Responsible Business

"At Comerica, we expect and encourage all of our colleagues to do what's right. Our Core Value — Trust. Act. Own. — cultivates an environment where people are invested with the power to fulfill their responsibilities, while keeping ourselves and each other accountable for our actions and commitments."

Jay Oberg

Senior Executive Vice President,
Chief Risk Officer

Responsible Business

Our business is based on the trust of our customers, communities and entire value chain, and we are committed to earning and maintaining that trust through ethical operations and doing business the right way — with honesty, integrity and transparency. This commitment to responsible business is embedded in our Core Values and culture and forms the foundation for the way we operate on a daily basis.

Beginning in 1849, Comerica has stood as a beacon of strength in the communities we serve, earning the trust and confidence of our colleagues, customers and stakeholders. Since then, we have worked to protect and enhance our brand and reputation as a leader in our industry, delivering a premium blend of service and value while ensuring transparency in our disclosures and reporting as well as our interactions with colleagues, customers, investors and other stakeholders. Increasingly, customers are interested in doing business with companies they admire and trust. By living our **Core Values**, we put ourselves in the best position to maintain our strong reputation as an admired and trusted organization in the financial services industry and the markets we serve.

Business Risk Management

With a consistent and conservative approach to banking, Comerica has always prioritized effective risk management and oversight. It is critical to our growth, success and organizational resilience, enabling us to respond to evolving business trends, market demands and an increasingly complex regulatory environment. It also allows us to proactively respond to external threats and events, including risks and opportunities arising from environmental, social and governance issues.

We continuously strive to improve and develop our risk management and oversight. While we assume various types of risk during the normal course of business, we work to understand, manage and carefully consider the risks we are willing to take and accept. In this way, we appropriately balance revenue targets with our corporate strategy, risk appetite, mission and Core Values.

Transparency is one of the most significant topics for our stakeholders and, as a result, one of our Impact Topics. As a leader in the financial services industry, we understand the importance of sound, verifiable data and visibility into our methods of disclosure. We provide robust financial, environmental and social reporting, using well-understood metrics to demonstrate our performance, progress and successes. We are committed to the implementation, control and maintenance of systems and procedures to obtain and verify information we disclose, including how we track and manage our sustainability impacts, risks and opportunities.

15th	14	10
consecutive corporate responsibility-related report	consecutive years responding to CDP's annual climate change questionnaire	consecutive years of third-party assured GHG data

In 2022, we made enhancements to our risk management tools and resources, including:

- Implementation of a new Compliance Management System (CMS), including detailed responsibilities, policies and procedures for the first and second lines of defense to drive full compliance with applicable laws and regulations
- Continued enhancement and implementation of a streamlined third-party risk program
- Development and implementation of an Enterprise Issue Management Governance program to drive consistency in how Comerica documents, manages and reports on all issues, no matter the identification source
- Development and implementation of an enhanced Complaints Management System to ensure broader and consistent capture of all complaints across all lines of business and third parties
- Automation of various control processes to improve efficiency and reduce error rates
- Improved cybersecurity and technology risk assessment processes and controls

Risk Management Oversight

Our governance structure is a multilayered approach that fully supports our enterprise risk management framework. This framework provides guiding principles and recommended practices to ensure a consistent, holistic approach to risk management. It is composed of a governance structure overseen by the Board of Directors, which approves Comerica's Risk Appetite Statement and outlines key risk management components, including the risk taxonomy, risk assessments, risk policies and our Three Lines of Defense.

BOARD RISK OVERSIGHT AND THE THREE LINES OF DEFENSE

Comerica Board of Directors		
Audit Committee	Enterprise Risk Committee	
Internal Risk Management Committees		
Three Lines of Defense		
First Line of Defense	All Comerica Colleagues	Responsible for identification and ownership of risks and implementation of appropriate controls to mitigate risks within the risk appetite
Second Line of Defense	Chief Risk Officer and Enterprise Risk Division	Provides independent risk oversight and guidance to the First Line of Defense to ensure that risks are appropriately mitigated within the risk appetite
Third Line of Defense	Internal Audit	Provides independent assurance that appropriate controls are in place and operating effectively in first and second lines of defense

First Line of Defense: Every individual at Comerica plays a role in managing risk to help achieve our strategic goals of the **Comerica Promise.** Our colleagues are our first line of defense and are responsible for the day-to-day management and ownership of risks.

Second Line of Defense: Each of the major risk categories are further monitored and measured by specialized risk managers in our Enterprise Risk Division. This second line of defense is led by the Chief Risk Officer and provides consistent processes and tools for how our business units identify, measure and manage existing and emerging risks, ensuring alignment of risk practices across the company.

