April 12, 2021

Via Electronic Submission

Ann E. Misback, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

Re: **Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers (FRB Docket No. R–1736 and RIN 7100–AG06)**

Dear Ms. Misback:

The Clearing House Payments Company (TCH)[1] appreciates the opportunity to provide comments on the notice of proposed rulemaking issued by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation (collectively, the "Agencies") regarding the computer-security incident notification requirements for banking organizations and their bank service providers (the "Proposal").[2] TCH recognizes the importance of the Agencies being made aware of emerging threats that may significantly impact individual banking organizations or, potentially, the broader financial system and takes seriously and has consistently fulfilled its responsibility as a payment system operator to provide timely information to its participants about operational incidents that impact them.

While TCH appreciates the Agencies' impetus in drafting the Proposal and their efforts to minimize regulatory burden, TCH believes that the Agencies have significantly underestimated the impact of the Proposal to bank service providers and their bank customers and that the Proposal seeks to address a

[1] Since its founding in 1853, The Clearing House has delivered safe and reliable payments systems, facilitated bank-led payments innovation, and provided thought leadership on strategic payments issues. Today, The Clearing House is the only private-sector ACH and wire operator in the United States, clearing and settling nearly $2 trillion in U.S. dollar payments each day, representing half of all commercial ACH and wire volume. It continues to leverage its unique capabilities to support bank-led innovation, including launching RTP®, a real-time payment system that modernizes core payments capabilities for all U.S. financial institutions. As the country's oldest banking trade association, The Clearing House also provides informed advocacy and thought leadership on critical payments-related issues facing financial institutions today. The Clearing House is owned by 23 financial institutions and supports hundreds of banks and credit unions through its core systems and related services.

[2] OCC, FRB, FDIC, Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, Notice of Proposed Rulemaking and Request for Comment, 86 Fed. Reg. 2299 (Jan. 12, 2021).

need that is already satisfied by existing financial market utility practices. As further discussed in our comments below, TCH respectfully suggests

- For services provided by financial market utilities[3] (FMUs), the most efficient and least burdensome way to achieve the Agencies' goal is to allow the utilities to continue their current practices of notifying their primary federal regulator and bank customers of material operational incidents without regulatory mandate;
- If, in the alternative, there is a regulatory mandate for FMUs to provide certain notices, the mandated notices should be provided to their primary federal regulator for actual and material operational incidents without regard to the cause of incident and the FMUs should continue to provide non-mandated notices to their bank customers of operational incidents consistent with their current practices; and
- Separate from the Proposal, the Board of Governors of the Federal Reserve System (Board) should publicly commit to hold the Federal Reserve Banks to the same notification standards as private sector FMUs with respect to all Federal Reserve financial services.

Discussion

1. The stated purpose of the Proposal is already met by existing FMU practices.

As stated above, TCH recognizes the importance of the Agencies being made aware of emerging threats that may significantly impact individual banking organizations or, potentially, the broader financial system. At the same time we observe that there is no statute that requires the notifications contemplated by the Proposal. Hence, we believe the Agencies should be cautious about imposing obligations on bank service providers in the absence of statute and should look for the least costly way to achieve their goal.

a. Purpose of notifications

The Agencies intend that they be given an "early alert" of "notification incidents" so that they have "earlier awareness of emerging threats" to individual banks or potentially the broader financial system.[4] Once aware of a threat the Agencies believe they can better perform their safety and soundness missions by assessing the extent of the threat and potentially providing information to and facilitating assistance for impacted banks. The Agencies also suggest that the notifications could also serve as data for future supervisory analysis and guidance.

[3] TCH intends financial market utility to have the same general meaning as the term defined in the Dodd Frank Act. The act defines financial market utility as "any person that manages or operates a multilateral system for the purpose of transferring, clearing, or settling payments, securities, or other financial transactions among financial institutions or between financial institutions and the person." 12 U.S.C. § 5462(6). While the definition excludes certain entities that are subject to the Commodity Exchange Act (7 U.S.C. 1 et seq.) and the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.), TCH does not have a view as to how such entities should be treated for purposes of the Proposal.

[4] 86 Fed. Reg. at 2301.

With respect to incidents that involve bank service providers the Proposal would create an indirect information flow in which bank service providers notify their bank customers of "computer security incidents"[5] and each bank customer independently evaluates the notice it has received to determine if the computer security incident impacts its institution to a sufficient degree as to constitute a "notification incident." The Proposal sets the standard for a notification incident to be an incident that materially impacts a bank's ability to carry out its banking operations or services to a material portion of its customer base. Following a determination that a bank service provider's computer security incident is a notification incident, bank customers would then notify their primary regulator of the incident.

b. Existing expectations and practices

While not mandated in TCH agreements or operating rules, TCH notifies its bank customers, either directly or through their technology agents, when there are operational incidents that impact TCH payment systems. However, these notices are not needed to accomplish the Agencies' goal of providing early visibility to the regulatory community of emerging threats. This is because as a matter of practice, TCH currently notifies its primary supervisor when it experiences material operational incidents that impact any of its payment systems. TCH notifies its supervisor for similar types of incidents contemplated by the Proposal: operational problems that cause any of its payment systems to stop operating for more than a short period of time and which may possibly continue for an extended period of time. TCH notifies its supervisor of such incidents whether they are due to a non-cyber cause or (hypothetically) a cyber cause.

