



## **BOARD OVERSIGHT OF INFORMATION SECURITY, INCLUDING CYBER SECURITY AND DATA PRIVACY:**

Protecting and respecting the privacy of our clients' and customers' personal information and maintaining the security of our systems and networks are priorities at Bread Financial. Our Board of Directors is committed to ensuring that the Company continues to maintain effective privacy and security controls and protections in order to maintain the trust of our clients and customers in an evolving environment. The Risk Committee has primary responsibility for overseeing the Company's risk management program relating to data privacy and cybersecurity. To this end, the Board and Risk Committee receive at least quarterly updates on both data privacy and cybersecurity matters. These reports focus on, among other things, the evolving threat environment, vulnerability assessments, specific cyber incidents and management's efforts to stay current and comply with applicable privacy regulations and monitor, detect and prevent cyber threats to the Company.

### **Data Privacy**

Based upon the NIST Privacy Framework, our privacy program drives our commitment to the responsible collection, use and sharing of personal information, and we balance our product development activities with a commitment to transparency, fairness and non-discrimination. We designed our multi-layered information security and data privacy programs and practices to ensure the security and responsible use of the information and data our stakeholders entrust to us. Our associates receive privacy awareness training on a regular cadence addressing relevant topics from best practices to more role-based topics. Our programs leverage third-party assessments and advice regarding best practices from consultants, peer companies and advisors. We closely monitor and track proposed privacy legislative and regulatory changes as well as industry-related trends and adjust the program accordingly as the privacy landscape evolves.

### **Information Security, including Cybersecurity**

Based upon the NIST Cybersecurity Framework, our information security program deploys a defense-in-depth strategy to ensure that security is an integral and integrated part of our technology investment. We leverage multiple industry solutions to provide data protections with automated controls and ongoing penetration testing of both the internal and external environment. We partner across the lines of defense and with outside parties to continually evaluate our program effectiveness due to the ever-changing threat landscape and to assure alignment with regulatory guidance. An essential component of our program is using current trends to train our associates on a continuous basis. We conduct tabletop exercises with various subject matter experts across the Company on a regular cadence to walk through cybersecurity incidents and continue to improve our internal processes. Additionally, we provide in-depth associate training, consisting of targeted role-based training, general awareness training and continuous phishing simulation and awareness testing based on real-life scenarios. We maintain an active network of collaboration with law enforcement, industry groups, Information Sharing and Analysis Centers, and peers in the areas of threat intelligence, response and detection, and program best practices. We continuously assess the risks and threats through our cyber defense team around the clock and dynamically adjust our program and investments as required.