Risk management committees, chaired by various members of Executive Management with risk subject matter expertise, serve as a point of review and escalation for risks that may have material impacts, risk interdependencies or risk levels that may be nearing the limits outlined in the Comerica Risk Appetite Statement. These committees are comprised of senior-level leaders who represent views from both the lines of business and Enterprise Risk.

Third Line of Defense: Internal Audit, the third line of defense, monitors and assesses the overall effectiveness of the risk management framework on an ongoing basis and provides an independent, objective assessment of the Corporation's ability to manage and control risk to management and the Audit Committee of the Board.

The Board's Enterprise Risk Committee meets quarterly and is chartered to assist the Board in promoting the best interests of the Corporation by overseeing policies and risk practices related to enterprise-wide risk and ensuring compliance with bank regulatory obligations and applicable laws.

The overall effectiveness of our risk management framework is regularly reviewed through internal and external audits, examinations by federal and state regulators, self-assessments and benchmarking. We conduct a myriad of risk assessment exercises across the organization, including regular stress testing and scenario assessment processes for identifying significant risks to our company. For more on risk identification and management, see our **2022 10-K.**

Supplier Risk Management

Our risk management framework extends to those who do business with us. We conduct initial and ongoing risk evaluations of our suppliers and perform due diligence reviews of potential suppliers based upon the scope of services to be provided and the potential risk to our organization. Click **here** to learn more about how we effectively manage supplier risk.

Key Enterprise Risks

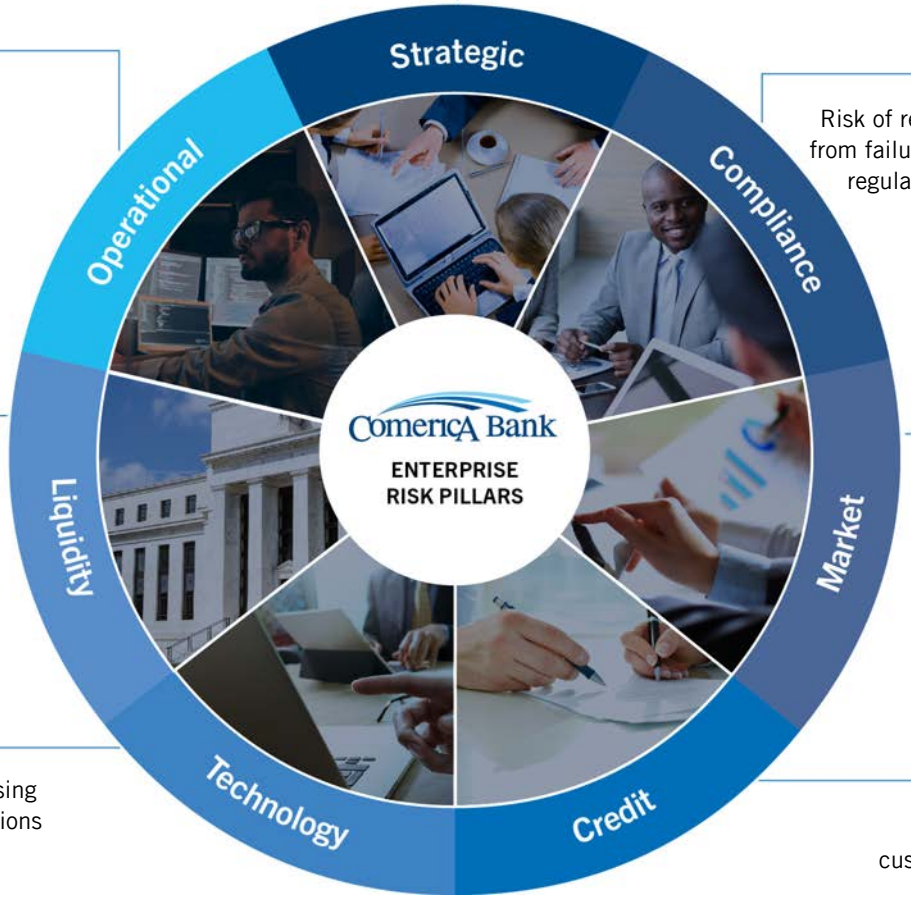
Risks we manage through our Enterprise Risk Management Framework include:

Strategic

Risk of inadequate income/returns or loss due to impairment of reputation, failure to develop and execute business plans, failure to assess business opportunities and failure to identify appropriate return for risk taken

