Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990 Division of Risk Management Supervision

MEMORANDUM TO: Board of Directors

FROM: Doreen R. Eberley
Director, Division of Risk Management Supervision

SUBJECT: Computer-Security Incident Notification Requirements for Banking Organizations and Their Service Providers

SUMMARY

The Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (FRB), and the Office of the Comptroller of the Currency (OCC) (collectively, "the agencies"), have drafted a proposed rule that would require banking organizations (generally, insured depository institutions) to promptly notify their primary federal regulator whenever they experience a computer-security incident that they believe in good faith could materially disrupt, degrade, or impair their operations or may threaten the financial stability of the United States. Such occurrences are defined in the proposed rule as notification incidents. Additionally, a bank service provider, as described in the Bank Service Company Act (BSCA), would be required to notify at least two individuals at affected banking organization customers immediately after it experiences a computer-security incident that the bank service provider believes in good faith could disrupt, degrade, or impair services provided subject to the BSCA for four or more hours.

A severe computer security incident may impair the ability of banking organizations to provide financial services to their customers for an extended period of time, or even threaten the viability of the institutions. There is, however, no federal requirement that banking organizations promptly notify regulators of such incidents. Currently, a banking organization is expected to notify its primary federal regulator of a computer-security incident when the incident involves unauthorized access to sensitive customer information,[1] but timing is variable. Furthermore, although many incidents will be reported under part 353 of the FDIC's rules and regulations concerning Suspicious Activity Reports, part 353 does not require the filing of a Suspicious Activity Report until up to 60 calendar days after the suspicious activity is identified. From an analysis of suspicious activity reports, staff believes that very few computer security incidents at the severity level identified in the proposed rule typically occur.

Accordingly, staff recommends that the Board of Directors (Board) authorize for publication in the *Federal Register* the attached notice of proposed rulemaking to amend 12 C.F.R. part 304.

Concur:

Nicholas J. Podsiadly
General Counsel

[1] *See* 12 C.F.R. § 364 app'x B, supp. A (FDIC) ("Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice").

BACKGROUND

Federal banking regulators have observed an increase in frequency and severity of malicious cyberattacks, as highlighted in a recent *Joint Statement on Heightened Cybersecurity Risk* (January 16, 2020), issued by the FDIC and the OCC.[2] Such cyberattacks often involve the targeted criminal use of destructive malware to exploit weaknesses in the computers or networks of a banking organization or bank service provider. These incidents have the potential to alter, delete, or otherwise render a banking organization's data and systems unusable. Depending on the scope of the incident, a banking organization's backup data may also be impacted, which can severely impair the banking organization's ability to recover operations. These incidents can result in customers being unable to access their deposits and other accounts. In rare instances, a significant computer-security incident may jeopardize the viability of a banking organization. From an analysis of suspicious activity reports, staff believes that very few computer security incidents at the severity level identified in the proposed rule typically occur.[3]

Knowing about and responding to significant computer-security incidents at banking organizations is important to banking regulators' missions. Federal banking agencies wish to gather timely computer-security incident information for a variety of reasons, including:

- The receipt of computer-security incident information may give the agencies earlier awareness of emerging threats to individual banking organizations and, potentially, to the broader financial system;

- An incident may so severely impact a banking organization that it can no longer support its customers, and the incident could impact the safety and soundness of the banking organization, leading to its failure. In these cases, the sooner the agencies know of the event, the better they can assess the extent of the threat and take appropriate action;

- Based on the agencies' broad supervisory experiences, they may be able to provide information to a banking organization that may not have previously faced a particular type of computer-security incident;

- The agencies would be better able to conduct analyses across supervised banking organizations to improve guidance, adjust supervisory programs, and provide information to the industry to help banking organizations protect themselves; and

- Receiving notice would enable the primary federal regulator to facilitate and approve requests from banking organizations for assistance through the U.S. Treasury Office of Cybersecurity and Critical Infrastructure Protection.

[2] Available at https://www.fdic.gov/news/financial-institution-letters/2020/fil20003.html.

[3] The agencies reviewed available supervisory data and SARs involving cyber events against banking organizations to develop an estimate of the number of notification incidents expected to be reported annually. This review focused on descriptive criteria (e.g., ransomware, trojan, and zero day) that may be indicative of the type of material computer-security incident that would meet the notification incident reporting criteria. Based on this review, the agencies estimate that approximately 150 notification incidents may occur on an annual basis.

