

Business Resiliency Statement

Fedwire® Funds Service and Fedwire Securities Service

Federal Reserve Financial Services (FRFS) operates two core services that support critical U.S. financial markets activity – the Fedwire Funds Service and the Fedwire Securities Service (collectively known as the Fedwire Services).

The Fedwire Funds Service is a real-time, gross settlement system that banks, businesses and government agencies rely on for mission-critical, same-day transactions. Each transaction is processed individually and settled upon receipt via a highly secure electronic network. Settlement of funds is immediate, final and irrevocable. The Fedwire Securities Service provides cost-effective issuance, maintenance, transfer and settlement services for all marketable U.S. Treasury securities, as well as certain securities issued by other federal government agencies, government-sponsored enterprises and international organizations. The Fedwire Securities Service processes securities transfers on an individual basis in real time, and the transfer of the securities and the related funds (if any) is final and irrevocable when made.

Systemically important financial market infrastructures (FMIs) are expected to meet the public policy objectives of the CPMI-IOSCO *Principles for Financial Market Infrastructures* (PFMI).¹ The Board of Governors of the Federal Reserve System has incorporated principles 1 through 24 of the PFMI into part I of the Federal Reserve Policy on Payment System Risk (the PSR policy).² As stated in the PSR policy, the Fedwire Services are expected to meet or exceed the risk management standards applicable to financial market infrastructures and as set forth in part I of the PSR policy. For detailed information regarding how the Fedwire Services observe the principles of the PSR policy in maintaining a robust resiliency program, see the PFMI Disclosure Statements for the Fedwire Funds Service and the Fedwire Securities Service.^{3,4}

FRFS has a number of procedures in place to ensure the resiliency of the Fedwire Services. These procedures are routinely tested across a variety of contingency situations to help to ensure

¹ Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO), *Principles for Financial Market Infrastructures* (Apr. 2012), available at <http://www.bis.org/cpmi/publ/d101a.pdf>. In addition, CPMI and IOSCO published related guidance on how the PFMI applies to central bank FMIs, *Application of the Principles for Financial Market Infrastructures to Central Bank FMIs* (Aug. 2015), available at <http://www.bis.org/cpmi/publ/d130.pdf>.

² Board of Governors of the Federal Reserve System, *Federal Reserve Policy on Payment System Risk* (amended July 20, 2023), available at https://www.federalreserve.gov/paymentsystems/files/psr_policy.pdf. The Board of Governors has noted that, in applying part I of the PSR policy, it would be guided by the key considerations and explanatory notes in the PFMI.

³ PFMI Disclosure Statements for the Fedwire Funds Service, available at <https://www.frbervices.org/assets/financial-services/wires/funds-service-disclosure.pdf>, and for the Fedwire Securities Service, available at <https://www.frbervices.org/assets/financial-services/securities/securities-service-disclosure.pdf>.

⁴ While not subject to the enhanced risk-management and disclosure requirements applied to the Fedwire Services under the PSR policy, the National Settlement Service, a multilateral settlement service owned and operated by the Federal Reserve System, is part of the same resiliency program as Fedwire Funds Service and Fedwire Securities Service.

resumption of Fedwire operations in the event of a local, regional or widespread disruption. The suite of Fedwire applications and associated recovery procedures are regularly evaluated and enhanced to address various emerging risk scenarios, such as those that might occur during a cyber event. The below sections generally describe certain safeguards and other measures designed to protect the Fedwire Services in the event of a disruption but are not intended to specifically describe what will happen in such event.

Data Centers

FRFS operates the applications that are necessary for the operation of the Fedwire Services from several different data centers, which are located with sufficient geographical dispersion to mitigate the effects of most natural disasters, power and telecommunication outages, and other widespread regional disruptions. Fedwire Services operations regularly rotate between two primary data centers. The data centers have the necessary staffing, equipment and security to resume operations and include various contingency features, such as redundant power feeds, environmental and emergency control systems, dual computer and network operations centers, and dual customer service centers. The primary data centers include full same-site processing redundancy to address local failures. The primary data centers also support full cross-site processing redundancy, so either data center can quickly take over production processing if the data center that had been processing production work is, or is expected to be, disrupted.

In the event of a primary data center outage or in advance of an impending contingency event, the affected applications will be recovered to the other primary data center within an established time objective, with a somewhat longer recovery time for the various ancillary applications supporting the Fedwire Services. These recovery objectives are documented requirements in agreements with Reserve Bank service providers. If, in the course of restoring production-processing capability the Reserve Banks detect data loss, they have reconciliation processes in place to identify and inform participants of transactions that may need to be resubmitted.

The Fedwire operation sites that support the Fedwire Services are located in different geographic regions of the country to help ensure they can continue to support the Fedwire Services even in the midst of a widespread disruption. Furthermore, FRFS personnel with key recovery and crisis management responsibilities are also located in different areas of the country to help ensure critical operations can be conducted if a disruptive event affects a particular region. Fully trained personnel capable of opening and closing the applications that support the Fedwire Services are located around the country. These personnel routinely provide production support to help ensure their skills remain current.

Contingency Testing

Several alternate-site recovery tests are conducted per year for the Fedwire Services. In addition, once a year, FRFS conducts a third-site test in which core applications are failed over to the backup data center.

Certain large Fedwire Services participants are required to participate in at least one of these contingency tests per year. During the contingency tests, participants test their ability to reconcile and resume processing of their transactions following a Fedwire Funds Service or Fedwire Securities Service application recovery event. Additionally, Fedwire Services participants are encouraged to conduct testing from their alternate site during regularly scheduled customer test windows. FRFS also shares the schedule of these tests so they may occur when other FMI's are conducting similar contingency tests.

Furthermore, full cross-site processing redundancy, including by rotating Fedwire Services operations between the primary data centers for production processing, are conducted multiple times a year. FRFS also coordinates and participates in tabletop exercises to test resiliency procedures, including scenarios such as a protracted disruption of the Fedwire Services. Such tests and exercises help to identify the risks the Fedwire Services face and to help FRFS improve the resiliency of the Fedwire Services.

Lastly, FRFS has taken a number of other steps to minimize the likelihood that an event at one of the Reserve Bank locations will affect the operation of the Fedwire Services. For example, Reserve Banks routinely test their own physical security, evacuation procedures, emergency notification plans, smoke-detection systems, fire extinguishers and uninterruptible power supplies. They also have procedures in place to mitigate the impact of a reduction in staff across multiple locations in a pandemic situation. Specifically, they have cross-trained staff so that they can continue to operate critical activities effectively in reduced-staff scenarios.

Fedwire participants may contact their designated relationship manager for additional information.

The Federal Reserve Financial Services logo, "Fedwire" and "Wired to Deliver" are service marks of the Federal Reserve Banks. A list of marks related to financial services products that are offered to financial institutions by the Federal Reserve Banks is available at [FRBfinancialservices.org/terms](https://frbfinancialservices.org/terms).

Updated June 2024