April 12, 2021

James P. Sheesley
Assistant Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429

RE: Fiserv Comment on RIN 3064-AF59 Notice of Proposed Rulemaking on Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers

Mr. Sheesley:

Fiserv, Inc. (NASDAQ: FISV), appreciates the opportunity to comment on the joint Federal Reserve System (Fed), Federal Deposit Insurance Corporation (FDIC), and Office of the Comptroller of the Currency (OCC) (collectively, the "joint regulators") Notice of Proposed Rulemaking (NPR) related to bank service provider and banking organization outage incident notification requirements.

Fiserv understands the intent driving this proposed regulation is to make banks and their prudential regulators more aware of outages that threaten the security of a system or that makes the system otherwise unavailable. Additionally, we agree that timely notification is an important component of safety and soundness, and we support the practice of having bank service providers provide transparent and consistent notification to their bank customers when systems are unavailable or compromised. In this spirit, we appreciate the opportunity to provide our feedback to the joint regulators as you work to further develop and finalize this rule.

Ultimately, while we support the intent of the proposed regulation, we believe that some adjustments should be considered to ensure that the rules and requirements include clear and understood definitions, and afford market participants the necessary disclosure protections given the potentially sensitive nature of these notification disclosures. Further, we believe that an effective framework for outage incident notifications should complement current regulatory practices, should provide clear guardrails against irrelevant or unimportant notifications to banking organizations, and provide guidance to all banking system participants in a manner that supports the mission of the joint regulators. A notification structure that inundates banking organizations, service providers, and the joint regulators with non-essential notifications will make it more challenging to identify and respond to significant threats to the banking system.

To achieve these outcomes, we offer four technical suggestions that in our view, if adopted, will align with the joint regulators' efforts to craft rules that balance transparency, information sharing, and early indicators of market disruptions with the potential for notification fatigue or desensitization.

About Fiserv
Fiserv is a global leader in financial services enabling technology and payment processing, and we interact daily with financial institutions of all asset sizes, businesses, and individual consumers. We are a leading account processor, commonly referred to as a "core" provider, delivering digital solutions to

financial institutions in the United States, as well as a provider of many other services to financial institutions, including card processing, bill payments, network services, and security and fraud protection.

Fiserv Perspective

Fiserv supports the desire of the joint regulators to have greater transparency into the health of banking organizations' digital systems and processes and early warning of incidents that pose threats to the confidence and stability of the banking system. Based on the background included within the NPR, we recognize that this proposal is not aimed solely at security incidents, but rather at any outage that could materially disrupt a banking organization's operations and thereby threaten the confidence in the banking system.

Fiserv is focused on providing clarity and transparency to its banking clients about outages that interrupt or degrade systems managed by Fiserv for our banking organizations. These technical comments provide perspective on how Fiserv interprets the NPR and, with adjustment, how we believe the NPR can be strengthened.

As the joint regulators further contemplate the need for a final rule, Fiserv recommends considering the following:

1. provide an express exemption from the bank service provider's notification standard for scheduled or planned maintenance windows;
2. modify the title and definition of *Computer Security Incident* to distinguish between system outages and cyber security outages;
3. modify the bank service provider's notification standard to reduce the potential for over-notification; and
4. redefine *Affected Banking Organizations* to include only *Impacted Banking Organizations and* eliminate the expansion of the notification standard for bank service providers beyond the joint regulators' intended audience.

1. <u>Exempt Scheduled Maintenance Windows from Notification Requirement</u>

As written, the NPR's definition of *Computer Security Incident* could include scheduled and planned maintenance outages that are essential to the integrity and security of digital systems, processes, and programs. Fiserv establishes maintenance windows to perform necessary work on the programs and systems we manage for our banking customers and proactively communicates the cadence and schedule of those maintenance windows. As such, we're concerned that the omission of this exemption could lead to redundant notifications.

Generally, bank service providers will schedule maintenance for a regular cadence during off-peak hours, such as on a Sunday from 12:00 AM ET to 5:00 AM ET. Leading up to this pre-planned maintenance, the bank service provider may also communicate with the bank customer whether it intends to use this window. Within this notification, the bank service provider typically includes an estimated timeframe within the window of an outage and the reason for the maintenance.

If the definition of *Computer Security Incident* does not exclude scheduled or planned maintenance outages, a bank service provider would not only provide advanced notice of the upcoming window (and associated communications), but at the start of the planned outage (in the example above 12:00 AM ET), it would also be required to notify two individuals at the bank of an outage that may last 4 or more

hours, pursuant to the NPR's proposed standards. This second communication could potentially generate an unnecessary and redundant notification. Fiserv does not believe it is the intent of this NPR for the bank service provider to provide an outage notification for this type of outage.

This exemption, however, should not extend beyond the timeframe provided to the bank in the pre-planned scheduled maintenance window. For example, if, in the above example, the bank service provider's maintenance extends past 5:00 AM ET, the outage could result in a notifiable incident under the NPR, should the outage have the potential to extend 4 or more hours beyond the planned maintenance window.

2. Modify the *Computer Security Incident* Definition

As previously stated, Fiserv acknowledges the desire of the joint regulators to provide banking organizations with increased information about all system outages, not just those deriving from cyber security events. This is a standard that Fiserv currently employs and agrees it is an important standard to promote industry wide. The technical corrections that we propose to this definition are intended to provide greater uniformity and clarity to the industry about what constitutes an incident and what constitutes a reportable incident.