While the Proposal assumes that bank customers need to individually evaluate the impact of a bank service provider's "computer security incident" on their institution, TCH believes such evaluation is unnecessary with respect to material operational incidents that impact services provided by FMUs. Such material operational incidents would be of a nature equivalent to a "notification incident" given the critical role that payment systems and other interbank clearing and settlement systems play in the financial system and their importance to the core banking operations and services of their bank customers.

For these reasons, TCH strongly believes that with respect to FMU services the most efficient and least burdensome way of meeting the Agencies' desire for early awareness of emerging threats is for an FMU to simply continue its existing practice of providing timely notice of material operational incidents to its primary federal supervisor. The FMU's primary federal supervisor may in turn share the information as needed within the regulatory community. To the extent the Agencies do not think that all FMUs have

[5] As discussed further below in our comments, we think "computer security incident" can be read to suggest that the Agencies only need to be informed of cyber-related incidents. TCH believes the impact of an operational incident on banks or the financial system is more relevant than the cause of the incident.

a practice of providing timely notice to their primary federal regulator of material operational incidents, such expectations can be articulated through the supervisory process.

2. A regulatory mandate to provide notices will impose significant cost and burden on FMUs.

TCH disagrees with the Agencies' expectation that the Proposal would have "*de minimis*" additional compliance costs for bank service providers.[6] In fact, as further described below, TCH would incur significant costs in standing up internal processes and procedures to comply with a new federal regulatory mandate, bear ongoing cost and burden in having to analyze all operational incidents against the Proposal's definition, and potentially revise its payment system rules and participant agreements to address anticipated vendor management and compliance needs of bank customers.

a. Notices

TCH uses email distributions to provide timely notification to its customers or their technology agents when there are operational incidents that in any way impact the customers of one or more TCH payment systems. Importantly, TCH is able to do this in an efficient and timely way today because TCH (i) does not have to evaluate incidents against a regulatory definition to determine if notice is mandated, (ii) provides notice when there is an actual (rather than a potential) impact to one or more of its payment systems, and (iii) uses existing email distribution groups of operational contacts rather than needing to determine that it has contact information for two separate individuals at each customer.

TCH does not have "automated" means of contacting at least two individuals at each bank customer as the Agencies assume. As noted above, TCH has email distribution lists for operational contacts. These emails are not automated. They must be drafted based upon the circumstances of the incident, reviewed by internal stakeholders, and then sent out. While TCH expects to enhance its customer communication capabilities to better prepare for operational incidents, such communications will always involve some degree of fact-specific drafting and require steps to be executed such that notices cannot be sent "immediately" on an "automated" basis.

With respect to the operational contacts TCH sends the emails to, in the case of customers that connect directly to TCH's payment systems, these contacts are employees of the customer though TCH does not know with certainty whether it has two separate contacts for each such customer. Further, it is common for payment system operators to allow customers to use a third-party service provider as a means of connecting to their systems. In such cases, the payment system operator deals primarily with the third-party service provider as the technical agent of many customers and may not have any operational contacts at the end customer to whom it would provide notifications. Consequently, TCH would need to review its existing distribution lists to determine if it has two separate contacts for each customer that connects directly to TCH systems and acquire additional contacts for those customers for

[6] 86 Fed. Reg. at 2305

which TCH does not have two contacts. It would also need to revise its agreements with customers that use third-party service providers to specifically authorize TCH to provide notices under the Proposal to the service provider as their technical agent. Or, if the final rules do not permit notice to a technical agent, TCH would have to send the mandated notices to the banks rather than their technical agents.