Operational

Risk of loss due to the inadequacy of or failures related to internal processes, suppliers and people or from external events, excluding those driven by technology



Compliance

Risk of regulatory or legal sanctions or loss from failure to comply with applicable laws, regulations and other banking standards

Liquidity

Risk that Comerica does not have sufficient access to funds or the ability to raise or borrow funds to maintain normal operations

Market

Risk of financial loss due to adverse movements in interest rates, foreign exchange rates and commodity and equity prices

Technology

Risk of loss or adverse outcomes arising from the people, processes, applications and infrastructure that support the technology environment

Credit

Risk of loss due to the failure of a customer or counterparty to meet the terms of lending/funding-related contracts or from a lack of diversification

Enterprise Security

Comerica's Enterprise Security program is aligned with business imperatives, organizational risk and technologies to protect, monitor, detect and respond to the ever-changing financial services and threat landscape. We do this by focusing on effectively managing cybersecurity risks for the organization and our customers. We align resources into centers of excellence, maintaining standards and best practices in detection and response, dissemination of information and performance measurement. Our teams provide a comprehensive set of services within Comerica across data protection, cyber threat mitigation, risk management and fraud detection.

Our Enterprise Security program includes our Cybersecurity program, Corporate Physical Security program and Business Continuity program. It is administered by our Chief Information Security Officer and Chief Operating Officer, who work closely with the Enterprise Risk Committee to monitor, improve and enhance the program in response to changing risk environments.

Mission and Guiding Principles

Our Mission:

The Enterprise Security Program drives resilience and supports a culture of risk understanding, leveraging controls and technologies to protect Comerica's colleagues and assets to enable Comerica's business objectives.

Goals: **To Defend** **To Protect** **To Enable**

The guiding principles of the Cybersecurity Program are:

- **Focus on Solutions**
- **Seek to Educate & Learn**
- **Invest in People & Technology**
- **Take Ownership**
- **Cultivate a Shared Vision**
- **Support Business Objectives**

Oversight and Governance

Enterprise Security uses a combination of strong Board oversight and executive leadership. We take a cross-functional approach to ensure that we have an effective, evergreen Enterprise Security Program. The Board, primarily through the Enterprise Risk Committee, is kept apprised of the following the by CISO: overall status of the program, effectiveness of policies and procedures, material risk issues, risk management, control decisions and services providers.

ENTERPRISE SECURITY FUNCTIONS

Program Governance & Risk Management	Maintains effective risk and cybersecurity program management through identifying, monitoring, responding to and reporting risks and metrics, enabling the business by providing guidance and support to manage cyber risk.
Cyber Defense Operations	Provides capabilities to protect, monitor, detect, respond and recover from incidents, with efforts focused on effectively managing cyber risk.
Business Enablement & Security Assessments	Applies detailed security and technical information to drive cybersecurity and technology risk strategy. Includes cyber engineering and architecture, architecture and design, cyber risk management, and the business security and risk champions sub-functions.
Identity & Access Management (IAM)	Drives the strategy, policies and procedures to support capabilities for IAM governance, Identity Management, Privileged Access Management, Customer Identity and Access Management to meet business needs, reduce overall information security risk and improve the user experience.
Business Continuity	Manages organizational resources and skills sufficient for Comerica to provide ongoing financial support and services to customers during events that disrupt or impair the enterprise. Business Continuity is also responsible for coordinating the annual Business Continuity Program requirements.
Corporate Physical Security	Develops the enterprise physical security strategy, policies and standards that ensure the physical safety of all visitors, colleagues and customers at the bank's facilities as well as the security of property and assets.

Cybersecurity

Comerica's customers, colleagues, business partners and other stakeholders trust Comerica to protect their personal information and financial data, and we are committed to maintaining their trust. Our **Security Commitment** outlines how our online banking systems use various methods, tools and processes to help keep customer accounts and information secure.

The Cybersecurity Program Charter, through the approval of Comerica's Enterprise Risk Committee (ERC) of the Board, assigns the authority of the Cybersecurity Program to the Comerica Bank Incorporated Technology Risk Committee and the Chief Information Security Officer (CISO).

The Enterprise Information Protection Framework

The Enterprise Information Protection Framework, managed by our second line of defense, establishes the role of several other policies governing operational, technology and compliance risks along with behavioral expectations for protecting information at Comerica. These include but are not limited to, Comerica's Third-Party Risk Policy, Contract Administration Policy, Privacy Policy, HIPAA Policy and Corporate Physical Security Policies. Components of each of these policies are taken into consideration in the implementation of the Cybersecurity Program.

