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

Date: February 5, 2024

To: Board of Governors

From: Staff[1]

Subject: Recommended amendments to the operational risk management expectations in Regulation HH

ACTION REQUESTED

Staff requests approval to publish the attached draft *Federal Register* notice and draft final rule, which amends the operational risk management requirements for designated financial market utilities (designated FMUs) in Regulation HH.[2] The updates reflect changes in the operational risk, technology, and regulatory landscapes since 2014, when the Board last substantively updated the regulation. Staff requests the authority to make technical, non-substantive changes to the *Federal Register* notice and final rule prior to publication.

Additionally, § 234.3(a)(17)(vi)(A) of the final rule would require designated FMUs subject to Regulation HH to notify the Board of certain incidents, in accordance with the process established by the Board. Staff requests that the Board approve the attached order delegating to the Director of the Division of Reserve Bank Operations and Payment Systems (or his or her delegatee), after consultation with interested Division Directors, the authority to establish the process for receiving notifications described in section 234.3(a)(17)(vi)(A) of the Board's Regulation HH and to provide notice of this process to affected firms.

[1] Jennifer Lucier, Stuart Sperry, Emily Caron, Angela Thalakottur, Katherine Standbridge, and Elliot Chau (RBOPS); Evan Winerman, Corinne Milliken Van Ness, and Benjamin Snodgrass (Legal).

[2] The expectations in the amended requirements for designated FMUs would also apply to the Fedwire Services, which are Reserve Bank-operated services that play a critical role in the financial system. As noted in part I of the *Federal Reserve Policy on Payment System Risk* (PSR Policy) in applying the policy to the Fedwire Services and other FMIs subject to the policy, the Board is guided by its interpretation of the corresponding provisions of Regulation HH.

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.

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 for two of them – The Clearing House Payments Company, L.L.C. (on the basis of its role as operator of the Clearing House Interbank Payments System (CHIPS)) and CLS Bank International.[3]

By law, the Board is required to prescribe risk-management standards governing the operations of the designated FMUs for which it is the supervisory agency.[4] The Board's Regulation HH includes a set of 23 principles-based 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 *Principles for Financial Market Infrastructures* (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

[3] 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 Securities and Exchange Commission (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 Commodity Futures Trading Commission (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.

[4] 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 CFTC and the SEC the authority to prescribe such risk-management standards for a designated FMU that is, respectively, a derivatives clearing organization 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).

provided by an FMU.[5] 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.[6] 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. The operational risk management standard, along with the regulation's requirements on governance and addressing losses from operational events, promotes operational resilience.[7]

The broader operational risk, technology, and regulatory landscape has evolved since the Board last substantively updated Regulation HH in 2014.[8] 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 have also advanced since 2014, including the development of new tools 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 regulators have strengthened expectations for supervised financial institutions.[9]

In light of these changes, staff conducted a review of the operational risk management standard in Regulation HH in order to promote effective risk management in a rapidly evolving risk environment; identify opportunities to address challenges that supervisory teams have faced in applying the existing standards; and further align the regulation, as appropriate, with relevant requirements established by regulators such as the U.S. Securities and Exchange Commission

[5] 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.

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

[7] *See* 12 CFR § 234.3(a)(2), (a)(15).

[8] 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.

[9] 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).

(SEC) and the U.S. Commodity Futures Trading Commission (CFTC). Staff believes that the current provisions of the regulation are generally still relevant and comprehensive but has identified several areas where it believes updates to the rule are necessary.

DISCUSSION

1. Summary of the Proposed Rule and Comments

On October 5, 2022, the Board published a proposal to amend Regulation HH. The proposed amendments addressed (1) incident management and notification, (2) business continuity management and planning, (3) third-party risk management, and (4) review and testing.[10] In most cases, the proposed amendments were largely consistent with the existing practices of Board-supervised designated FMUs, although some of the proposed amendments represented new or heightened regulatory requirements.

The Board received six comment letters. Two letters were from entities that operate designated FMUs, one letter was from a non-profit organization, and three letters were from individuals. Commenters were generally supportive of the Board's proposals. Staff considered each of these comments in its analysis and recommends final amendments to the rule.

Of the three substantive comment letters received, one commenter expressed support for the amendments as proposed. Two commenters, while expressing support for the overall proposal, raised concerns that aspects of the proposal were broader than necessary. These commenters suggested that amendments to Regulation HH should permit a designated FMU to use a risk-based and proportionate approach to operational risk management. This comment was made both generally and with respect to specific aspects of the proposed revisions.[11] The two commenters also provided detailed comments on specific aspects of the proposed amendments. Brief summaries of those comments are included below.

