Robert M. Fisher, *Chairman*
Brad M. Bolton, *Chairman-Elect*
Russell L. Laffitte, *Vice Chairman*
Gregory S. Deckard, *Treasurer*
Tim R. Aiken, *Secretary*
Noah W. Wilcox, *Immediate Past Chairman*
Rebeca Romero Rainey, *President and CEO*

Via Electronic Mail

April 12, 2021

Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency
400 7th Street SW, Suite 3E-218
Washington, DC 20219

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

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 – OCC [Docket ID OCC–2020–0038; Board [Docket No. R-1736] RIN 7100-AG06; and FDIC - RIN 3064–AF59

Dear Sir or Madam:

The Independent Community Bankers of America ("ICBA")[1] appreciates the opportunity to respond to the Office of the Comptroller of the Currency's, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation (collectively, the "Agencies") notices of proposed rulemaking. The proposed rulemaking would require a bank to notify its primary federal regulator when it believes in good faith that a significant ''computer-security incident'' has occurred. The proposal would also require a bank service provider to notify at least two individuals at an affected bank immediately after experiencing a computer-

[1]*The Independent Community Bankers of America creates and promotes an environment where community banks flourish. ICBA is dedicated exclusively to representing the interests of the community banking industry and its membership through effective advocacy, best-in-class education, and high-quality products and services.*

With nearly 50,000 locations nationwide, community banks constitute 99 percent of all banks, employ more than 700,000 Americans and are the only physical banking presence in one in three U.S. counties. Holding more than $5 trillion in assets, over $4.4 trillion in deposits, and more than $3.4 trillion in loans to consumers, small businesses and the agricultural community, community banks channel local deposits into the Main Streets and neighborhoods they serve, spurring job creation, fostering innovation and fueling their customers' dreams in communities throughout America. For more information, visit ICBA's website at www.icba.org.

security incident that it believes in good faith could disrupt, degrade, or impair services for four or more hours.

Executive Summary

ICBA believes that expanding a bank's notification requirements to its regulator, when a significant computer incident occurred, is duplicative, will be a burdensome task and difficult to implement, and strongly opposes the finalization of such a provision.

In the event the Agencies finalize this proposal, ICBA offers comments and recommendations noted below for the Agency's consideration:

- Provide a safe harbor to banks who, in good faith, may have erred in their initial incident evaluation.
- Replace the NIST term "computer-security incident" with the NIST term "cybersecurity incident."
- Replace the triggering term to report a computer-significant incident from "significant" to "critical" to better capture the intended purpose of reporting an incident.
- Recognize the positive impact of mitigation strategies on an incident and its impact.
- Indicate that an outage, less than 48-hours in duration, does not represent a "notification incident."
- Increase the timeframe to report significant incidents and outages to five business days for banks under $20 billion in assets.
- Develop procedures, with notice and opportunity for comment, the Agencies will take upon receipt of a bank's "incident notification" and how this process will improve a bank's incident response capability.
- Define the term "bank service provider" to be more consistent with the definition of "technology service provider."
- Work with all stakeholders, including core and third-party service providers, to determine appropriate contractual provisions to ensure community banks and third-party service providers can comply with any new requirements.
- Extend the compliance date by 3 years, for community banks, to meet the requirements of the proposed rule.

Background

Cyberattacks reported to federal law enforcement have increased in frequency and severity in recent years. These types of attacks may use destructive malware or other malicious software to target weaknesses in the computers or networks of banking organizations supervised by the Agencies. Some cyberattacks have the potential to alter, delete, or otherwise render a banking

organization's data and systems unusable. Depending on the scope of an incident, a bank's data and system backups may also be affected, which can severely affect its ability to recover operations.

The Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice[2], which interprets section 501(b) of the Gramm-Leach-Bliley Act ("GLBA") and the Interagency Guidelines Establishing Information Security Standards ("IGEISS")[3] generally sets forth the supervisory expectation that a banking organization notify its primary federal regulator ''as soon as possible'' if the organization becomes aware of an incident involving unauthorized access to, or use of, sensitive customer information. Additionally, Under the reporting requirements of the Bank Secrecy Act ("BSA") and its implementing regulations, financial institutions are required to file a Suspicious Activity Report ("SAR") when they detect a known or suspected criminal violation of federal law or a suspicious transaction related to a money-laundering activity. However, the Agencies maintain that the 30-calendar day reporting requirement under the BSA framework (with an additional 30-calendar days provided in certain circumstances) does not provide the Agencies with a sufficiently timely notice of reported incidents.

