December 5, 2022

Via Electronic Submission

Ann E. Misback, Secretary
Board of Governors of the Federal Reserve System

Re: **Notice of Proposed Rulemaking – Regulation HH, Operational Risk (Docket No. R-1782)**

Dear Ms. Misback:

The Clearing House Payments Company L.L.C. ("TCH")[1] appreciates the opportunity to comment on amendments to Regulation HH that have been proposed by the Board of Governors of the Federal Reserve System ("Board").[2] The amendments would revise Regulation HH's operational risk management requirements for TCH and the other designated financial market utility ("DFMU") over which the Board has oversight under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act. TCH embraces a risk management culture and understands the importance of operational risk management. We are generally supportive of the Board's proposed changes and agree that the changes are largely consistent with TCH's existing operational risk management framework. However, there are some aspects of the changes that we believe need to (i) more clearly allow for customary risk-based and proportionate approaches to addressing operational issues; (ii) expressly incorporate important clarifications that the Board makes in the supplementary information to the notice of proposed rule making ("NPR"); or (iii) be more narrowly scoped.

For reasons further detailed in our comments below, TCH respectfully requests that the Board revise the proposed amendments by:

- Providing DFMUs with 180 days from publication of a final rule to comply with the new requirements;
- Including certain clarifications that the Board has made in the supplementary information with respect to its two hour recovery and resumption expectations;
- Limiting notification requirements to actual material operational incidents;

[1] The Clearing House Payments Company L.L.C. owns and operates core payments system infrastructure in the United States, clearing and settling more than $2 trillion each day. *See* The Clearing House's website at www.theclearinghouse.org.

[2] Financial Market Utilities, 87 Fed. Reg. 60314 (October 5, 2022) (to be codified at 12 C.F.R. pt. 234).

- Relating the new requirements for reconnection criteria, third parties, testing framework, and post-incident review and remediation to a DFMU's customary risk-based approach to addressing operational issues; and
- Taking int account the limitations DFMUs have in imposing information-sharing requirements on Federal Reserve Banks as service providers and large vendors.

In addition, we respectfully request that appendix 1 of the Payment System Risk Policy be revised so that it more closely aligns with Regulation HH.

Discussion

1. Compliance Date

   Based on its belief that the proposed amendments are largely consistent with existing measures that DFMUs take to comply with the Regulation HH, the Board suggests that the amendments would become effective and require compliance 60 days after a final rule is published. As noted above, we agree that the changes are largely consistent with TCH's existing operational risk management measures. Nonetheless, TCH will need to socialize the final rule with relevant internal stakeholders and review its existing policies, procedures, and practices against the new regulatory requirements. TCH expects it will need to make some changes to its policies, procedures, practices and possibly contracts to conform to the new regulatory requirements. TCH does not think 60 days is a realistic time frame in which to complete this work and therefore asks that the changes require compliance 180 days following publication of a final rule.

2. Business Continuity

   TCH understands and embraces its responsibility to be able to rapidly recover from operational incidents and to resume critical operations and services as quickly as possible. Business continuity of the CHIPS®[3] service has always been a matter of great importance to TCH. In recent years TCH has devoted significant resources to further increasing the CHIPS service's cyber resiliency and we take seriously the ongoing need to continuously evaluate and evolve our capabilities in response to the cyber threat environment. We also take very seriously compliance with regulation.

   Because we take regulatory compliance very seriously we are concerned with the proposed requirement in §234.3(a)(17)(viii)(E)(2) that a DFMU be able to demonstrate that its solutions for data recovery and data reconciliation enable it to meet a two hour recovery time objective, even in cases of extreme circumstances, including data loss and corruption. TCH believes there are

[3] "CHIPS" and The Clearing House logo are registered service marks of The Clearing House Payments Company, L.L.C.

extreme yet plausible circumstances in which it would not be able to recover in two hours.[4] We believe the Board also understands this, based upon its commentary in the NPR.[5]

