BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
DIVISION OF RESERVE BANK OPERATIONS AND PAYMENT SYSTEMS

Date: September 6, 2022

To: Board of Governors

From: Staff[1]

Subject: Proposed amendments to the operational risk management requirements for designated financial market utilities (Regulation HH)

ACTION REQUESTED

Staff requests approval to publish the attached draft *Federal Register* notice,[2] which invites comments on proposed changes to the operational risk management requirements for designated financial market utilities (designated FMUs) in Regulation HH. The updates reflect changes in the operational risk, technology, and regulatory landscapes since 2014, when the Board last substantively updated the regulation to incorporate the *Principles for Financial Market Infrastructures* (PFMI).[3]

BACKGROUND

FMUs provide essential infrastructure to clear and settle payments and other financial transactions. The Board has long promoted the safety and efficiency of FMUs in order to foster the safety and soundness of U.S. financial institutions and promote financial stability.[4]

In recognition of the criticality of FMUs to the stability of the financial system, the Dodd-Frank Act established a framework for enhanced supervision of FMUs that have been designated as systemically important by the Financial Stability Oversight Council (FSOC). At present, there are eight designated FMUs, and the Board is the supervisory agency under the Dodd-Frank Act for two of them – The Clearing House Payments Company, L.L.C. (on the basis of its role as

[1] Jennifer Lucier, Stuart Sperry, Emily Caron, Kathy Wang, and Katherine Standbridge (RBOPS); Evan Winerman, Cody Gaffney, Ben Snodgrass (Legal).
[2] Staff requests the authority to make technical, non-substantive changes to the FRN prior to publication.
[3] The PFMI, published by the Committee on Payment and Settlement Systems (now the Committee on Payments and Market Infrastructures) and the Technical Committee of the International Organization of Securities Commissions in April 2012, is widely recognized as the most relevant set of international risk-management standards for payment, clearing, and settlement systems.
[4] For example, in 2004, the Board approved changes to Part I of the *Federal Reserve Policy on Payment System Risk* (PSR policy) addressing risk management in payment and securities settlement systems. 69 FR 69926 (Dec. 1, 2004).

operator of the Clearing House Interbank Payments System (CHIPS)) and CLS Bank International.[5] By law, the Board is required to prescribe risk-management standards governing the operations of these FMUs.[6] Thus, the Board's regulation includes a set of 23 risk-management standards addressing governance, transparency, and the risks that could arise in a designated FMU's payment, clearing, and settlement activities, including legal, financial, and operational risks. These standards are based on and generally consistent with the PFMI.

One of the risk-management standards in the regulation addresses operational risk, which is the risk that deficiencies in an FMU's information systems, internal processes, and personnel or disruptions from external events will result in the deterioration or breakdown of services provided by an FMU.[7] The regulation requires a designated FMU to manage its operational risks by establishing a robust operational risk-management framework that is approved by its board of directors.[8] The regulation also contains several specific minimum requirements for business continuity planning, including a requirement for the designated FMU to have a business continuity plan. Importantly, effective operational risk-management, in combination with sound governance arrangements and effective management of general business risk including the risk of losses from operational events, promotes operational resilience.

The broader operational risk, technology, and regulatory landscape has evolved since the Board adopted the current regulation in 2014.[9] New challenges to operational risk management have emerged, including a global pandemic and severe weather events. In addition, certain types of cyberattacks that were once thought to be extreme or "tail-risk" events, like those on the supply chain and ransomware attacks, have become more prevalent. Technology solutions for the management of operational risk have also advanced since 2014, including the development of

---

[5] The Dodd-Frank Act defines "Supervisory Agency" as the Federal agency that has primary jurisdiction over a designated FMU under Federal banking, securities, or commodity futures laws. 12 U.S.C. 5462(8). The SEC is the Supervisory Agency for The Depository Trust Company (DTC); Fixed Income Clearing Corporation (FICC); National Securities Clearing Corporation (NSCC); and The Options Clearing Corporation (OCC). The CFTC is the Supervisory Agency for the Chicago Mercantile Exchange, Inc. (CME); and ICE Clear Credit LLC (ICC). See https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc/designations.

[6] Section 805(a)(1)(A) of the Act requires the Board to prescribe risk-management standards, taking into consideration relevant international standards and existing prudential requirements, governing the operations related to payment, clearing and settlement activities of designated FMUs. In addition, section 805(a)(2) of the Act grants the U.S. Commodity Futures Trading Commission (CFTC) and the U.S. Securities and Exchange Commission (SEC) the authority to prescribe such risk-management standards for a designated FMU that is, respectively, a derivatives clearing organization (DCO) registered under section 5b of the Commodity Exchange Act, or a clearing agency registered under section 17A of the Securities Exchange Act of 1934. 12 U.S.C. 5464(a)(1).