ICBA Comments

The Agencies are proposing two primary notification requirements. The proposed rule would require a bank to notify its primary federal regulator of any computer-security incident that rises to the level of a notification incident as soon as possible and no later than 36-hours after the bank believes in good faith that a notification incident has occurred. The proposal would also require a bank service provider to notify at least two individuals at an affected bank immediately after experiencing a computer-security incident that it believes in good faith could disrupt, degrade, or impair services for four or more hours.

Regulator notification.
ICBA contends that the Agencies' proposal would be duplicative with other requirements and burdensome on community banks. ICBA urges the Agencies do not finalize the proposed incident notification rule.

Community banks report incident information to several different governmental agencies, departments, and private organizations when an incident occurs. Community banks must report incident information to their primary regulator, to FinCEN through SAR filings, and shared through information sharing organizations such as the Financial Services Information

[2] 12 CFR 208; 12 CFR 225; 12 CFR 30; 12 CFR 364; 12 CFR 568
[3] 12 CFR Appendix F to Part 225

Sharing and Analysis Center ("FS-ISAC")[4], an organization created specifically to share incident information, between private and public partners.[5]

Community banks' reporting of an incident to the Agencies, where customer data is accessed or there is an impact to systems that hold customer data, is already required under GLBA. The Agencies wish to expand the types of incidents that banks report to the Agencies, to include systems that do not hold customer data. However, ICBA contends that access to or outages of systems that do not hold customer data should not be considered critical, since those systems do not represent the essential operations of a bank and the services that they provide to their customers.

Additionally, decreasing the timeframe to report an incident to the Agencies to 36 hours, for community banks, does not provide more utility or value than the GLBA requirement that is already in place, which is to report incidents that impact customer data, as soon as possible.

Should the Agencies move forward with finalizing their proposal, against ICBA's request to the contrary, then ICBA offers comments and recommendations noted below for the Agency's consideration:

Safe harbor.
The proposal requires banks to notify its primary regulator when it believes in good faith that a "notification incident" occurred. While ICBA appreciates the Agencies' flexibility in recognizing good faith efforts, ICBA suggests that there be additional clarity by providing a safe harbor to banks who - in good faith - erred in their initial incident evaluation. Incidents can be difficult to initially diagnose and prone to changing conditions and impacts. A safe harbor should also be given to banks in instances where an incident was initially determined to be relatively non-impactful, but later rises to the condition of a "notification incident."

Computer-security incident definition.
In the proposed rule, the Agencies use the National Institute of Standards and Technology ("NIST") term "computer-security incident", which is defined as an occurrence that:

(i) results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits; or
(ii) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

[4] FS-ISAC was Launched in 1999, FS-ISAC, established by the financial services sector in response to 1998's Presidential Directive 63. That directive, later updated in 2003 by Homeland Security Presidential Directive 7, mandates that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure.
[5] https://www.cisa.gov/critical-infrastructure-sectors

ICBA recommends that the Agencies replace the NIST term "computer-security incident" with the NIST term "cybersecurity incident,"[6] which is defined as a cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery. The term "cybersecurity incident" is more applicable for use in the Agencies' proposed rule as it better reflects the Agencies' definition of a "notification incident." Notification incident is defined as an incident that could materially disrupt, degrade, or impair:

(i) The ability of the banking organization to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business;
(ii) Any business line of a banking organization, including associated operations, services, functions and support, and would result in a material loss of revenue, profit, or franchise value; or
(iii) Those operations of a banking organization, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.

Significant computer security incident.
The Agencies' proposal would require a banking organization to notify its regulator when it believes in good faith that a significant ''computer-security incident'' has occurred. ICBA recommends the Agencies change the term "significant" to "critical" to better capture the intended purpose of reporting an incident. Additionally, the term "significant" is more subjective while the definition for "critical" is not. Critical is defined as "having the potential to become disastrous," or "at the point of crisis."