Enterprise Information Protection Framework

Cybersecurity Responsibilities

Board of Directors	Oversees and holds senior management accountable for implementing an effective Cybersecurity Program and managing cybersecurity risks within Comerica's relevant risk appetites
	Receives regular updates (typically on a quarterly basis) from Comerica's Chief Information Security Officer (CISO)
Enterprise Risk Committee of the Board	Assists the Board in discharging its oversight duties, and, along with the Board, periodically reviews and evaluates the performance of the program and its ability to appropriately manage risk
	Reviews management responses to security incidents, including those involving identity theft or personal health information, and makes recommendations for program changes
Technology Risk Committee	Provides executive management oversight and monitors the operational effectiveness of the program, along with ensuring corporate-wide implementation and oversight of the controls necessary to deliver the objectives of the Cybersecurity Program
Chief Information Security Officer	Leads the Cybersecurity Program and is accountable for implementing, managing and monitoring the effectiveness of the cybersecurity strategy
	Annually evaluates the strategy with first and second line of defense executive leadership and technology executive leadership
	Reports quarterly to the Enterprise Risk Committee of the Board

Policies and Standards

Enterprise Security has a Technology Risk Management Policy that establishes the principles and guidelines for effective identification, measurement and appropriate management of cybersecurity and technology risks. Our program is also aligned with industry standards such as National Institutes of Standards and Technology (NIST) and International Organization for Standardization (ISO) frameworks.

Monitoring and Mitigation

Enterprise Security evaluates the effectiveness of our framework and cybersecurity programs through adherence to the following best practices:

- Risk control self-assessments conducted by our business units, including regular stress-testing and scenario assessment processes for significant identified risks to Comerica
- Cybersecurity reviews by well-known industry professionals in addition to regular internal reviews
- Comprehensive evaluations carried out by external regulatory examiners
- Three Lines of Defense built on internal audits, oversight and effective challenge
- Maintenance of a continuous monitoring program
- Participation in several industry-wide initiatives to help keep us informed of new fraud trends and meaningful threat intelligence and to enable us to develop appropriate countermeasures

Training and Awareness

Comerica's colleagues are our first line of defense and are important to identification and awareness of security and risk issues. Comerica provides mandatory annual information security training, mobile device trainings and phishing intervention workshops. We review and update the courses each year to include relevant threats and topics. In 2022, nearly 100% of colleagues completed the training.

2022 Cybersecurity Highlights

- Matured our Security Awareness Program from strictly compliance-based to behavior change-focused
- Established new Identity Access Management capabilities
- Modernized our Security Operations Center
- Created a new Transformation Office and Process, Risk and Control Library and Metrics Program
- Enhanced email security and endpoint protections

Business Continuity

Effective business continuity and recovery management preparedness are crucial ways that Comerica proactively addresses potential risks to the business. From monitoring our systems for internal and external threats to monitoring Comerica locations for natural disaster or pandemic events, we strive to ensure the continuity of critical products and services provided to our customers as well as the safety and well-being of our customers and colleagues. We also recognize the impact of climate change and the potential for increased frequency and severity of storms and other natural disasters, further elevating the importance of our business continuity practices.

Our Business Continuity Management program enables Comerica management to oversee and implement resilience, continuity and response capabilities to safeguard colleagues, customers and our products and services in the event of a disruption to regular operations. Our overall objective is to support operations at an acceptable level and recover within an acceptable time frame. Therefore, we develop, maintain and regularly test our enterprise-wide continuity and disaster recovery plans that consider all critical elements of our business. We prioritize business objectives and operations that are essential for recovery and ensure that our disaster recovery planning prepares for the recovery or continuation of technology systems and assets, infrastructure and applications that are critical to our business functions.

2022 Business Continuity Highlights

- Completed an in-depth review of our Work Area Recovery requirements in conjunction with the rollout of our WorkBest hybrid work program
- Conducted tabletop business continuity exercises for active shooter, power outage and ransomware scenarios
- 100% completion of:
  - Business Continuity Plan Approvals
  - Incident Support Plan Approvals
  - Annual Training and Testing Requirements

COVID-19 Pandemic Lessons Learned

The COVID-19 pandemic demonstrated the capability of our business continuity programs and enabled both critical and routine business to continue without interruption.

From this event, lessons learned led to a completely revised Pandemic Plan, a restructured Business Continuity Event Management organization and the transition of more than 62% of the workforce to a work-from-home environment.