- **Incident management and notification** – Commenters urged the Board to limit the types of incidents that would require notification. They made recommendations on how notice should be provided to the Board and requested clarification on the timing of the notice requirement.
- **Business continuity management and planning** – Commenters suggested that the Board state in Regulation HH that the existing two-hour recovery and resumption objectives in

[10] The proposed revisions also included technical or conforming changes in Regulation HH's risk-management standards.

[11] Staff generally understands a "risk-based and proportionate approach" as an approach whereby entities identify, assess, and understand the risks to which they are exposed and take measures commensurate with those risks.

Regulation HH, which the Board did not propose to change, should not be interpreted to require a designated FMU to resume operations in a compromised or otherwise untrusted state. Commenters also expressed concern regarding the proposed requirement that a designated FMU demonstrate that its solutions for data recovery and reconciliation enable it to meet the recovery and resumption objectives. They also suggested that the Board clarify a proposed requirement to have criteria and processes to reconnect to participants and other entities following a disruption.

- **Third-party risk management** – Commenters suggested narrowing the scope of the definition of "third party" and suggested that designated FMUs should be permitted to take risk-based approaches to managing third-party risk. They also noted that, for some third parties, designated FMUs may not be able to negotiate information-sharing arrangements or require participation in business continuity testing.
- **Review and testing** – Commenters suggested the review, testing, and remediation provisions be revised to expressly contemplate a risk-based approach. They also suggested revisions to limit more clearly the scope of the review requirement and permit greater flexibility in remediating, mitigating, or accepting the risk of deficiencies in a risk-based manner.
- **Competitive impact** – One commenter asked the Board to revise the risk-management standards in the appendix to the *Federal Reserve Policy on Payment System Risk* (PSR Policy) to align more closely with the wording of Regulation HH and to revise part I of the PSR Policy to include an expectation that the Reserve Banks' National Settlement Service (NSS) meet or exceed the risk-management standards in the appendix.
- **Compliance date** – Commenters expressed the need for additional time to comply with the final rule. They requested 180 days after publication of the final rule in the *Federal Register*, rather than the 60 days proposed by the Board.

2. *Final Rule*

Staff recommends that the Board adopt the attached amendments to the operational risk management requirements in Regulation HH to reflect changes to the operational risk environment. Staff has consulted with the member agencies of the FSOC as required under the Dodd-Frank Act.[12]

The final rule is largely consistent with the proposal, although staff recommends making certain changes in response to public comment and further internal analysis. Staff notes that the final rule would not expressly specify that designated FMUs may use a risk-based and proportionate approach to comply with the amended operational risk management standard. Staff believes that doing so could lead to inconsistent drafting between the operational risk management standard and other sections of Regulation HH that do not expressly refer to a risk-

[12] *See* 12 U.S.C. 5464(a)(1).

based and proportionate approach. Designated FMUs currently use risk-based and proportionate approaches to manage operational risk, and the final rule is not intended to affect designated FMUs' continued use of such approaches where appropriate. Staff, however, recommends revisions in the final rule to incorporate certain specific comments raised by the commenters. The main elements of the final rule and recommended revisions from the proposed rule are summarized below.

Incident management and notification. The final rule would establish incident management and notification requirements for designated FMUs. The final rule would require a designated FMU to immediately notify the Board of material operational incidents, in accordance with the process established by the Board. The final rule would also require a designated FMU to establish criteria and processes for providing timely communication and responsible disclosure to other parties, such that a designated FMU provides (1) immediate notice to 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 (2) timely notice to participants and other relevant entities of material operational incidents that would require immediate notification to the Board, as appropriate, taking into account the risks and benefits of disclosure to the designated FMU and to participants and other relevant entities.[13]

The final rule differs from the proposal in three ways. First, the final rule would clarify that a designated FMU must notify the Board when there is "a vulnerability that could allow for unauthorized entry" into certain designated FMU systems; the proposal would have required notification to the Board when there is a "potential for unauthorized entry." Second, the final rule would clarify that the Board will establish a process for the Board to receive notifications from a designated FMU.[14] Third, the final rule would also clarify that the decision of whether and when to provide notice of material operational incidents to participants and other relevant

[13] By requiring "immediate" notifications to the Board and to the designated FMU's participants, the final rule would establish heightened requirements relative to incident notification requirements for banking organizations and bank service providers, respectively. This heightened requirement is consistent with the systemic importance of designated FMUs. The preamble of the attached *Federal Register* notice reiterates that the term "immediately" is meant to convey urgency and does not mean "instantaneous."