Mitigation strategies.
The Agencies provide a non-exhaustive list of events that the Agencies consider ''notification incidents''. ICBA contends that if there are mitigation strategies in place that offset the impact to a bank or its customers, the incident does not then represent a significant or critical incident and therefore is not a notification incident. ICBA strongly recommends that the Agencies include provisions that recognize the positive impact of mitigation strategies.

An incident may have a high inherent risk and impact, but with mitigation strategies in place often the residual risk and impact is much lower to both the bank and its customers. In the non-

[6] The definition of Cybersecurity Incident can be found at https://csrc.nist.gov/glossary/term/Cybersecurity_Incident
Source(s): NIST Cybersecurity Framework Version 1.1 and NIST Privacy Framework Version 1.0

exhaustive list of events, the Agencies, as an example, indicate that large-scale distributed denial of service ("DDOS") attacks, that disrupt customer account access for an extended period (e.g., more than 4 hours), would be a "notification incident." ICBA contends that there are many situations where a DDOS attack, such as this might not represent a significant or critical incident or outage and would not have a significant impact on the bank or its customers. For example, online banking is typically the primary target of DDOS attacks. While this might cause an outage to online banking, there are other channels where access to that data and services would remain. Those include mobile banking, text banking, phone banking, drive-thru, and in person visits to bank branches and offices, to name a few. In this very common example, a 4-hour DDOS attack to online banking, where the bank uses mitigation strategies, would not represent a "notification incident."

Duration of incident.
The non-exhaustive list of events that are considered ''notification incidents'', in most cases does not include a time-period for the event. While many of the notification incidents listed in the proposal would be significant or critical, and impactful to a community bank or its customers, providing a duration for the outage would assist in evaluating the criticality of the incident. ICBA recommends that the Agencies indicate that an outage less than 48-hours in duration does not represent a "notification incident."

As examples, a failed system upgrade or a ransomware event that is resolved and recoverable within a short period of time would not be impactful to the bank or its customers. In many situations, community banks have mitigation strategies in place to provide services and access to data within a 48-hour outage period, reducing the impact of the outage so that it does not rise to a significant or critical incident within 48-hours.

Notification period.
The proposed rulemaking would require a bank to notify its regulator as soon as possible and no later than 36-hours after it has determined that a notification incident has occurred. ICBA strongly believes that the 36-hour notification time period is an exceptionally short time period given a bank would likely be going through the process of evaluating and potentially responding to the incident. Smaller community banks will likely still be evaluating the severity of an incident within the first 36-hours since they typically rely on vendors and their core providers for incident response. This process may take longer than 36-hours to determine if it is a notifiable incident. ICBA urges that the notification timeframe be extended to a minimum of five business days for community banks under $20 billion in assets. This would provide banks adequate time to work with vendors and their core processors to provide accurate notifications.

Impact to banks.
To determine the regulatory burden associated with this proposal would have on banks, the Agencies identified the number of notification incidents expected to be reported annually by reviewing the available supervisory data and SARs involving cyber events against banking organizations. The agencies believe that the regulatory burden would be de minimis.

ICBA contends that the proposed cost estimates are significantly understated. More information and data needs to be collected and analyzed for a more accurate assessment of the regulatory impact of this proposal. ICBA urges the Agencies to seek additional comments on the estimated costs and benefits of the proposed rule.

For example, the Agencies based their estimate on reported SARs. Incidents, such as those involving no criminal activity or criminal intent, are not reported on a SAR. Examples of outages not reported through SARs includes an outage caused by a bank employee that executes a poorly written database query which takes down systems or significantly degrades performance. Additionally, outages caused by failed upgrades or server hardware failures, would not be reported on a SAR. The number of notification incidents would be significantly higher than estimated by the Agencies. ICBA urges the Agencies to seek additional comments on the estimated costs and benefits of the proposed rule. Collecting data from broader data sets would provide the Agencies with a more accurate estimate of compliance costs.

Agency receipt procedures.
The Agencies proposal would require banks to notify their regulator after a notification incident has occurred. ICBA suggests that each agency designate a centralized office to receive bank incident notifications and provide contact information for that designated office and personnel. Additionally, a single Agency notification should be deemed sufficient if there is a dual Agency notification requirement. ICBA urges the Agencies to develop procedures, with notice and opportunity for comment, that will be taken upon receipt of the bank's incident notification information and any subsequently gathered information related to the incident. ICBA respectfully suggests that the Agencies' shared procedures should address, among other things, the following:

(i) How the Agencies will notify the bank of receipt of the bank's incident notification.
(ii) How the incident notification information, once provided by a bank, will be shared between regulatory agencies and OCCIP.
(iii) How the incident notification information, once provided by a bank, will be consolidated and shared with the notifying bank to improve a bank's incident response or the sector's incident response capability.
(iv) How the incident notification information, once provided by a bank, will be protected and secured by the regulatory agencies.