[7] Although the term "operational risk" is not defined in current Regulation HH, when the Board proposed amendments to section 234.3(a)(17) in 2014, it described operational risk as such. The Board also adopted this definition of operational risk in the PSR policy and the ORSOM rating system for designated FMUs.

[8] In this notice, section 234.4(a)(17) will be informally referred to as the "operational risk management standard."

[9] For example, in 2016, the CPMI and IOSCO published *Guidance on cyber resilience for financial market infrastructures* (Cyber Guidance), which supplements the PFMI and provides guidance on cyber resilience.

new technologies that have the potential to improve the resilience of designated FMUs. Finally, the legal and regulatory landscape in which designated FMUs operate has evolved to reflect these changes and strengthen expectations for supervised financial institutions.[10]

In light of these changes, staff conducted a review of the operational risk management standard in the regulation in order to promote effective risk management in a rapidly evolving risk environment, identify opportunities to help address challenges that supervisory teams have faced in applying the existing principles-based standards, and further align, as appropriate, with relevant requirements established by regulators such as the U.S. Securities and Exchange Commission (SEC) and the U.S. Commodity Futures Trading Commission (CFTC). Following staff's review of the operational risk management standard in the regulation, we believe that the current provisions of the regulation are generally still relevant and comprehensive. However, staff identified several areas where it believes updates to the rule are necessary.

Staff recommends that the Board request comment on amendments to the operational risk management requirements in the regulation to ensure its expectations reflect changes to the environment. We have consulted informally with CFTC and SEC staffs in the development of this draft proposal.

DISCUSSION

The draft proposal would make revisions to the regulation addressing (1) incident management and notification, (2) business continuity management and planning, (3) third-party risk management, and (4) review and testing.[11] Although some of staff's recommended amendments represent new or heightened regulatory requirements, in most cases, they are largely consistent with existing measures that designated FMUs take to comply with the regulation. We believe they would create minimal added burden for the designated FMUs that are subject to the regulation.

Incident management and notification. Staff is recommending that the Board propose to establish incident management and notification requirements. The regulation currently does not have specific requirements on incident management or notifications. Staff, however, believes that incident management (which would include internal and external escalation considerations)

[10] For example, in November 2021, the Board, the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC) adopted requirements on computer-security incident notifications for banking organizations and bank service providers. 86 FR 66424 (Nov. 23, 2021).

[11] Staff is also recommending several technical or conforming amendments throughout the risk-management standards in Regulation HH.

is a critical aspect of a designated FMU's ability to effectively manage its operational risks. Accordingly, staff believes that the existing operational risk requirements in the regulation include implicit expectations on this topic.

Staff recommends making these expectations explicit, in part, in light of the recent Board, OCC, and FDIC joint rulemaking requiring computer-security incident notification by banking organizations and bank service providers. The interagency rule scoped out designated FMUs. It also explained that the Board believes it is important for designated FMUs to inform Federal Reserve supervisors of operational disruptions on a timely basis and has generally observed such practice by designated FMUs.[12] It also noted that the Board would consider proposing amendments to Regulation HH in the future to formalize its incident-notification expectations and promote consistency between requirements applicable to Board-, SEC-, and CFTC-supervised designated FMUs.[13]

The proposed amendments would require a designated FMU to immediately notify the Board of material operational incidents; immediately notify affected participants in the event of actual disruptions or material degradation to the designated FMU's critical operations and services or to its ability to fulfill its obligations on time; and establish a plan to notify in a timely manner all participants and other relevant entities of all other material operational incidents that would require immediate notification to the Board. For this purpose, a "material operational incident" would occur when the designated FMU activates its business continuity plan or has a reasonable basis to conclude that (1) there is an actual or likely disruption, or material degradation, to any of its critical operations or services, or to its ability to fulfill its obligations on time; or (2) there is unauthorized entry, or the potential for unauthorized entry, into the designated financial market utility's computer, network, electronic, technical, automated, or similar systems that affect or have the potential to affect its critical operations or services.

Staff notes that requiring "immediate" notifications to the Board and to the designated FMU's participants would establish heightened requirements relative to incident notification

[12] *Id*. at 66428.

