Cybersecurity & business continuity disclosure

Cybersecurity & business continuity programs

The ongoing evaluation of The Bancorp's internal and external operating environment is a vital component that contributes to the success of the bank and the security of our clients and partners. Our Information Security team and Business Continuity specialists continuously work to identify potential threats and assess risks which may have an impact on our business operations.

Cybersecurity program

We recognize that the secure transmission of confidential information over public networks and other mediums is a vital element of our business model but presents associated risks. Accordingly, our processes to identify, assess, and monitor material risks from cybersecurity threats are part of our overall enterprise risk management program and integrated into our operating procedures, internal controls, and information systems. We utilize secure, multi-tiered architecture, using processes and controls from a wide variety of security industry leaders, through which we provide financial products and services.

We maintain an effective and comprehensive Cybersecurity Program under the direction of a dedicated Chief Information Security Officer (CISO). Our established Cybersecurity Program is mapped to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), Payment Card Industry Data Security Standards (PCI DSS), the Center for Internet Security® (CIS) Critical Security Controls, and the relevant International Organization for Standardization (ISO) standards to maintain the confidentiality, integrity, and availability of our information systems, networks, and corporate and customer data.

Highlights of the Cybersecurity Program include:

- Annual PCI certification for applicable in-scope environments
- Employment of highly experienced cybersecurity professionals who continuously evaluate, monitor, and test potential threats to our systems and critical applications and compliance with our Cybersecurity Program.
- Risk Assessments and compliance audits against the above-referenced standards to benchmark and evaluate program maturity with industry leaders.
- 24/7 end-to-end Security Operations Center ("SOC") to monitor, detect, alert and respond to any unusual, suspicious or malicious activities.
- Incident response program and internal forensics capabilities with third party forensic experts on retainer.
- Internal and external audits to ensure compliance with standards and applicable legal requirements.
- Third party oversight to evaluate and monitor the cybersecurity practices of new and existing third party service providers and partners using a risk-based approach.
- Monitor and report on systems and critical applications.
- Conduct regular vulnerability assessments with detailed vulnerability management.

- Regularly review and maintain The Bancorp's standards to securely configure and administer firewalls, routers, databases, antivirus systems, wireless networks, remote access, and security logging and monitoring systems.
- Train employees on our Cybersecurity Policy and enforce policy.

The Board of Directors oversees cybersecurity and information security risk and carries out this oversight through its Risk Committee. The Risk Committee meets at least quarterly and receives updates from management, including the Chief Information Security Officer regarding cybersecurity, information security, and related risk matters.

Privacy

The protection of customers' and employees' personal and financial information is a vital component of our business operations. We safeguard personal information through a wide range of technological, administrative, organizational, and physical security measures. We also impose contractual, policy, and risk-based management requirements, as applicable, on third parties that access or process personal information on our behalf. In addition, our Code of Ethics and Business Conduct, Record Retention Policy (and associated retention schedules), and other policies and procedures establish how employees should handle and safeguard confidential business information. We have an incident management process in place to respond to any suspected or actual incident involving unauthorized access to, or disclosure of, personal information, its availability or an impact on its integrity. This process requires escalation to a dedicated response team for mitigation, severity assessment, root cause analysis and corrective actions. We also have policies and procedures in place in order to notify impacted individuals of privacy breach incidents in accordance with applicable state or federal law, should such a breach occur.

The Bancorp has not experienced any material data breaches involving personally identifiable information during the reporting period.

Business continuity program

The Bancorp has implemented and continues to maintain a robust Business Continuity Program that aligns with our risk analysis and federal regulatory expectations. Ensuring the continuity of business operations is fundamental to the success of the bank and our business model. Our collaboration with a wide range of business partners and service providers necessitates the need for strong business continuity controls principally focused on mission-critical systems. In response to an evolving risk landscape, including cybersecurity threats, climate-related events, and global disruptions such as pandemics, The Bancorp maintains a dynamic and adaptive Business Continuity Program designed to address both physical and non-physical risks to operations.

Consistent with guidance issued by the FFIEC, our Business Continuity Program:

- **Identifies** critical business processes and their internal and external dependencies, including reliance on third party service providers and infrastructure located in geographically diverse regions

- **Performs business impact** assessments annually, incorporating loss scenarios such as but not limited to climate-related physical risks such as severe weather events, flooding, and other environmental hazards
- **Incorporates** scenario analysis and resilience planning, where applicable, to assess the potential impact of high-severity, low-frequency events on operations
- **Defines** and documents steps that can be taken to mitigate the impact if a disaster strikes
- **Validates**, as applicable, recovery capabilities for key services, systems, and certain third parties against established recovery objectives.

End of document