(v) What services and supports the regulatory agencies will provide to banks who have notified their regulator of a "notification incident."

Bank service providers.
The proposal would require a bank service provider to notify at least two individuals at an affected bank immediately after experiencing a computer-security incident. A bank service provider is a company that provides services as described in the Bank Services Company Act.[7] The definition of "bank service provider" should be clarified to include all significant financial sector and third-party service providers within the Agencies' authority that have access to bank customer information, bank systems, or provide banking systems or services. ICBA recommends that "bank service provider" be defined similarly to the definition of "technology service provider," which is:

> Technology service providers encompass a broad range of entities including, but not limited to affiliated entities, nonaffiliated entities, and alliances of companies providing products and services. This may include but is not limited to core processing; information and transaction processing and settlement activities that support banking functions such as lending, deposit-taking, funds transfer, fiduciary, or trading activities; internet-related services; security monitoring; systems development and maintenance; aggregation services; digital certification services, and call centers. Other terms used to describe service providers include vendors, subcontractors, external service provider ("ESPs") and outsourcers.[8]

Third-party service provider notifications.
The Agencies are seeking feedback on how service providers notify banks of service disruptions under existing contracts. Experiences vary greatly between various types of service disruptions and service providers.

Very often, core or third-party service providers do not initiate a notification to banks regarding an outage or degraded service. Rather, the core or third-party service provider provides information on an outage or degraded service, after a bank requests such information.

Sometimes, however, community banks may receive an initial notification of an outage from a core or third-party service provider within one to 24-hours of the outage's occurrence.

[7] 12 USC 1861-1867(c).
[8] FDIC Financial Institution Letters, Effective Practices for Selecting a Service Provider, 2014.

However, additional information regarding the outage is generally not as forthcoming. Disruptions, such as degraded service, may not generate a notification at all from the service provider since a degraded service is often not seen as an outage by the service provider. Degraded service is an area often poorly defined in contracts and service level agreements. Additionally, many core or third-party service provider contracts do not specify what constitutes a notifiable event. Therefore, notices are provided based on each third-party service providers' internal policies and procedures.

The Agencies are also seeking comment on a proposed requirement for bank service providers to notify at least two individuals at an affected bank after an outage. ICBA supports this provision and suggests that a third notification be sent to a bank's general email or telephone number, so that in cases where individual bank staff are not available, the notification is logged.

Third-party service provider contracts.
The Agencies are seeking comment on whether existing contracts between banking organizations and bank service providers already have provisions that would allow banking organizations to meet the proposed notification incident requirements? There are existing contracts between banks and third-party service providers, and it is unlikely that existing contracts would include provisions to address the proposed provisions.

Community banks have very little negotiating power with their core and third-party service providers for specific provisions in contracts. Often when a vendor is asked to make a modification to the provisions of a contract, community banks are told that it is standard contractual language, and the request is rejected. To assist banks, ICBA asks that the Agencies work with all stakeholders, including core and third-party service providers, to determine appropriate contractual provisions to ensure that community banks and third-party service providers can comply with any new requirements.

ICBA also recommends that during Federal Financial Institutions Examination Council ("FFIEC") examinations of core and third-party service providers, examiners review standard contracts to ensure specific provisions for complying with these requirements are included. Additionally, often contracts are three, five or seven years in duration. In these instances, ICBA would ask that the Agencies extend the compliance date for a minimum of three years or the length of an existing contract, whichever is greater.

Conclusion

ICBA asks the Agencies carefully consider these comments and address our concerns as they consider rules which would impact how community banks provide incident information to the

Agencies and how core and third-party service providers provide incident and outage information to community banks.

ICBA appreciates the opportunity to provide comments in response to this request. If you have any questions, please do not hesitate to contact me at Joel.Williquette@icba.org or (202) 821-4454.

Sincerely,

/s/

Joel Williquette
Senior Vice President, Operational Risk Policy