[13] *Id.* SEC-supervised designated FMUs are subject to the SEC's Regulation SCI, which generally requires covered entities to notify the SEC "immediately" and their members or participants "promptly" of an SCI event. *See* 17 CFR 242.1000 (defining "SCI Event") and 242.1002 (imposing notification requirements related to SCI Events). Similarly, a CFTC-supervised designated FMU must notify the CFTC "promptly" of an "exceptional event". *See* 17 CFR 39.18(g). An "exceptional event" includes "[a]ny hardware or software malfunction, security incident, or targeted threat that materially impairs, or creates a significant likelihood of material impairment, of automated system operation, reliability, security, or capacity; or [a]ny activation of the designated FMU's business continuity and disaster recovery plan." *Id.*

requirements for banking organizations and bank service providers, respectively.[14] The proposed requirement is consistent with the systemic importance of designated FMUs and with existing SEC and CFTC incident notification requirements for the designated FMUs for which either the SEC or the CFTC is the supervisory agency under the Dodd-Frank Act.

Business continuity management and planning. Staff is recommending that the Board propose amendments to its current requirements on business continuity planning under the regulation in order to emphasize the need for designated FMUs to continue to make progress in advancing their cyber resilience capabilities specifically and to demonstrate their business continuity capabilities generally.

The proposed change would require that a designated FMU's business continuity plan set out criteria and processes addressing the reconnection of a designated FMU to its participants and other entities following a disruption to the designated FMU's critical operations or services.[15] Staff believes that the existing requirements to plan for recovery and resumption include an implicit expectation that a designated FMU plan to reconnect to its participants and other relevant entities following a disruption. However, staff believes it is important to make this expectation explicit in order to emphasize the importance of *ex ante* planning for when and how a designated FMU will reconnect to its participants and other relevant entities. For cyber incidents, it is particularly important for a designated FMU to be prepared to assure its participants, other connected entities, and regulator(s) that its remediation efforts are complete and that it has achieved a safe and trusted state.

The proposal would also amend the current regulation, which requires the business continuity plan to be "tested at least annually," by separating it into two requirements addressing testing and review. The proposal would maintain the requirement for at least annual testing, and elaborate on three minimum required outcomes of testing – a designated FMU must demonstrate

[14] The preamble to the FRN explains that "immediate" is meant to convey a sense of urgency in these types of notifications and that it is not meant to be "instantaneous" notification. Under the interagency rule, a banking organization must notify its primary Federal regulator of certain computer-security incidents "as soon as possible and no later than 36 hours" and a bank service provider must notify affected banking organization customers "as soon as possible."

[15] In this context, the staff considers a disruption to a designated FMU's critical operations or services broadly as a form of "disconnection" to external parties such as the designated FMU's participants. This would include situations where a designated FMU deliberately takes itself offline such that participants cannot access its services (for example, if it experiences a major cyberattack that it needs to contain); it would also include situations where a designated FMU loses connection to its participants due to another type of external event (for example, if its production site loses power due to a severe weather event in its region).

that it is able to run live production at its two sites with distinct risk profiles;[16] that its solutions for data recovery and data reconciliation enable it to meet its objectives to recover and resume operations two hours following a disruption and enable settlement by the end of the day of the disruption even in case of extreme circumstances, including if there is data loss or corruption;[17] and that it has geographically dispersed staff who can effectively run the operations and manage the business of the designated FMU.

The proposal would require a designated FMU to review its business continuity plans at least annually. The objectives of this review would be twofold: (1) to incorporate lessons learned from actual and averted disruptions, and (2) to update the scenarios considered and assumptions built into the plan in order to ensure responsiveness to the evolving risk environment and incorporate new and evolving sources of operational risk (e.g., extreme cyber events).

Third-party risk management. Staff is recommending that the Board propose to add a requirement to the regulation regarding the management of risks associated with third-party relationships.[18] The proposal would require a designated FMU to have systems, policies, procedures, and controls in order to effectively identify, monitor, and manage risks associated with third-party relationships. Additionally, for any services that are performed for the designated FMU by a third party, these systems, policies, procedures, and controls must ensure that risks are identified, monitored, and managed to the same extent as if the designated FMU were performing the service itself.[19] Importantly, the risks associated with third-party

[16] Staff also recommends updating the current terminology related to required backup sites in § 234.3(a)(17)(vii)(A), in order to accommodate data center arrangements with multiple production sites, rather than arrangements where one site is considered "primary" and another site is treated distinctly as a "secondary" site. Currently, § 234.3(a)(17)(vii)(A) requires a designated FMU to have a secondary site that is located at a sufficient geographical distance from the primary site to have a distinct risk profile. Staff recommends replacing the references to "secondary site" and "primary site" with a general reference to "two sites providing for sufficient redundancy supporting critical operations and services" that are located at a sufficient geographical distance from "each other" to have a distinct risk profile (collectively, two sites with distinct risk profiles).

