TheBancorp™

Disclosure

Consumer protection practices disclosure

Consumer protection practices

The Bancorp is committed to providing quality financial services to consumers in a fair and responsible manner. By doing so, we can build lasting relationships and help consumers meet their financial goals.

Ethical business practices

Consistent with our Corporate Values, we strive to deliver products and services with the highest standard of financial and ethical responsibility and accountability. The Bancorp Code of Ethics and Business Conduct sets the standard for these practices and requires, among other things, honest and ethical conduct and compliance with:

- The letter and spirit of applicable laws, including consumer protection laws
- Rules and regulations that prohibit unethical, discriminatory, or predatory practices
- Laws prohibiting Unfair, Deceptive or Abusive Acts or Practices (UDAAP)

All employees have a responsibility to comply with the Code of Ethics and Business Conduct and are required to read and acknowledge the Code annually. Employees must also complete UDAAP compliance training on an annual basis.

Consumer compliance

Our Compliance Department plays a key role in the Company's commitment to providing products and services fairly and responsibly. The Bancorp has implemented a *Compliance Risk Management Program* ultimately intended to facilitate consumer protection. Experienced compliance personnel are consulted during the development and marketing of products and services to ensure that principles of consumer protection are top-of-mind. During a product's life cycle, the Bank applies a layered testing protocol designed to assess compliance with applicable consumer protection laws and to confirm that our offerings are delivered to customers consistent with applicable requirements and product design. This includes, as applicable, compliance with the following consumer protection laws and their implementation regulations:

- UDAAP
- Truth in Lending Act
- Truth in Savings Act
- Fair Credit Reporting Act
- Electronic Fund Transfer Act
- Other applicable consumer protection laws

Compliance personnel work with the Bank's lines of business as well as our clients and business partners to develop and communicate products and services to consumers in a clear, honest and compliant manner.

Product and service reviews

New products and services as well as product and service expansions and modifications are also carefully reviewed by our New Products, Services or Approval for Change (NPSAC) Committee or Program Approval Committee (PAC). Comprised of our business-line leadership, as well as representatives from the Bank's Compliance, Legal, Risk, Marketing, Financial Crimes Risk

Management and other corporate functions, the NPSAC and PAC Committees provide a centralized forum for presenting and evaluating new or modified product and service offerings. This process includes documenting and discussing material risks associated with such offerings and implementing controls designed to manage or mitigate such risks. The chairperson of NPSAC is the Director of Enterprise Risk Management. The Director of the Program Approval Committee is the Managing Director, Chief Commercial Officer of Fintech Business Development. Any escalations arising from NPSAC or PAC Committees are escalated to the Board directed Risk Committee or the Board of Directors.

Complaint management

As we deliver products and services, listening and responding to customer complaints is a top priority. We collect customer feedback through a range of channels, including:

- Our website
- Applications
- Telephone
- Social media
- Regulatory agencies
- Reporting from our clients and program partners

We take this feedback seriously and consider it as we work to improve our approach and offerings. To aid this effort, we have a robust complaint management process as required by our Complaint Policy which is led by our Complaint Leadership team under our Chief Compliance Officer. This includes policies and procedures designed to ensure timely and effective resolution of complaints, regular reporting to management, and trending and root cause analyses to determine potential solutions.

Information security

Protection of customers' 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 and we require that applicable third parties, such as our suppliers and vendors, protect this information as well. In addition, our Code of Ethics and Business Conduct and other policies include specific guidelines about how employees should safeguard customers' information.

We have an incident management process in place to respond to any suspected or actual incident involving unauthorized access to, disclosure of, or other compromise of personal information, including impacts to the availability or integrity of such information. This process requires escalation to a dedicated response team for mitigation, severity assessment, root cause analysis and corrective actions. We notify impacted individuals of privacy breach incidents in accordance with applicable state or federal law. See our disclosure on Cybersecurity & Business Continuity Programs for more on our approach to cybersecurity.

End of document