Consequently, we urge the Board to revise §234.3(a)(17)(viii)(E)(2) to reflect the more realistic and nuanced sentiment that is articulated in the supplementary information to the NPR. In particular, §234.3(a)(17)(viii)(E)(2) should recognize that cyber threats to DFMUs and the technological solutions to address them are still evolving and that DFMUs, in consultation with their supervisors, should "identify reasonable approaches to prepare for and recover from extreme cyber-attacks."[6] Ideally, the final regulation would expressly state that "these recovery time objectives should not be interpreted as a requirement for a [DFMU] to resume operations in a compromised or otherwise untrusted state."[7] Without this critical clarification we are concerned that should TCH experience an extreme cyber event, it may be forced to choose between the operational risk implicit in resuming critical operations and services in an untrusted state and the legal risk of noncompliance with Regulation HH.[8] Such a result would be contrary to the intention of the Board[9] and the direction of TCH's governance bodies.

We also request that the new requirement proposed under §234.3(a)(17)(viii)(D)[10] specify that criteria and processes for reconnection should be risk-based to account for the fact that a reconnection process may not be necessary for all disruptions to critical operations or services or aspects of the process may not be needed. For example, incidents in which there was no malicious intent or external intrusion into DFMU information systems may not necessitate certain reconnection criteria and may not have resulted in disconnection in the first place. We do not think it would be a good use of internal resources to apply reconnection criteria when in TCH's judgment reconnection presents no risk to participants or other entities. Further, the application of criteria in such circumstances would be counter to the larger goal of resuming critical operations and services as quickly as possible so long as the DFMU's systems are in a trusted state.

---

[4] We understand the reference to a DFMU's "recovery and resumption objectives" in proposed §234.3(a)(17)(viii)(E)(2) to mean two hours because §234.3(a)(17)(viii)(B) currently requires a DFMU to have a business continuity plan "designed to enable critical systems, including information technology systems, to recover and resume critical operations and services no later than two hours following disruptive events."

[5] In the NPR the Board notes that " . . . the two-hour recovery time objective has been a particular area of focus during bilateral discussions with Board-supervised [DFMUs], as well as in broader domestic and international fora, specifically in the context of extreme cyber events. At the center of those discussions is the balance between timely recovery and resumption of critical operations and appropriate assurance that critical operations are restored to a trusted state." 87 Fed. Reg. at 60319, 60320.

[6] *See* 87 Fed. Reg. at 60320.

[7] *Id.*

[8] Admittedly this risk exists today, but with this revision of Regulation HH the Board has an opportunity to mitigate that risk.

[9] In the NPR the Board notes that " . . . these recovery time objectives should not be interpreted as a requirement for a [DFMU] to resume operations in a compromised or otherwise untrusted state." 87 Fed. Reg. at 60320

[10] This proposed section would require that a DFMU have a business continuity plan that "[s]ets out criteria and processes that address the reconnection of the designated financial market utility to participants and other entities following a disruption to the designated financial market utility's critical operations or services." 87 Fed. Reg. at 60326.

3. Notification Requirement

New proposed requirements under §234.3(a)(17)(vi) would require TCH to include in its incident response framework a plan for notification and communication of material operational incidents to the Board, participants, and other relevant entities. Specifically, TCH would be required to immediately notify the Board when TCH activates its business continuity plan for the CHIPS service or has a reasonable basis to conclude that (1) there is an actual or likely disruption or material degradation to any of the critical operations or services of the CHIPS service or its ability to ability to fulfill its obligations on time; or (2) there is an unauthorized entry, or the potential for unauthorized entry, into CHIPS systems that affects or has the potential to affect the critical operations or services of the CHIPS service. In addition, TCH would be required to notify affected participants immediately of actual disruptions or material degradation to any critical operations or services of the CHIPS service, or to the ability of the CHIPS service to fulfill its obligations on time. Lastly, TCH would be required to timely notify participants and other relevant entities of material operational incidents that TCH has reported to the Board but that do not meet the criteria for immediate notice to participants and other relevant stakeholders.

When TCH experiences material operational incidents involving the CHIPS service, it already provides very prompt notice (during business hours) to members of its Federal Reserve supervisory team. Similarly, TCH already provides very prompt notice to CHIPS participants of actual disruptions to the CHIPS service. While the creation of a regulatory notice requirement will require TCH to implement formal policies and procedures to demonstrate its compliance with Regulation HH, which will take longer than 60 days, TCH does not disagree with a regulatory requirement for notice.