[14] As noted above in further detail, staff is requesting that the Board delegate the authority to establish the process for receiving such notifications and to provide notice of this process to affected firms.

entities should take into account the risks and benefits of the disclosure to the designated FMU and to its participants and other relevant entities.

Business continuity management and planning. The final rule would amend current requirements on business continuity planning under Regulation HH to emphasize the need for designated FMUs to continue advancing their cyber resilience capabilities and to demonstrate and assess their business continuity capabilities generally.

The final rule would require a designated FMU's business continuity plan to set out criteria and processes by which it will reestablish availability for affected participants and other entities following a disruption to the designated FMU's critical operations or services. Staff believes that the existing requirements to plan for recovery and resumption include an implicit expectation that a designated FMU plan to reestablish availability to affected participants and other 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 make itself available to its participants and other relevant entities.[15]

The final rule would retain the existing requirement in Regulation HH that a designated FMU's business continuity plan be "tested at least annually," and would elaborate on three minimum requirements for that testing. First, a designated FMU would be required to demonstrate that it is able to run live production at two sites with distinct risk profiles.[16] Second, a designated FMU would be required to assess the capability of its systems and effectiveness of its procedures for data recovery and data reconciliation in order to meet Regulation HH's objectives to recover and resume operations within two hours of a disruption and enable settlement by the end of the day of the disruption, even in case of extreme circumstances,

[15] 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.

[16] The final rule also would update 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. The final rule would replace 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).

including if there is data loss or corruption.[17] Finally, a designated FMU would be required to demonstrate that it has geographically dispersed staff who can effectively run the operations and manage the business of the designated FMU.

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

The requirements on business continuity management and planning in the final rule differ from the proposal in two ways. First, the final rule would require a designated FMU's business continuity plan to address how it will "reestablish availability for," rather than "reconnect to," affected participants and other entities. This change recognizes that some disruptions may not technically result in a "disconnection." Second, the final rule would require a designated FMU to "assess," rather than "demonstrate," its ability to meet Regulation HH's recovery and resumption objectives. This modification is intended to recognize, as noted by commenters, that there are certain cyber scenarios which may result in extreme data loss or data corruption for which a designated FMU may not be able to demonstrate at this time that its solutions for data recovery and data reconciliation enable it to meet the recovery and resumption objectives. The preamble of the attached *Federal Register* notice explains that the designated FMU should be able to demonstrate to its supervisors that it is working toward increasing the capability of its systems and effectiveness of its procedures to be able to meet those recovery and resumption objectives in the future.

[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 final rule. The preamble of the attached *Federal Register* notice 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, the preamble notes that 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.

Third-party risk management. The final rule would add a requirement to Regulation HH regarding the management of risks associated with third-party relationships. The final rule would define "third party" as "any entity, other than a participant of a designated [FMU] acting in that capacity, with which a designated FMU maintains a business arrangement, by contract or otherwise."[18] The final rule would require a designated FMU to have systems, policies, procedures, and controls that 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, a designated FMU's systems, policies, procedures, and controls would need to ensure that risks are identified, monitored, and managed to the same extent as if the designated FMU were performing the service itself.[19] The risks associated with third-party relationships would include both the risks stemming from the third party itself and risks stemming from the supply chain of the third party.[20]

In addition to the general requirements described above, the final rule would require a designated FMU to (1) regularly conduct risk assessments of third parties; and (2) for third parties that provide functionality, support, or services to the designated FMU without which there could be a material impact on the designated FMU's critical operations or services, (a)

[18] This definition is consistent with the definition of "third-party relationship" in the *Interagency Guidance on Third-Party Relationships: Risk Management*, recently published by the Board, OCC, and FDIC (88 FR 37920), although the exclusion of a designated FMU's participants is specific to Regulation HH. Staff believes the final rule would be broadly consistent with the interagency guidance.

[19] Relatedly, the staff believes the final rule is consistent with section 807(b) of the Dodd-Frank Act, which provides each Supervisory Agency of a designated FMU with authority to 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).

[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.

establish information-sharing arrangements, as appropriate, and (b) address such third parties in the designated FMU's business continuity management and testing, as appropriate.[21]

The final rule differs from the proposal in three ways. First, the definition of "third party" in the final rule has been revised in response to comments to clarify that relationships between a designated FMU and its participants are not "third-party" relationships when the participant is acting in that capacity only.[22] Second, the final rule has been revised in response to comments to limit the scope of the information-sharing and business continuity management and testing requirements; in particular, these requirements would apply only with respect to third parties that provide functionality, support, or services to a designated FMU without which there could be a material impact on any of the designated FMU's critical operations or services. Third, the final rule has been revised to more clearly accommodate approaches to business continuity management and testing that may not include direct participation by each third party.

