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 privacy and security 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;
- Respond to information security and privacy incidents in a timely manner.

Enterprise Information Security

Our Enterprise Information Security Program is reviewed and approved by the Board of Directors and 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 our Enterprise Information Security teams perform application and network threat modeling and penetration testing.

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

- Comply in good faith with applicable laws, regulatory guidance, and financial institution standards to protect the confidentiality, integrity, and availability of non-public personal and other confidential 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.

The program seeks to:

- **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:
The Bank has a formal Incident Response Program that encompasses reporting, response, and notification procedures. The program includes processes to respond to a breach of electronic or physical security or the loss or exposure of data that has the potential to result in unauthorized access to confidential 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:
The 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, 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

The Bank's policy is to comply in good faith with applicable privacy laws and regulations. The Privacy Office establishes and maintains an enterprise-wide data privacy and protection program.

Personal Information and Sensitive Personal Information:
The Bank maintains a program to help safeguard personal information, including sensitive personal information, like social security numbers, government issued identification numbers, and financial account numbers, through the use of ongoing risk assessments, monitoring, and control testing. In addition, privacy training is delivered to employees regarding the handling and safeguarding of personal information. The Bank's privacy notices and online privacy practices may be viewed on the Bank's websites.

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 providing a compliant and consistent approach to data protection and individual rights in compliance with the GDPR's requirements.

Individual Rights:
Where required by law, we respond to an individual's request regarding their personal information held by the Bank, such as the rights to request access, delete, or opt out of the sale of their personal information. Certain residents of California are granted these rights under the California Consumer Privacy Act (CCPA) and can exercise these rights by visiting mufgamericas.com/privacy.

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