Where TCH has concerns is with the requirement to notify the Board and participants of likely disruptions or incidents that have the potential to affect critical operations or services. "Likely" and "potential" impact is a low standard for a regulatory notice requirement. We are concerned that notices of likely or potential impacts will (i) cause unnecessary apprehension for matters that turn out to be false alarms or that are quickly resolved without actual disruption to the CHIPS service; (ii) give the impression to our participants that the CHIPS service is unreliable simply because it experiences short, occasional operational occurrences that do not cause actual disruptions; and (iii) desensitize the Board and participants to notifications such that they cannot discern notices of significant incidents from short, occasional occurrences.

Further, requiring notice for likely or potential impacts is inconsistent with other relevant standards for notice. Under the Computer Security Incident Rule, which the Board refers to in the NPR, TCH must provide notice for its non-CHIPS services to its participants for actual incidents that are expected to impact a service for four or more hours.[11] We further anticipate that TCH as

[11] A "computer security incident" is defined as "an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits." 12 CFR §225.301(b)(4). TCH, as bank service provider, must notify at least one contact at each affected bank when it determines that a computer security incident has materially disrupted or degraded, or is reasonably

the operator of the CHIPS service will have notification requirements under future regulations that implement the Cyber Incident Reporting for Critical Infrastructure Incident Act, which also limits notification to actual incidents.[12] Consistency with these reporting standards will simplify TCH's internal policies and procedures and enable TCH to more efficiently respond to operational incidents.

For the reasons explained above, we suggest that proposed §234.3(a)(17)(vi) be revised to require (i) immediate notification to the Board and participants of actual operational incidents that disrupt or materially degrade any of the critical operations or services of the CHIPS service or the ability to fulfill its obligations on time; (ii) immediate notification to the Board and timely notification to participants of actual unauthorized entry into CHIPS systems that affects the critical operations or services of the CHIPS service; and (iii) timely notification to stakeholders TCH has identified in its incident management plan of incidents TCH has reported to participants.

Regarding the requirement that TCH provide "immediate" notice to the Board and, under certain circumstances, to its participants, TCH believes it is important that the concept stated by the Board in the supplementary information that "immediate" is meant to convey urgency but does mean instantaneous needs to be stated expressly in Regulation HH.[13] Additionally, if the Board wishes to receive immediate notice as it has proposed, TCH would need to know whom to contact and how to contact them during overnight, weekend, and holiday hours. Last, in response to the Board's question about whether it should establish a central point of contact for notices or whether DFMUs should provide notice to their supervisory teams, TCH believes it is more practical to contact its supervisory team, assuming the team can be reached outside of business hours. This will prevent TCH from having to notify a central contact and its supervisory team separately since TCH believes its supervisory team will continue to expect to be notified regardless of how this notification requirement is finalized.

4. Third-Party Risk Management

While TCH has a robust third-party risk management practices today, proposed §234.3(a)(17)(ix) presents certain challenges for us. First, and most importantly, the definition of third party would include the Federal Reserve Banks since they provide the Fedwire® Funds Service, the National Settlement Service, and the CHIPS Prefunded Balance Account, which are critical services for the CHIPS service and ones that can only be provided by the Federal Reserve Banks. TCH does not have the ability to compel the Federal Reserve Banks to provide it with information about disruptions to their services or information about their information security controls or

---

likely to materially disrupt or degrade, covered services provided to a bank for four or more hours. 12 CFR §225.303(a).

[12] Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, 136 Stat. 49 (2022). Under the statute, covered entities are required to notify the Cybersecurity and Infrastructure Security Agency of certain covered cyber incidents, which are defined to exclude "an occurrence that, imminently, but not actually jeopardizes (i) information on information systems, or (ii) information systems." Cyber Incident Reporting for Critical Infrastructure Act § 103(a) (codified at 6 U.S.C. § 2240(6)).