We reduced the allocation of Work Area Recovery physical space within select Comerica locations by approximately 70%.

BUSINESS CONTINUITY EXECUTIVE TEAM		
NATIONAL BUSINESS CONTINUITY PLANNING TEAM		
Incident Support Team California	Incident Support Team Michigan	Incident Support Team Texas, Florida, Arizona
Business Unit Recovery Teams	Business Unit Recovery Teams	Business Unit Recovery Teams

Corporate Physical Security

Our Corporate Physical Security program safeguards the integrity, confidentiality and availability of our organization's critical assets, information and resources. We are committed to providing a secure and resilient environment for our colleagues, clients and other stakeholders. Comerica is also committed to providing a safe and secure work environment in accordance with applicable employment, safety, health, anti-discrimination and other workplace laws. By maintaining a robust corporate security program, we aim to mitigate threats, prevent disruptions and foster trust in our operations, thereby enabling sustainable growth and ensuring the long-term success of our organization.

Key duties of our Corporate Security team include:

Risk Assessment and Management: Conducting regular assessments to identify potential security risks, evaluating their potential impact and implementing appropriate measures to mitigate these risks.

Physical Security Awareness and Training: Educating colleagues and stakeholders about security best practices, promoting a culture of security awareness and providing training programs to enhance their understanding of potential risks and the role they play in maintaining a secure environment.

Technical Security: Implementing measures to protect physical assets, including facilities, equipment and data centers. This involves managing access control systems, video surveillance, alarm systems and physical security incident response protocols.

2022 Corporate Physical Security Highlights

- Completed all security surveys and robbery awareness training at banking centers
- Kicked off new Executive Protection program
- Continued to unlock new features in our access control software that benefit the organization
- Completed installation of exterior cameras at our banking center locations
- Played a leading role in Return to Office

Privacy and Data Protection

Customer privacy and data protection are key topics critical to our business success. In addition to our robust cybersecurity program and Enterprise Information Framework that help protect against unauthorized access to customer data, we have a strong, compliance-led program designed to ensure we are meeting our customers' needs and complying with applicable state, federal and international laws and regulations. Our **Online Privacy Notice** outlines our online privacy practices and how customer information is collected. Comerica has a **Biometric Data Policy** that explains how information is collected, used and secured.

Our approach to managing customer privacy has proven effective, and adjustments that are in line with our overall risk management strategies are made as needed.

Mission and Guiding Principles

Comerica is committed to maintaining customer privacy. We are guided by our Core Values and a detailed list of information-sharing principles, highlights of which include:

- Limiting the amount of personally identifiable information collected
- Holding colleagues to strict standards of conduct to ensure confidentiality
- Maintaining accurate customer information and responding promptly to customer requests to correct information
- Not selling or sharing customer information with third parties for marketing purposes, except through a contractual joint marketing agreement
- Allowing customers to opt out of sharing their information with affiliates (for marketing purposes) and joint marketing partners
- Maintaining a process for properly reporting privacy incidents or suspected privacy incidents

Oversight and Governance

Overall privacy is overseen by Comerica's Compliance department. Corporate Compliance is the owner of Comerica's Privacy Policy, which includes principles for information-sharing practices across Comerica. As part of those principles, Corporate Compliance supports a process for properly reporting privacy incidents or suspected privacy incidents, including incidents involving protected health information. Data Privacy is overseen by Comerica's Chief Information Security Officer.

Policies and Standards

Changes to privacy laws and regulations are monitored by Corporate Compliance through the Change Management Procedure. Corporate Compliance monitors and provides updates related to laws and regulations that impact Comerica. Outside counsel and/or external advisors are engaged on an as-needed basis for guidance on changing laws and regulations.

Training and Awareness

All Comerica colleagues complete mandatory Information Lifecycle Management training, with 99.9% of colleagues completing the course in 2022. Additional training is provided to Technology and Cybersecurity colleagues around Corporate Information Protection.

Compliance and Ethics

As one of the leading financial institutions in the U.S., we are committed to earning the trust and confidence of our customers, colleagues and stakeholders. We demonstrate the highest standards of ethics and integrity in everything we do. This commitment is founded in our Core Values and embedded in our culture. We provide our colleagues, senior leaders and Board of Directors with the tools and knowledge to take ownership of this commitment and to act with integrity and in compliance with all ethical and legal responsibilities.

Codes of Ethics

We maintain **Codes of Ethics** to instill an ethical culture at Comerica, guide our treatment of customers, colleagues, business partners and the communities we serve; and help ensure compliance with applicable laws and regulations. Our principal Code of Ethics applies to all colleagues, and we have additional codes for senior financial officers and members of our Board of Directors to reflect their heightened responsibilities.

