Security and privacy programs

Summary of information security and privacy programs

Executive Summary

MUFG Union Bank, N.A. considers your information to be a critical and valued asset that you entrust to the bank and its subsidiaries (collectively, the “Bank”). We are committed to safeguarding the information entrusted to us and we actively maintain enterprise-wide programs in good faith compliance with applicable laws and regulations.

Our programs are designed to:

- Provide appropriate governance and clear guidance to our employees about the protection of customer information;
- Monitor our systems for threats to customer information;
- Provide security solutions that minimize the threat to customer information;
- Train and raise awareness among our employees to understand their responsibilities with respect to the protection of customer information and the security of our systems;
- Require that third-party service providers adhere to applicable security policies, standards, and regulatory obligations;
- Address all customer notification and other requirements regarding information protection, including raising awareness about information security and privacy among consumers.

Enterprise Information Security

Our Enterprise Information Security Program is reviewed and approved by our most senior cybersecurity officers. The Bank’s Enterprise Information Security Program is also regularly reviewed by federal regulators. In addition, the Bank’s internal auditors perform audits and evaluations of the Bank’s internal control environment, and we perform ongoing application and network threat modeling and penetration testing.

The Objectives of our Enterprise Information Security Program are designed to:

- Comply in good faith with Gramm-Leach-Bliley Act (GLBA) and other applicable laws, regulatory guidance and financial institution standards to protect the confidentiality, integrity and availability of non-public personal information;
- Oversee the necessary control framework to mitigate information security risks and detect emerging threats;
- Maintain an appropriate governance model for executive and Board oversight; and
- Sponsor and execute relevant activities and projects across the enterprise to strengthen the Enterprise Information Security Program.

Enterprise Information Security Program’s Areas of Focus[1]:
The program’s areas of focus help identify and prioritize the Bank’s actions for reducing information security risk, and is a tool for aligning policy, business, and technological approaches to managing risk.

There are five functions that organize the Bank’s information security activities at their highest level. These are:

- **Identify:** Recognize risks to systems, assets, data, and capabilities in order to prioritize the Bank’s information security efforts.
- **Protect:** Use the appropriate safeguards to protect customers’ privacy and information.
- **Detect:** Identify and detect cybersecurity anomalies and events through continuous monitoring and detection processes.
- **Respond:** Once a cybersecurity event is detected, respond to contain the impact.
- **Recover:** Reduce the impact of a cybersecurity event through resilience and timely recovery to normal operations.

(continued)

Incident Response Program:

We have a formal Incident Response Program that encompasses reporting, response, and notification procedures. The program also includes our Data Breach Response Program that outlines the process used in the event of a breach of electronic or physical security or the loss or exposure of data that has the potential to result in unauthorized access to sensitive, confidential, or classified information.

The Incident Response Program is structured to provide timely and efficient assessment and response to all reported incidents, in compliance with state and federal laws and regulations.

Third-Party Service Provider Management:

Our Third Party Risk Management Program is governed by the Third Party Risk Management Group which establishes the policy and framework to identify, monitor, manage, and report risks associated with third-party service provider relationships across the enterprise and in accordance with applicable laws, regulations, and regulatory guidance.

Security Awareness, Employee Training and Compliance:

Our Security Awareness Program informs and engages employees through multiple communication vehicles and channels, including face-to-face interaction, digital communications through the Bank's internal network, computer-based training, and email distribution of newsletters and alerts. Our Security Awareness Program also encompasses messaging via external communications channels, such as email, social media, branch monitors, ATM screens, and newsletters that inform our customers and clients about information security.

All Bank employees are responsible for appropriately handling and maintaining the confidentiality of customer information. Additionally, all employees are responsible for adhering to the Bank's Business Standards for Ethical Conduct Policy, as well as to all policies and procedures pertaining to the access, use, and protection of customer information. All employees are required to take Privacy, Incident Notification, and Information Security trainings and to recertify these trainings periodically.

The Bank's Privacy Program

Privacy Notice:

The Bank's policy is to comply in good faith with applicable privacy laws and regulations. The Bank is required to provide a copy of its GLBA Privacy Notice to all customers and clients and to anyone who requests it. In addition, the California Privacy Notice (Important Privacy Choices) is provided to California customers. The Bank's privacy notices and online privacy practices may be viewed on the Bank's Privacy and Security Center at https://www.unionbank.com/privacy.

Health Insurance Portability Accountability Act (HIPAA):

We established a formal Corporate HIPAA Privacy Program. This program provides governance including: policy, scope, key requirements, roles, and responsibilities, exceptions to policy, oversight, and related policies and procedures. Our Data Breach Response program also supports HIPAA requirements for the Bank to be able to effectively, if they arise, coordinate and respond to incidents that involve an unauthorized disclosure of protected health information (PHI).

Along with these measures, the Bank continues to develop risk and measurement tools to mitigate and safeguard protected healthcare information (PHI) through the use of ongoing risk assessments, monitoring, key indicators, and control testing. In addition, training is delivered to employees to ensure the privacy and information security of customer data, including PHI.

European Union (EU)'s General Data Protection Regulation (GDPR):

The Bank is committed to ensuring the security and protection of the personal information that we process and to provide a compliant and consistent approach to data protection. Where applicable, in light of required changes to data privacy and data protection based on the EU General Data Protection Regulation which went into effect in the European Union on May 25, 2018, we have updated and expanded our existing data protection program to meet the demands of the GDPR. The Bank has appointed a Data Privacy Team to develop, implement and maintain our roadmap for complying with this new data protection regulation. The team is responsible for promoting awareness of the GDPR across the organization and to ensure full compliance with the new policies, procedures and measures.

[1] From the National Institute of Standards and Technology 'Framework for Improving Critical Infrastructure Cybersecurity' dated 4/16/2018.