As written, Fiserv believes the title and definition of *Computer Security Incident* alludes to the joint regulators' interest and focus on cyber events, such as hacking, malware, or denial of service. As a result, Fiserv proposes that the title and definition should be amended to provide uniformity and clarity and align on the scope of the proposal.

First, Fiserv recommends that the title be renamed to *Outage Notification Incident*. This retitle, or a similar title, increases clarity for bank service providers and banking organizations that the proposal expands beyond cyber security events.

Second, Fiserv believes the NPR would be improved by creating two distinct types of outages identified within an *Outage Notification Incident.* These two forms of outages could be defined as a (1) *System Outage,* or those incidents focused on server interruptions, software issues, natural disasters, or other non-cyber security related events; and (2) *Computer Security Outage,* or those focused on cyber incursions and disruptions.

Moreover, we ask the joint regulators to consider defining *Computer Security Outage* in a way that conforms the language to the definition of "cybersecurity incident" in the following existing federal standard:

- **National Institute of Standards and Technology (NIST) "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1"** –
    - Cybersecurity – The process of protecting information by preventing, detecting, and responding to attacks.
    - Cybersecurity Event – A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).
    - Cybersecurity incident – A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.

Taken together, Fiserv envisions the definition set to read:

> "*Outage Notification Incident" means an occurrence that results in a*
>
> *(1) "System Outage" – the unavailability of an information system or the information the system processes, stores, or transmits; or*
>
> *(2) "Computer Security Outage" – a cybersecurity incident, defined in the National Institute of Standards and Technology "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1."*

3. Modify Bank Service Provider Notification Standard

Fiserv is concerned that the NPR includes duplicative and potentially overly broad language that could result in the unintended expansion of notifications made by bank service providers. The inclusion of both *potential harm* within the *Computer Security Incident* definition and *disrupt, degrade, or impair* within the notification standard for bank service providers could lead bank service providers to create disparate notifications standards.

Focusing solely on computer security, coupling a notification requirement triggered by ***potential*** *harm to the confidentiality, integrity or availability of an information system* **and** a good faith belief it ***could*** *disrupt, degrade, or impair service for four or more hours,* means that identified, interrupted, and mitigated cyber incursion attempts could still result in a bank service provider notifying banking organizations out of an abundance of caution. We believe this may be an unintended expansion of the purpose and scope of the NPR.

Moreover, with both terms included in the NPR, a denial of service attempt against a bank service provider, which is identified and mitigated against – but that results in only slight degradations to a system managed by a bank service provider, could trigger a notification. In this example, despite the fact that the event was identified, mitigated, and was ultimately not a threat to the stability of the bank service provider, banking organization or the financial system – the potential such event could slightly degrade services for 4 or more hours would deem it to be a notifiable incident under the NPR.

We understand that the proposal is intended to promote the safety and soundness of banking organizations by providing an "early alert" of serious threats to the banking system. Successfully identified and mitigated cyber security events do not pose a threat to the safety, soundness, or confidence in a bank or the broader financial ecosystem – and no regulatory alert should be needed in these controlled situations.

As a result, Fiserv recommends that the bank service provider reporting standard be modified to state:

> *A bank service provider, after confirming it is experiencing a [outage notification incident], which it believes in good faith will last more than 4 hours, shall notify the designated 2 individuals at the directly impacted banking organizations of the [outage notification incident].*

4. *Affected Banking Organization* Not Defined – Implication on Bank Service Providers

Fiserv believes the aim of the NPR and any subsequent rule issued by the joint regulators regarding notification requirements is to create a uniform standard that prevents bank service providers or banking organizations from being required to interpret and establish unique and disparate standards and policies. We are concerned, however, that the NPR's broad and undefined use of *affected banking*

organization within the bank service provider notification standards fails to achieve this goal. Fiserv recommends, as highlighted in the updated notification standard above, that only banking organizations directly impacted by an outage should be notified.

As written in the NPR, *affected banking organizations* could be interpreted several ways. Without clarification, it is possible that bank service providers will feel compelled to notify banking organizations of all potential incidents not based on the observance of an actual outage or incident, but based on the location of the banking organization's services within the infrastructure of the bank service provider.

For example, a bank service provider that supports 20 banking organizations on the same multi-tenant platform is informed of a service degradation by a banking organization. Under the proposed notification structure, it is possible that the bank service provider, before knowing the severity, extent, scope, or cause of the degradation, could decide that it is obligated to notify all 20 banking organizations on the multi-tenant platform, to find out upon further review that only one banking organization should have been notified based on actual service degradation.

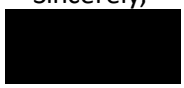
As a result, as drafted, the NPR could compel bank service providers to "over notify" banking organizations, resulting in the unintended consequence of notification fatigue and dilution in the quality and importance of notifications related to the actual safety and stability of the banking system. Fiserv recommends amending the NPR to remove the term *affected banking organizations* and include the clear obligation to notify *impacted banking organizations*.

Conclusion

As the joint regulators further examine the need for a final rule providing outage notification requirements, we believe that our role as a bank service provider positions us well to assist in this effort, and we are willing to provide further technical comment and suggestions as needed. We respectfully request review of the four technical amendments expressed in this comment, as we believe that incorporation of them will enable consistent and uniform notification standards across the financial system and a final rule that achieves the goals laid out in the NPR.

Once again, Fiserv appreciates the joint regulators' willingness to accept comments on this NPR, and we welcome continued engagement, should the joint regulators find further dialogue useful.

Sincerely,



Kim Ford
Senior Vice President, Government Relations
Kim.ford@fiserv.com
(202) 478-1112