CODE NAME	DESCRIPTION	APPLIES TO:
Code of Business Conduct and Ethics for Employees	Provides guidance on issues such as ethical business practices, bribery, corruption, fair dealing, maintaining professional relationships, avoiding conflicts of interest and reporting illegal or unethical behavior	All colleagues
Senior Financial Officer Code of Ethics	Outlines additional requirements and highlights the importance of honesty, integrity and sound judgment of our senior financial officers	Chairman, President and CEO/ Senior Financial Officers
Code of Business Conduct and Ethics for Members of the Board of Directors	Provides guidance on recognizing and handling ethical issues, sets expectations regarding a variety of situations and provides information on how to manage unethical conduct to assist in fostering a culture of openness and accountability	Board of Directors

Oversight and Governance

We have a robust governance program, overseen by our Board of Directors and senior leadership, to help support a culture of compliance at all levels of the organization and to operationalize compliance throughout the business.

COMPLIANCE RESPONSIBILITIES	
Enterprise Risk Committee of the Board of Directors	Maintains accountability for Comerica's compliance with applicable legal and regulatory requirements
	Reviews and approves Comerica's Compliance Management System (CMS) program and Compliance Risk Management Policy
Chairman and CEO	Holds all colleagues accountable for appropriately assessing and effectively managing compliance risks associated with their activities
Enterprise Wide Compliance Committee	Composed of senior and executive business unit managers as well as managers responsible for compliance, audit and overall risk
	Oversees and reviews CMS program and Compliance Risk Management Policy at least annually
Chief Risk Officer and Compliance Leadership	Set the overall vision and approach for management of compliance risk within Comerica
	Develop, implement and maintain an effective CMS program
Corporate Compliance	Maintains Comerica's CMS program and Compliance Risk Management Policy
	Maintains and deploy appropriate systems, tools and awareness in support of the CMS program
	Directs training efforts in support of the CMS program
	Provides guidance to first line of defense (FLOD)
Risk Liaisons	Coordinate with the Business Units, Corporate Compliance and other stakeholders
Business Units	Own the risks created by FLOD activities
	Hold FLOD colleagues accountable for appropriately assessing and effectively managing compliance risks associated with their activities

Compliance Management System

Comerica's CMS program is designed to effectively identify, measure, monitor and control compliance risk and maintain compliance with applicable laws, rules and regulations as well as applicable governance documents.

In 2022, we launched a Committed to Compliance program to enhance our CMS. Among other goals, this program will strengthen colleagues' compliance skills and knowledge to align with industry best practices.

Supplier Conduct

We also require that all suppliers (and/or third parties acting as agents of Comerica) conduct themselves with the same high standards of honesty, fairness and integrity. Suppliers must abide by all applicable federal, state and local laws, rules and regulations while ensuring that all services are conducted with a high degree of professionalism and in accordance with the terms and conditions of the relationship. Additional information on supplier requirements can be found on **Comerica.com**.

Communication and Training

We use a variety of communication channels, including mandatory annual online training and our intranet site, to emphasize personal accountability in complying with our Code of Business Conduct and Ethics for Employees provisions and to remind colleagues of the importance of reporting inappropriate and/or illegal conduct. Our contingent workers also complete training, which includes information on the Code of Business Conduct and Ethics for Employees. In 2022, 99.9% of active colleagues completed the annual mandatory Code of Business Conduct and Ethics training.

Comerica colleagues complete additional annual mandatory training courses on topics that include regulatory issues, privacy and information protection, anti-money laundering, diversity, equity and inclusion, workplace harassment, workplace safety and fair lending/anti-discrimination as well as a one-time sustainability training course for new hires.

The Corporate Learning department tracks training completion and provides access to reporting to Corporate Compliance to escalate with senior management, as appropriate, if training is not completed. For additional compliance training metrics, review our **Responsible Business Key Metrics Table.**

Reporting and No Retaliation Policy

At Comerica, we foster a culture where colleagues are encouraged to speak up and raise questions and concerns without fear of retaliation, as outlined in our non-retaliation statement included in our Code of Business Conduct and Ethics for Employees. We provide several channels for reporting violations of laws, rules and regulations that apply to our business, in addition to violations of our Code of Business Conduct and Ethics for Employees and other Comerica policies. Comerica maintains two hotlines for colleagues that provide a confidential reporting process through a third-party vendor. Calls to these hotlines can be made anonymously. In 2022, 52 concerns were recorded via the hotline, with 12 from Q4 2022 pending resolution at 2022 year end.