Review and testing. The final rule would add a set of requirements on review and testing to provide more specificity regarding the Board's expectations.[23] Currently, Regulation HH requires a designated FMU 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 final rule is intended to ensure that a designated FMU takes a comprehensive and risk-based approach to its operational risk management testing and review program, in accordance with a documented testing framework that addresses, at a minimum, scope, frequency, participation, interdependencies, and reporting. Under the final rule, a designated

---

[21] The final rule would define "critical operations or services" as "any operations or services that the designated [FMU] identifies under 12 CFR 234.3(a)(3)(iii)(A)." Section 234.4(a)(3)(iii)(A) of Regulation HH, which would remain unchanged, requires a designated FMU to have an integrated plan for its recovery and orderly wind-down that, among other things, identifies the designated FMU's critical operations and services related to payment, clearing, and settlement.

[22] If a participant maintains other relationships with a designated FMU such as acting as a provider of pricing data, financial risk modeling services, liquidity, or asset custody services, the participant would be within the scope of the definition of "third party" as it relates to its other business arrangements with the designated FMU.

[23] As a technical revision, § 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 apply to the systems, policies, procedures, and controls developed to mitigate the impact of the designated FMU's sources of operational risk.

FMU would be required to do the following: assess whether its systems, policies, procedures, or controls function as intended; review the design, implementation, and testing of affected and similar systems, policies, procedures, and controls after it experiences material operational incidents or after significant changes to the environment in which it operates that could significantly affect the plausible sources or mitigants of operational risk; and remediate deficiencies identified during testing and review as soon as possible.

The final rule differs from the proposal in several ways in order to align with a risk-based approach. The final rule also makes certain clarifications to the scope of the review requirement. These changes are consistent with statements made in the preamble to the proposal but not included in the proposed regulatory text. In addition, the final rule clarifies that a designated FMU is not required to approach all deficiencies in the same manner. The preamble of the attached *Federal Register* notice further explains that remediation could include a range of actions, depending on the facts and circumstances.

Competitive impact. The Fedwire Services are Reserve Bank-operated services that play a critical role in the financial system. Part I of the PSR Policy requires the Fedwire Services to meet or exceed risk-management standards that (like those in Regulation HH) are based on the PFMI. The PSR Policy further states that the Board will be guided by its interpretation of the corresponding provisions of Regulation HH in its application of the risk-management expectations in the PSR Policy.[24]

Although one commenter asked the Board to revise the PSR Policy to more closely align with Regulation HH, staff does not believe such a change is necessary. Staff expects that the Board will continue to hold the Fedwire Services to the same requirements as those in Regulation HH, and therefore staff does not believe the final rule will have any direct and material adverse effect on the ability of private-sector FMUs to compete with the Reserve Banks.

Staff also does not believe that it is necessary at this time to revise the PSR Policy to include the Reserve Banks' NSS. The exclusion of NSS from the list of Federal Reserve services subject to the risk-management standards in the PSR Policy does not have a direct and material effect on the ability of other service providers to compete with the Reserve Banks.

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

Compliance date. In consideration of the public comments as well as internal analysis, the final rule would provide additional time to comply with the rule. The compliance date for most provisions of the final rule would be approximately 180 days following publication in the *Federal Register*. However, designated FMUs would be expected to comply with the requirement to establish a documented framework for incident management approximately 90 days following publication in the *Federal Register*. Staff believes that designated FMUs will be able to leverage existing incident management and notification practices and that an earlier compliance date for this aspect of the final rule would balance the importance of prompt conformance with the final rule with the overall compliance burden on designated FMUs.

3. *Delegation*

As discussed above, the final rule would require designated FMUs subject to Regulation HH to immediately notify the Board of certain incidents, in accordance with the process established by the Board. Staff requests that the Board delegate to the Director of the Division of Reserve Bank Operations and Payment Systems (or his or her delegatee), after consultation with interested Division Directors, the authority to establish the process for receiving notifications described in § 234.3(a)(17)(vi)(A) of the Board's Regulation HH and to provide notice of this process to affected firms. The requested delegation is ministerial in nature and would not affect the types of incidents subject to the notification requirement or the timing for notification. Rather, the requested delegation would permit staff, with the appropriate approvals, to develop and communicate to affected firms the mediums of communication, such as email addresses and telephone numbers, and associated procedures for providing notice to the Board.

Attachment