[17] The two recovery and resumption objectives of enabling recovery and resumption "no later than two hours following disruptive events" and "completion of settlement by the end of the day of disruption, even in case of extreme circumstances" would remain unchanged under the proposal. The preamble of the FRN reiterates that the Board continues to believe it is imperative to financial stability that a designated FMU be able to recover and resume its critical operations and services quickly after disruptive events, physical and cyber, and to complete settlement by the end of the day of the disruption. However, these recovery time objectives should not be interpreted as a requirement for a designated FMU to resume operations in a compromised or otherwise untrusted state.

[18] The proposal would define "third party" as "any entity with which a designated FMU maintains a business arrangement, by contract or otherwise." Participants of designated FMUs would not be considered third parties. This definition is consistent with the definition of "third-party relationship" in the July 2021 *Proposed Interagency Guidance on Third-Party Relationships: Risk Management*, published by the Board, OCC, and FDIC (86 FR 50789). Staff believes the proposed requirements under Regulation HH would be broadly consistent with the proposed interagency guidance.

[19] Relatedly, the staff believes this proposal is consistent with section 807(b) of the Dodd-Frank Act, which provides each Supervisory Agency of a designated FMU with authority examine the provision of any service integral to the operation of the designated FMU for compliance with applicable law, rules, orders, and standards to the same extent as if the designated FMU were performing the service on its own premises. 12 U.S.C. 5466(b).

relationships would include both the risks stemming from the third party itself, as well as risks stemming from the supply chain.[20]

As with other proposed requirements, staff believes that the current text of the regulation – which requires a designated FMU to identify its "plausible sources of operational risk, both internal and external" and mitigate their impact through appropriate systems, policies, procedures, and controls – includes implicit expectations related to third-party risk management. Staff recommends making this expectation explicit because of the importance of ensuring that a designated FMU's activities do not become less safe when they are outsourced to third parties, and because of the importance of managing particular sources of operational risk associated with third-party relationships, including supply chain risk.

Review and testing. Staff is recommending that the Board propose to add a set of requirements on review and testing in order to provide more specificity regarding the Board's expectations.[21] Currently, the regulation requires designated FMUs to identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate operational risk measures that are reviewed, audited, and tested periodically and after major changes.

The proposed amendments are intended to ensure that a designated FMU takes a comprehensive and risk-based approach to its operational risk management testing and review program, including by assessing whether its operational risk measures function as intended; reviewing the design, implementation, and testing of these operational risk measures after it experiences material operational incidents or after significant changes to the environment in which it operates; and remediating any deficiencies identified during testing and review as soon as possible.

Competitive impact. The Fedwire Funds Service and Fedwire Securities Service are Reserve Bank-operated services that play a critical role in the financial system. Part I of the *Federal Reserve Policy on Payment System Risk* (PSR policy) requires the Fedwire Services to meet or exceed the risk-management standards set forth in the policy, which (like those in the

[20] Supply chain risk encompasses the potential for harm or compromise to a designated FMU that arises as a result of security risks from its third parties' subcontractors or suppliers, as well as the subcontractors' or suppliers' supply chains, and their products or services (including software that may be used by the third party or the designated FMU). The Board identified supply-chain risk as a threat on which the Board is focused in its September 2021 Cybersecurity and Financial System Resilience Report https://www.federalreserve.gov/publications/files/cybersecurity-report-202109.pdf.

[21] As a technical amendment, proposed § 234.3(a)(17)(i) would also emphasize that, just as the current general review and testing requirement applies broadly to the designated FMU's systems, policies, procedures, and controls, the proposed new requirements would also apply to the systems, policies, procedures, and controls developed to mitigate the impact of the designated FMU's sources of operational risk.

regulation), are based on the PFMI. The PSR policy further states that the Board will be guided by its interpretation of the corresponding provisions of the Regulation HH in its application of the risk-management expectations in the PSR policy.[22]

Staff would expect to hold the Fedwire Services to the same requirements as those proposed for the regulation. Therefore, staff does not believe the proposed rule will have any direct and material adverse effect on the ability of private-sector FMUs to compete with the Reserve Banks.

Attachment

[22] *See* section I.B.1 of the PSR policy.