TCH notes that it routinely sends operational notices about many different types of operational matters. Indeed, operations bulletins are almost a daily event. The great majority of these notices involve planned activities or low-level issues. To ensure that bank customers can distinguish between routine notices and mandated computer security incident notices that will trigger regulatory responsibilities for them, TCH would need to classify or label computer security incident notices as such. Otherwise bank customers would have to evaluate all TCH operational notices to determine if they are notification incidents that require notice to their regulator.

b. Internal policies and procedures

If TCH is required to provide mandated computer security incident notices to its customers, it would also incur significant cost and burden because it would need to develop internal policies and procedures to ensure compliance with the regulation. A likely consequence of such policies and procedures would be a need for TCH to (i) develop and document internal controls to ensure that it is managing the risk of noncompliance with the new regulatory mandate, and (ii) create new internal artifacts to document for its internal audit function and its supervisors that TCH is evaluating each operational incident that occurs against the external definition of what triggers the mandated notice, that mandated notices are being provided "immediately" upon determination that the notice has been triggered, and that it is maintaining updated contact lists that ensure that at least two employees or agents of each customer can be reached. We note that because TCH experiences many low-level operational incidents each year these new evaluation and documentation requirements would require significant staff time.

c. Legal terms

Contrary to the Agencies' assumption, the notices TCH provides today are not provided because there is a contractual obligation to do so. Rather TCH provides notices out of practical necessity and as part of good customer service. Although the Proposal states that bank customers would not be held accountable for a bank service provider's failure to provide a mandated notice, TCH's experience with bank customers' vendor management and compliance functions leads us to believe that TCH will in fact be expected to acknowledge the Proposal's requirements in the legal frameworks that govern its payment systems. While TCH previously did this to align with federal regulations regarding financial privacy, in that case the regulations and FFIEC guidance implemented a specific statutory requirement regarding data breach notifications.[7] In contrast, the Proposal does not appear to be implementing statutory

[7] *See* Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §§ 6801-6809.

requirements. Yet the result may well be the same, namely the imposition of contractual terms on privately negotiated agreements between TCH and its customers despite TCH having what it believes are appropriate notification practices in place today.

d. Incident management

The Proposal would also impact TCH's incident management practices. When TCH experiences operational incidents it would need to repeatedly assess such incidents against the definition of computer security incident as TCH understands more about the root cause of incidents and carries out its incident management work. For those incidents in which TCH determines that a mandated notice is required, we believe receipt of a computer security incident notice will prompt a higher level of concern and inquiry by customers than TCH's usual operational notices. This is due to both the regulatory nature of the notice and the fact that "computer security" suggests that there is a cyber element to the incident, even though it is far more likely that there would be a non-malicious root cause. This heightened level of customer inquiry and concern will dramatically increase the demands on internal resources and would detract from the main goal of addressing the incident itself.

3. If there is a regulatory mandate for FMUs to provide notices, certain changes are needed.

Although we strongly believe that the most efficient and least burdensome way for the Agencies to have early awareness of material operational incidents impacting FMU services is to continue existing practices under which FMUs notify their primary federal regulators, if, nonetheless, the Agencies determine that such services will be subject to a federally mandated notice requirement, TCH believes that FMUs should only be required to provide the mandated notification to its primary federal regulator.[8] We emphasize here the inefficiency and unnecessary cost and effort across the industry if FMU bank customers are each individually required to evaluate FMU mandated notices of material operational incidents and each individually notify their federal regulator. As explained previously, we believe this bank level evaluation is not needed given the interbank clearing and settlement functions FMUs provide. TCH would, of course, continue to provide its customary operational notices to its bank customers about the same incidents that it was mandated to report to its regulator; notices that to date have served our customer well.

[8] The Agencies asked whether Designated Financial Market Utilities, such as TCH, believe that mandated notices should be included in Regulation HH. TCH believes the notice requirement should only be in one regulation for all FMU activities.

If FMUs are required to provide mandated notices to either their primary federal regulator or their bank customers, we request the following additional changes to the Proposal.

a. Material operational incident

TCH finds the term and definition "computer security incident" problematic. Because the term and definition are taken from the NIST framework, they have specific meaning for information security programs. For this reason, some might read the Proposal as being limited to incidents that have an information security or cyber cause.

On the other hand, "computer security incident" is broadly defined to include "harm" to the confidentiality, integrity, and availability of information or information systems. When considered outside of the NIST context, such harm can be understood to simply mean any incident that causes an information system to be unavailable or unreliable. Such harm can occur from non-cyber causes such as human error, insufficient testing of technical changes, and hardware failures.[9] In fact, in TCH's experience material operational incidents in which an information system becomes unavailable are just as likely, if not more likely, to have a non-cyber cause than a cyber cause. For example, the unavailability of the Fedwire Funds service on April 1, 2019 and the general outage of all Federal Reserve services on March 24, 2021, which had material impact on banks and FMUs alike, are both understood to have been purely operational in nature without any cyber cause.