[13] 87 Fed. Reg. at 60318.

operational resilience objectives and capabilities.[14] Hence, for TCH to comply with the proposed amendments we request that the Board implement requirements for the Federal Reserve Banks to provide the information a DFMU needs to perform robust third-party risk management. Alternatively, we request that the Board exclude central banks from the definition of third party in the regulation. We also request that the definition of third party be revised to apply to a more specific set of entities. Third parties for purposes of Regulation HH should only include those entities with which a DFMU maintains a business arrangement that could have a material impact on its designated activities.

Another concern we have with the new third-party risk management requirement is that TCH does not have the negotiating power to require certain service providers, such as large telecommunication companies, to agree to the kinds of information sharing arrangements or business continuity testing that the Board has described in the supplementary information to the NPR. However, TCH mitigates potential risk posed by these service providers in other ways, such as having back up power systems and redundant and diverse telecommunication channels. We believe that these existing arrangements are sufficient to manage risk for these service providers. Similarly, we think it is important to clarify that the requirement to include third parties in business continuity management and testing is meant to be limited to outsourced services and not to other types of third-party arrangements like telecommunication service providers. Hence, it is important that proposed §234.3(a)(17)(ix) be revised to take into account both the need for risk-based systems, policies, procedures, and controls and flexibility in how DFMUs manage risk related to third parties, including a clear distinction between third parties providing outsourced services from other third parties.

Additionally, we note that for those third parties for which it is feasible to obtain contractual information-sharing undertakings, it may take more than 60 days for TCH to negotiate and put into place such terms.

5. Testing Framework, Review Following Material Operational Incidents, and Remediation

TCH has a robust testing framework that is consistent with the proposed new requirements in §234.3(a)(17)(i). However, similar to our suggestions for reconnection criteria and third parties, we think the proposed requirements in §234.3(a)(17)(i)(A),(B), and (C) should be expressly risk-based to ensure that a DFMU's testing, review, and remediation activities are proportionate to the level of risk that an event presents.

With respect to reviews that are performed after a material operational incident, TCH's standard post-mortem review identifies the systems, policies, procedures, or controls that were relevant to the incident and determines whether they functioned as intended. If systems, policies,

[14] "To assess risk levels of third parties and monitor any changes in these risk levels that may affect a designated FMU and its ecosystem, the designated FMU should ensure . . . that its information-sharing agreements include, where appropriate, information on the third party's information security controls and operational resilience objectives and capabilities." 87 Fed. Reg. at 60322.

procedures, or controls did not function as intended, TCH identifies why, including whether there was an issue with their design, implementation, or testing. TCH believes this existing practice is consistent with the kind of review that the Board expects to be performed following a material operational incident. But proposed §234.3(a)(17)(i)(B) does not indicate that the review should be focused on systems, policies, procedures, or controls that are relevant to the incident. TCH thus requests that the Board specify in the final rule that a risk-based review be performed on the design, implementation, and testing of the systems, policies, procedures, or controls that are relevant to the material operational incident. While we believe this is a logical reading of the proposed rule, without this clarification, TCH is concerned that the regulation could be read as requiring a review of all of a DFMU's systems, policies, procedures, and controls following each material operational incident.

We also think that the requirement in proposed §234.3(a)(17)(i)(B) to review the design, implementation, and testing of the systems, policies, procedures, and controls following significant changes in the environment in which a DFMU operates should be clarified. In particular, we think that only significant changes to the environment in which a DFMU operates that are reasonably likely to create operational risk should trigger a requirement for review. While we believe this is a logical reading of the proposed rule, without this change, TCH is concerned that the regulation could be read as requiring a review of all DFMU systems, policies, procedures and controls following environmental changes that do not reasonably create operational risk.

With respect to remediation, TCH's current practice is to remediate deficiencies in systems, policies, procedures, and controls that are identified in its post-mortem reviews when such deficiencies are capable of remediation. We believe there are some deficiencies that a DFMU may be unable to fully remediate but can mitigate to a level that is consistent with its risk appetite. We also believe that for situations in which a deficiency was a contributing factor but not a primary cause of a material operational incident, the DFMU should be able to accept the risk of the deficiency if that acceptance is consistent with its risk appetite. For these reasons, we suggest that the remediation that would be required under proposed §234.3(a)(17)(i)(C) be risk-based in order to allow for other responses to deficiencies that are identified in the review of systems, policies, procedures, or controls following a material operational incident so long as the other responses are consistent with the DFMU's risk appetite.