Anti-Money Laundering Compliance

The Comerica Anti-Money Laundering (AML) Compliance program covers Comerica Bank and all of its subsidiaries. We strictly comply with all Bank Secrecy Act (BSA) and USA PATRIOT Act requirements. In accordance with these requirements, the following people, policies and procedures are part of our AML Compliance program:

- A designated BSA/AML Compliance Officer
- Policies, procedures and controls designed to guard against money laundering
- Ongoing compliance training
- Independent auditing of the program

Our AML Compliance program deploys systems to monitor customer and business unit risks and implements additional controls and/or quality assurance reviews when specific risks are identified. Our policies are periodically reviewed, updated and approved by our Board of Directors and are independently tested annually by Internal Audit and outside regulatory agencies. We use the results to assess the effectiveness of and help enhance our compliance program.

Our robust Customer Identification program is a core element of our AML program and fulfills our obligations by collecting and verifying identifying information to ensure that we know who holds Comerica accounts. This information is compared to government lists of sanctioned parties and others with whom we are prohibited from doing business and helps prevent financial transactions when necessary.

For additional information, visit the **AML Compliance** section on our website.

AML Training

Colleagues, when applicable, are required to complete additional annual regulatory and AML Compliance training. In 2022, nearly 100% of relevant colleagues completed the AML training.

Human Rights

Through our Corporate Responsibility Council, we recently adopted a **Human Rights Statement** that outlines our commitments to protect and advance human rights throughout our business and across our supply chain. This statement complements our codes of ethics and policies on equal opportunity and affirmative action, workplace harassment and discrimination and fair lending. Highlights include:

- We support and respect the protection and preservation of human rights as directed by the principles in the United Nations Guiding Principles.
- We strive to create an environment of respect for all individuals. We do not tolerate corruption, discrimination, harassment, child labor, prison labor, forced labor or slavery in any form.
- We live our Core Values by supporting the protection of the rights of individuals who have been historically disadvantaged in the workplace and in society, including the rights of women, individuals from underrepresented ethnic/racial backgrounds, people with disabilities and LGBTQ+ individuals.

As Comerica primarily does business in the United States, we have no direct presence or investment in countries where lack of human rights protection is a known significant problem.

Fair and Responsible Banking

In 2022, Comerica established the new Office of Fair and Responsible Banking, consolidating its first line of defense fair lending and Community Reinvestment Act (CRA) compliance functions. The office's responsibilities include:

- Ensuring that all customers, prospective customers and communities are treated fairly and equitably regardless of race, sex or sexual orientation, color, national origin, religion, age, marital status, disability, familial status and other protected classes
- Ensuring that Comerica is meeting the credit needs of the communities where we do business, including low- to moderate-income (LMI) neighborhoods, and is not allowing discriminatory credit practices
- Understanding and identifying fair lending and responsible banking risks across the enterprise to help business leaders effectively mitigate and monitor those risks within their departments

The Executive Vice President, Corporate Responsibility oversees this office. The Fair and Responsible Banking Committee began meeting in the fourth quarter of 2022 and includes the Director of Corporate Compliance, the Manager of Fair Lending and Home Mortgage Disclosure (HMDA) and other compliance, risk, audit and legal representatives.

The office oversees the following six topics:

- Regulation B – Equal Credit Opportunity Act (ECOA)
- Regulation C – Home Mortgage Disclosure Act (HMDA)
- Regulation BB – Community Reinvestment Act (CRA)
- Fair Housing Act
- Limited English Proficiency
- Unfair Deceptive or Abusive Acts and Practices

In addition, the office ensures adherence to fair servicing related to Regulation V – Fair Credit Reporting, Fair Credit Reporting ACT, Fair Debt Collection Practices and Regulation X – Real Estate Settlement Procedures Act.

Community Reinvestment Act (CRA)

Comerica's CRA team oversees Comerica's CRA compliance across all lines of business, ensuring that Comerica is meeting the credit needs of the communities where we do business, including LMI neighborhoods, and maintains an ongoing monitoring program to provide lines of business with timely information about Comerica's CRA services, lending, products and investments. To support Comerica CRA activities, we have a dedicated team of 12 External Affairs market and community impact managers who work with community partners to identify and support the needs of the markets where we operate.