For these reasons TCH believes that the standard for determining whether an incident rises to the level to trigger mandated notices should be based on its impact to banks or the financial system and agnostic as to cause. Further, we think that to intentionally limit notices to incidents that have a cyber cause will create additional burden for FMUs and other bank service providers because their evaluation of operational incidents will need to consider both whether there is a cyber cause and what the expected impact is to bank customers and the financial system. This type of determination will generally take longer than determining that an incident has material impact to banks or the financial system. Indeed, the fact that an incident has a cyber cause may not be known until well after the incident has begun having the kind of impact for which the Agencies want to have early warning.

b. Actual incidents

Only actual incidents that a FMU experiences and that it believes in good faith are likely to materially impact its ability to carry out operations or services for an extended period of time should be subject to the mandated notice. The Proposal's definition of computer-security incident includes both actual incidents as well as "potential harm" to information systems and "imminent threat" of violation of security

[9] The Agencies appear to recognize that harm may result from non-cyber causes in their statement in the rulemaking that a "computer-security incident may be the result of non-malicious failure of hardware, software errors, actions of staff managing these computer resources, or potentially criminal in nature." 86 Fed. Reg. at 2300.

policies. It is not clear how TCH would know in the first instance when there is a potential harm or imminent threat of violation (beyond a theoretical understanding that such things could happen[10]) prior to the harm or violation actually happening. Even if it were to have some reason to know of such possibilities, it seems speculative for TCH to conclude that the possible harm or threat of violation could impact its systems for four or more hours. Nonetheless, TCH believes that if it were required to apply this standard it may under certain circumstances feel compelled to make such speculative conclusions and provide mandated notices of potential harms and imminent threats.

We believe that in the context of mandated notices to bank customers, reporting only actual incidents is very important. While TCH thinks that notices of potential events would not be actionable or useful information to the customers of any bank service provider, in the context of FMU services, notices of potential events may in fact be harmful to financial stability. Upon receiving such a notice from an FMU, a bank may overreact out of fear of a cyber event and disconnect from the FMU's system. This reaction may be further exacerbated due to the "immediate" notification requirement since a payment system operator may send such a notice and thereafter determine that the incident did not result in harm to the information system. One or more similar reactions may cause panic or instability across the broader financial system, and the risk that the incident reaches the public increases as larger numbers of banks are notified. Further, such notices may cause significant and potentially irreparable reputational harm to the payment system operator.

c. Timely notification

In addition, the financial industry would be better served by replacing the requirement for "immediate" notification by a federally regulated FMU to a "timely"[11] notice that allows the FMU take a reasonable amount of time to assess the severity of a "computer-security incident" and to ensure that its internal governance processes are followed before disclosing information that may cause instability in the financial market and create significant reputational harm. Similar to the reasoning above, premature notification of events that ultimately are not actual or material may cause more harm than good.

d. Notice to bank customers or their technical agent

If FMUs are required to provide mandated notices to their bank customers, the regulation should require bank customers to identify and update their contacts for mandated notices to their bank service providers rather than place the burden on bank service providers to request and seek updates to these contacts. The regulation should also specify that notice to a technical agent with whom an FMU typically interacts

[10] We note that with respect to the theoretical understanding of potential threats to the financial system, the industry has conducted tabletop exercises involving different kinds of the threats for many years. In recent years these exercises have focused on FMUs and cyber incidents. TCH believes these kinds of exercises have been an effective way for banks and FMUs to prepare for evolving threats.

[11] If FMUs are required to provide mandated notices to their primary federal regulator or their bank customers, FMUs should be given the same amount of time as banks are given for providing their notices to their regulator.

for operational matters involving a bank's connection to the FMU would satisfy the requirement to notify the bank.

e. No assessment

The Agencies stated in the Proposal that a bank's mandated notification to its primary federal regulator "is intended to serve as an early alert" and "is not intended to include an assessment of the incident."[12] Bank service providers, like banks, should also not be expected to provide an assessment as part of its mandated notice whether to its own primary federal regulator or to its bank customers. TCH believes that a bank service provider should not be forced to provide an assessment of an incident when the incident is still ongoing as complete and reliable information may not yet be available or there may not have been time to carefully analyze the information. Given the importance of whether an assessment is required or not, this detail should be included in the regulation and not just supplementary information to the rulemaking.

4. Federal Reserve Bank services should be held to the same substantive requirements as private sector services.

TCH recognizes that the Agencies do not have authority to include Federal Reserve Bank services in the Proposal. Nevertheless, as a matter of fairness and competitive equality, if private sector FMUs are required to provide mandated notices to either their primary federal regulator or their bank customers, the Board should publicly commit to hold Federal Reserve Bank services to an equivalent standard simultaneously with the effective date of the final rule. We note that today in many instances the Federal Reserve Banks notify customers of operational outages only by posting a notice on their public website. The Agencies may want to consider whether this practice should be permitted under the regulations for all service providers as a means of satisfying notice requirements for material operational incidents. If it is not found to be acceptable, TCH respectfully submits that more formal notice should be required of the Federal Reserve Banks for incidents

*****

[12] 86 Fed. Reg. at 2303.

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,

Russ Waterhouse
Executive Vice President
212.613.0171
russ.waterhouse@theclearinghouse.org