

Exhibit 7—U.S. Bancorp Enterprise Preparedness Program Overview

U.S. Bank's Enterprise Preparedness Program establishes and supports our organization's Business Continuity and Contingency Planning Program. The program is designed to evaluate the impact of significant events that may adversely affect customers, assets or employees. This program helps ensure that U.S. Bank and its applicable affiliates can recover our mission-critical functions and applications, thereby meeting our fiduciary responsibility to our stakeholders and complying with the requirements of the Federal Financial Institutions Examination Council (FFIEC), the Securities and Exchange Commission (SEC), the Office of the Comptroller of the Currency (OCC), the Financial Industry Regulatory Authority (FINRA) and the Office of the Superintendent of Financial Institutions (OSFI). In addition, we have met all recovery criteria as prescribed by the Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System.

The U.S. Bancorp Board of Directors approves the U.S. Bancorp Enterprise Preparedness Policy annually, and key issues and status are reported to the Board and senior executives on a periodic basis.

Crisis Management (CM) manages and coordinates the enterprise response to adverse events that threaten to harm our organization, stakeholders, employees, assets or reputation. The enterprise response focuses on the safety of all employees, customers and assets of U.S. Bank; minimizing disruption of service and/or inconvenience to customers; returning to a business-as-usual state as quickly as possible; and limiting any potential liability of the organization.

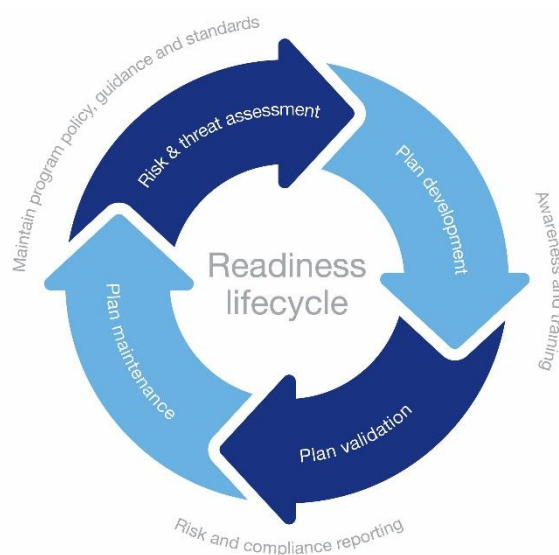
Additionally, CM maintains situational awareness and facilitates CM planning, conducts training, tests, exercises and maintains the emergency notification system. Crisis Management oversees the information flow between our lines of business, tiered response teams and executive management. The tiered incident response teams consist of the following:

- Executive Crisis Management Team
- First Response Executive Team
- International Response Team
- Emergency Response Team

The U.S. Bancorp Pandemic Preparation and Response Plan was developed in partnership with senior leaders and other critical support departments to prepare for the possibility of pandemic flu in the same way that we prepare for other events that could affect our employees, customers and communities. The plan was prepared in communication with public officials, pandemic planning experts, various state and local organizations, and other financial institutions and businesses. The plan augments procedures already in place as part of the existing Enterprise Preparedness Program and outlines strategies to mitigate the impact of a pandemic upon our company, employees and customers.

We have resources dedicated to the Enterprise Preparedness Program and detailed Business Continuity Plans and Disaster Recovery Plans for the restoration of critical processes, applications, infrastructure and operations. Key features of our planning process include:

- Employee safety strategies and communications/notifications



- Systems and telecommunications accessibility
- Alternate physical site location and preparedness
- Emergency notification processes and systems
- System and data backup and recovery
- Pandemic and high employee absenteeism

The Enterprise Readiness Services department coordinates strategy, planning, testing, reporting and monitoring of the U.S. Bank Enterprise Preparedness Program across our organization. The Enterprise Preparedness group has set forth guidelines which incorporate industry best practices for recovery of critical business units, recovery of technology, and emergency and crisis management response and integrates the program into the overall risk management framework.

- **Criticality assessments**—The Criticality assessments are used in the determinations of business process and application recovery time objectives, which addresses impacts based on financial, operational, reputational and regulatory risk factors.
- **Business impact analysis (BIA)**—The BIA measures the effects of resource loss and escalating losses over time in order to provide management with reliable data upon which to base risk mitigation and continuity planning. BIA is reviewed biennially in conjunction with plan.
- **Threat vulnerability assessment**—Our Enterprise Preparedness Program utilizes a Threat Vulnerability Analysis (TVA) process, biennially, to assess the risk of major natural hazard events and the impacts of those events on our corporate locations and the mission critical processes/technologies executed at those locations. This analysis drives strategic recovery planning for continuity of operations for these processes and technologies at the selected locations. The planning process assists in mitigating the potential concentration risk exposure of a single natural hazard or man-made event to any particular location or process.
- **Business continuity, disaster recovery and vendor service plans**—The plans are a documented collection of procedures and information that is developed and maintained to enable us to provide products and services at an acceptable predefined level in the event of a business, technology or third party disruption. Recovery plans are reviewed and approved by senior management biennially at a minimum, or as changes occur to mission critical functions and applications or as a result of issues discovered during exercises/tests.
- **Exercising/testing**—All aspects of the plans are exercised/tested in accordance with regulatory requirements and U.S. Bank Enterprise Preparedness Policy guidance, and to demonstrate the level of recoverability. This includes plan activation simulation, including recovery strategies, crisis management and response, business continuity processes and critical infrastructure disaster recovery. Key mission critical applications are exercised on a quarterly basis. Business Continuity Plans are exercised on an annual basis. Mainframe data is mirrored and replicated to the hot site and server backups are stored off-site in a secured climate-controlled environment. All exercise testing is measured and reported with identified issues documented and remediated.
- **Audit**—Annual internal audits and periodic OCC/Federal Reserve exams are conducted on the U.S. Bank Enterprise Preparedness Program.
- **Board of Directors Updates**—The Enterprise Preparedness group provides annual updates at a minimum on the status of our Enterprise Preparedness Program to the Audit Committee of the Board of Directors of U.S. Bancorp.
- **Employee training and awareness**—Employee training and awareness includes biennial training courses, evacuation procedure awareness and identifying employees' roles and responsibilities during an adverse event. Clear communication during an event is vital. Employees who support mission critical operations and technologies are trained through participating in functional exercises of recovery plans.

Our Business Continuity Plans are developed and maintained to address recovery strategies for such events as: pandemic/high employee absenteeism, technology outages, natural hazard impacts, etc. Below are examples of what might occur during an interruption of normal business operations.

In the event a business site becomes inaccessible, we presently employ the following recovery strategies for mission critical functions:

- **Transfer work**—Work is transferred to another location that does the same business function or has been cross trained.
- **Relocate people within business**—Team members are relocated to another site.
- **Relocate to regional recovery center**—A location, other than normal facility, will be used to process data and/or conduct critical or necessary business functions.
- **Vendor work area recovery**—An external site will be used for the recovery of mission critical personnel and processes utilizing a third party owned location.
- **Work from home**—Team members will work from home on a bank-owned device.

In the event of a data center outage, we utilize an internal alternate data center, which is geographically disbursed, and utilizes near real-time data replication on an encrypted WAN connection to our recovery data centers within the prescribed recovery point objectives.

In the event of a major disaster at U.S. Bank that impacts your product or service, a member of the applicable product or service client support team will communicate with you.

Since it is impossible to anticipate every type of potential disaster, there can be no assurance that there will be no interruption of our business functions in all circumstances. The mission of our Enterprise Preparedness program is to minimize the impact of any disruption.

This overview is subject to modification by U.S. Bancorp at any time.