CRA-related guidance and recommendations are made based on feedback received from our Community Development Advisory Councils (CDACs), other trusted community partners, data analysis, peer analysis, research related to current market conditions and the results of our CRA examinations. Refer to the **Community Reinvestment page on Comerica.com** or Comerica's **2021 Corporate Responsibility Report** for details on factors that supported our most recent CRA rating.

To share CRA best practices, benchmark our performance and achieve the greatest possible impact, Comerica participates in peer bank meetings across our markets. We require new External Affairs staff to take our in-house CRA training, and our External Affairs team provides CRA-related training to other relevant colleagues. In 2022, our External Affairs team hosted a CRA Event Series for all colleagues on the importance of CRA to Comerica and our communities.

Support for Our Communities in 2022

300+

senior officers and executives have a three-hour CRA Service Initiative training goal as part of their Annual Diversity Scorecard

1,000+

Comerica Financial Education Brigade members supported training in primarily LMI communities

8,900+

CRA-qualified service hours by CRA-trained Comerica volunteers to more than 300 organizations across all markets

Fair Lending and HMDA

This department is responsible for the compliance guidance and oversight of Comerica's fair lending and HMDA programs. The team holds first line of defense colleagues accountable for appropriately assessing and effectively managing fair lending and redlining risks associated with their activities, with effective challenge from Corporate Compliance. The team monitors lending practices, investments and potential service gaps.

Data and Regulatory Reporting

The Data and Regulatory Reporting department supports the HMDA, Fair Lending and CRA teams with data for monitoring and testing objectives. It also manages the annual regulatory data submission for all fair lending regulations, supports related regulatory examinations, consults with lines of business on data collection and reporting requirements and develops analytical reports for strategic decision-making.

Public Policy and Government Relations

Legislation passed at the state and federal levels can have a big impact on Comerica's products and services. Our Government Relations Group works closely with our lines of business to monitor the development of public policies that directly affect our company and industry.

Our advocacy efforts focused on the federal level and in our key market states. Comerica primarily engages with national and state financial services trade associations to inform them of our policy views so that they can advocate on behalf of the regional banking industry.

Another way Comerica participates in the political process is through contributions from its political action committee (PAC). The PAC annually solicits contributions from eligible colleagues and makes bipartisan contributions — all in compliance with local, state and federal election laws — to political candidates and committees who understand and support Comerica's pro-banking, pro-business philosophy. After suspending contributions from the PAC in early 2021, we resumed contributions later in the year after putting additional criteria in place to ensure that the candidates we support are also committed to working in a civil and constructive manner. Comerica does not use corporate funds to make direct political contributions to candidates for public office or groups organized to influence political campaigns, in accordance with Section 527 of the Internal Revenue Code.

$344,000

Comerica PAC contributions to political candidates and committees (November 1, 2021 to October 31, 2022)

Comerica is also an active member of several financial services trade associations across the country. Membership benefits include business opportunities for the company and effective grassroots advocacy on behalf of the industry. We monitor these organizations closely for any changes in policy positions to ensure transparency and alignment with Comerica Core Values. A portion of Comerica's trade associations' dues is used for lobbying and/or political activities and is non-deductible under Section 162(e)(1) of the Internal Revenue Code.

RESPONSIBLE BUSINESS	2020	2021	2022
Privacy & Protection			
Number of substantiated complaints received concerning breaches of customer privacy - complaints received from outside parties and substantiated by the organization	1	6	44
Total number of identified leaks, thefts or losses of customer data	52	63	83
Anti-Corruption, Ethics and Countering Bribery			
Number of internal incidents of alleged corrupt behavior investigated	277	242	225
Number of cases in which allegations were substantiated and/or colleague admitted involvement	86	75	70
Number of legal rulings against Comerica or its colleagues for corruption	0	0	0
Colleague Annual Compliance Training (percent relevant colleagues who completed the required course)			
Anti-Money Laundering	99.9	99.8	99.9
Comerica Code of Business Conduct and Ethics for Employees	99.9	99.9	99.9
Fair Lending Anti-Discrimination	99.8	99.9	99.8
Information Privacy and Protection	99.9	100.0	99.9
Community Reinvestment Act	99.8	99.9	99.9
Financial Exploitation of the Elderly or Dependent Adults	99.9	100.0	99.9
Workplace Harassment	99.9	100.0	99.9
Information Lifecycle Management	99.9	99.9	99.9
Diversity	100.0	100.0	99.9
Sustainability	100.0	100.0	100.0
Public Policy & Government Relations			
Comerica PAC contributions to political candidates and committees (thousands $)[44]	376	58	344

[44] Comerica PAC contributions (Nov. 1 previous year–Oct. 31 reporting year)