Although proposed §234.3(a)(17)(i)(C) itself does not address validation of remediated matters, the Board states in the supplementary information of the NPR that it would be "imperative" for a DFMU to perform subsequent validation to assess whether remediation measures have addressed the deficiencies without introducing new vulnerabilities.[15] For similar reasons to those discussed above with respect to remediation, we believe that the Board's expectations regarding validation should take into account that whether validation is performed and, when performed, the extent of validation should be risk-based and proportionate to the deficiency that is being

[15] "In order to ensure that remediation measures are effective, it would be imperative for a designated FMU to perform subsequent validation to assess whether the remediation measures have addressed deficiencies without introducing new vulnerabilities." 87 Fed. Reg. at 60317.

remediated. Currently, TCH validates remediations of internal audit findings, issues that are related to regulatory findings, and other issues that rise to a certain level of risk within its risk management framework. TCH may remediate issues that were contributing but not primary factors in a material operational incident but should not be required to validate remediations if they would not otherwise rise to the level for validation under TCH's policies and risk management framework.

We note that although TCH's current practices are largely consistent with proposed §234.3(a)(17)(i)(B) and (C), TCH would need to review its policies and procedures to ensure they align with the new requirements. Based on this review TCH may need to revise its documentation and, if the Board does not revise the requirements as we have suggested, implement new practices to comply with the requirements. It would take more than 60 days for TCH to complete this review and make any updates or changes that are necessary to comply with the final rule.

6. Competitive Impact

TCH appreciates the Board's commitment to apply risk management standards to the Fedwire Funds Service that are at least as stringent as the Regulation HH standards that are applied to TCH as the operator of the CHIPS service.[16] We understand the Board intends to apply the operational risk standard in part I of the Payment System Risk Policy in a manner that is consistent with the proposed changes to Regulation HH. To evidence the Board's intention to apply the new operational risk requirements as well as other aspects of Regulation HH to Fedwire services, we ask that the Board revise appendix 1 to the Payment System Risk Policy so that it more closely aligns with Regulation HH.

As the Board notes, Regulation HH reflects standards that are based on the Principles for Financial Market Infrastructures as well as "specific minimum requirements that a [DFMU] must meet in order to achieve the overall objective of a particular standard" for risk management. [17] In contrast, appendix 1 to the Payment System Risk Policy only restates the Principles for Financial Market Infrastructures. We believe that the standards and minimum requirements that the Board has developed for DFMUs are also generally relevant to applicable Federal Reserve services and that appendix 1 should reflect the standards and minimum requirements that are common for applicable Federal Reserve services and DFMUs. Operational risk management is a standard that we believe has common application.

Last, given the increased importance of the National Settlement Service to the cyber resiliency of the CHIPS service[18] and its longstanding role in supporting settlement of other payment and

[16] *See* 87 Fed. Reg. at 60324.
[17] *See* 87 Fed. Reg. at 60315.
[18] In March 2022, the CHIPS Rules and Administrative Procedures were revised to support use of the National Settlement Service for CHIPS funding and pay out under certain contingency circumstances in which the Fedwire Funds Service is unavailable. *See* Summary of Changes to CHIPS Rules and Administrative Procedures – effective

securities systems, including other DFMUs, we also request that the Payment System Risk Policy recognize the National Settlement Service in part 1 (B)(1)(a) as a service that is subject to appendix 1.

*****

Thank you for your consideration of these comments. If you have any questions or wish to discuss this letter, please do not hesitate to contact me.

Yours very truly,

Alaina Gimbert
Senior Vice President and Associate General Counsel
alaina.gimbert@theclearinghouse.org

March 21, 2022, *available at* https://mc-e3a82812-8e7a-44d9-956f-8910-cdn-endpoint.azureedge.net/-/media/New/TCH/Documents/Payment-Systems/Summary_of_CHIPS_Rule_Changes_03-18-2022.pdf?rev=95a1df1e4b4141fda5933fa8f233ddce.