EXISTING REPORTING REQUIREMENTS

Financial institutions that have experienced a malicious computer-security incident are required to file a Suspicious Activity Report (SAR) for activity that might signal criminal actions (e.g., money laundering, tax evasion, and computer crime). Under the reporting requirements of the Bank Secrecy Act (BSA) and its implementing regulations, financial institutions are required to file SARs within 30 days of detecting a reportable suspicious transaction (with an additional 30 calendar days provided in certain circumstances). As a result, the information from SARs is not timely enough for the agencies to provide support to a financial institution, or more broadly to allow the agencies to identify emergent risks that may become a challenge for the financial sector more broadly.

Additionally, the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, which interprets section 501(b) of the Gramm-Leach-Bliley Act (GLBA),[4] provides that financial institutions notify their primary federal regulator "*as soon as possible*" when an institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information.[5] While this provides for prompt federal regulator notice of certain computer-security incidents, this requirement is narrow in scope and does not capture serious operational incidents that do not involve compromised customer information. Specifically, the GLBA notice requirement does not reach highly disruptive incidents in which sensitive customer information was not, or does not appear to have been compromised. Further, if the institution is uncertain whether sensitive customer information has been compromised, regulator notification could be delayed.

Earlier notification would allow the agencies to assess the severity and spread of disruptive incidents. The agencies could then take appropriate actions, including alerting other banking organizations, consulting with other regulatory and law enforcement agencies, and assisting in coordinating a response. These actions could mitigate the impact of the incident and help preserve the safety and soundness of the financial industry.

THE PROPOSAL

The proposal would establish a new subpart C in part 304 of the FDIC's regulations (12 C.F.R. §§ 304.21–304.24) titled "Computer-Security Incident Notification." The FRB and the OCC would promulgate similar rules. The proposed rule would establish two primary requirements.

First, banking organizations would be required to notify their primary federal regulator within 36 hours of when they believe in good faith that a "computer-security incident" that rises to the level of a "notification incident" has occurred. The term "computer-security incident" is based

[4] See Pub. L. No. 106-102, § 501, 113 Stat. 1436 (1999) (codified at 15 U.S.C. § 6801).
[5] *See* 12 C.F.R. § 364 app'x B, supp. A.

on relevant terminology from the National Institute of Standards and Technology.[6] "Notification incident" in turn narrows reportable computer-security incidents to the following[7]:

> *a computer-security incident that a banking organization believes in good faith 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.*

Second, a bank service provider, as described in the BSCA, would be required to notify at least two individuals at affected banking organization customers immediately after the bank service provider experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair services provided subject to the BSCA for four or more hours.

The proposed notification requirement for banking organizations is intended to serve as an early alert to a banking organization's primary federal regulator about a notification incident, and is not intended to require comprehensive or elaborate reporting. The agencies recognize that a banking organization may be working expeditiously to resolve the notification incident—either directly or through their bank service provider—at the time they would be required to notify their primary federal regulator. The agencies believe, however, that 36 hours is a reasonable amount of time following a determination by a banking organization that it believes in good faith a notification incident has occurred for a banking organization to notify, particularly because the notification would not need to include a comprehensive assessment of the notification incident. Moreover, the notice could be provided through any form of electronic or oral communication, including through any technological means, to a designated point of contact identified by the FDIC. Staff analysis of proposed rule's impact on banking organizations and bank service providers concludes that there would be low impact because there are expected to be few notification incidents, and because banks currently notify regulators, and service providers their customers about such incidents, though later than is optimal for the purposes described herein.

---

[6] The proposed definition would be, "an occurrence that (i) results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information that 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."

[7] The definition of "notification incident" includes language that is consistent with the "core business line" and "critical operation" definitions included in the resolution-planning rule issued by the FRB and FDIC under section 165(d) of the Dodd-Frank Act. The agencies do not expect banking organizations that are not subject to the Resolution Planning Rule to identify "core business lines" or "critical operations," or to develop procedures to determine whether they engage in any operations the failure or discontinuance of which would pose a threat to the financial stability of the United States.

RECOMMENDATION

Staff requests that the FDIC Board approve this notice of proposed rulemaking, and authorize its publication in the *Federal Register* with a comment period deadline of 90 days after the date of *Federal Register* publication.

STAFF CONTACTS

RMS Operational Risk:		Legal:	
Martin Henning	(202) 898-3699	John Dorsey	(202) 898-3807
Rob Drozdowski	(202) 898-3971	Graham Rehrig	(202) 898-3829