key ethics helpline, or complete an online form on Key's intranet or from their personal computer.

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.

Key's ethics helpline 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.

Business ethics

Non-retaliation

Key is committed to supporting and sustaining the integrity of our company. Employees are required 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. Confidentiality is a cornerstone to all investigations of employee misconduct. In the event misconduct is found to have occurred, employees may be subject to consequences ranging from performance improvement plans to termination.

Anti-competitive activities

We are obligated to comply with all applicable country, federal, state, and local laws, rules, and regulations. This includes all applicable competition and antitrust laws and regulations.

Anti-bribery and anti-corruption

Key's anti-bribery policy is codified in the Code, which prohibits employees, directors, service providers, and agents acting on Key's behalf from engaging in bribery or corruption of any kind. Anti-bribery and corruption training is provided through the annual Code training. 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 and the Foreign Corrupt Practices Act. Typically, bribes are offered or given to obtain an illegal benefit or advantage and often take the form of excessive gifts or entertainment. 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. The Ethics Office administers an internal monitoring system designed to detect corruption and conducts a comprehensive bribery and corruption risk assessment every 18 months.

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 KeyCorp Board of Directors and the Risk Committee of the KeyCorp 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.

KeyBank'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 and Political Exposure
- Policies and procedures covering relationships with senior foreign political figures, their family, and close associates (collectively, PEPs), and PEP screening of Key's 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 foreign financial institution customers

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.

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

DATA PRIVACY AND SECURITY

Data privacy and security at Key

Keeping the personal and financial information of our clients and employees, as well as other individuals with whom we come into contact, protected and secure is one of Key's highest priorities. Strong data safeguards and controls, in conjunction with continuous monitoring of the threat landscape, helps 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 any 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 initiatives include:

- Strengthening authentication methods to make it easier and safer for clients to open and access Key accounts, while making it more difficult for bad actors to gain access
- Strengthening fraud monitoring processes through system integrations, automation, and additional fraud alerting and reporting capabilities
- Ongoing extension of security controls into the public cloud as Key continues to expand its footprint
- Maturing security hygiene and resiliency processes to mitigate workforce risks, such as access control and governance, privileged access management, remote workforce, insider threat, and phishing

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 reports 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 on page 61.

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 audits and assessments are used to mature 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 plan, which is a supplement to our corporate incident response plans. It provides 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.

We have processes in place to assess the potential impact of incidents on individuals and adhere to applicable laws, including notifying impacted individuals.

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 alerts about security and fraud with clients.

Data privacy

Key uses and maintains data lawfully and abides by data privacy standards. Key's Privacy Policy governs the lawful processing of personally identifiable information across our entire organization, including our affiliates and subsidiaries. It encompasses the complete life cycle of data including collecting, obtaining, using, sharing, selling, accessing, protecting, handling, retaining, and destroying data.

All employees and third parties, including contractors, consultants, suppliers, and service providers, are expected to adhere to our Privacy Policy. Employees and contractors are required to complete an annual training course focused on protecting Key's assets, which addresses security, privacy, and a range of other topics.

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 Board's 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 on page 61.

The Privacy and Cybersecurity teams work closely together to implement appropriate controls around how personally identifiable information is managed and protected, and to keep Key in 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 clients, 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.

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

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 ensure teammates are aware of how to identify and report 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, pandemic-related scams, identity theft, and remote work 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 top of mind for Key. 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 2021, we held more than 30 education and awareness campaigns for clients that focused on topics such as cybersecurity and privacy best practices, identifying and reporting account takeover and fraud scams, keeping your business safe and secure from threats such as ransomware, business email compromise, and social engineering. Campaigns were promoted through emails, social media posts, alerts, and information on Key's website, newsletters, and webinars.

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. We hosted nine cybersecurity interns from various colleges and universities in 2021, providing them with the opportunity to work and learn about multiple aspects of cybersecurity in a hands-on environment.

POLITICAL INVOLVEMENT AND ACTIVITY

Corporate political activity principles statement

For the second 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 2021 totaled $830,000.

$830K

REPORTABLE FEDERAL lobbying expenditures for 2021

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.

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.

Corporate political spending

KeyCorp does not contribute corporate funds for election campaigns. This includes prohibiting supporting candidate committees, political parties or committees, or political committees organized for the advancement of political candidates, to 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 ESG Information - 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 political action committee (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.

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