# The Banking Law Journal

Established 1889

An A.S. Pratt™ PUBLICATION

JUNE 2021





LexisNexis

# THE BANKING LAW JOURNAL

**VOLUME 138** **NUMBER 6** **June 2021**



LexisNexis®

## QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call:

Matthew T. Burke at ..... (800) 252-9257
Email: ..... matthew.t.burke@lexisnexis.com
Outside the United States and Canada, please call . . . . . (973) 820-2000

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3385
Fax Number . . . . . (800) 828-8341
Customer Service Website . . . . . http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call

Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (937) 247-0293

ISBN: 978-0-7698-7878-2 (print)
ISSN: 0005-5506 (Print)

Cite this publication as:

The Banking Law Journal (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.



Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

(2021–Pub.4815)

# *Editor-in-Chief, Editor & Board of Editors*

THE BANKING LAW JOURNAL (ISBN 978-0-76987-878-2) (USPS 003-160) is published ten times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices.  For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to bankers, officers of financial institutions, and their attorneys. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, LexisNexis Matthew Bender, 230 Park Ave, 7th Floor, New York, NY 10169.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, A.S. Pratt & Sons, 805 Fifteenth Street, NW, Third Floor, Washington, DC 20005-2207.

# Banks May Face New Computer-Security Incident Notification Requirements

***Michael J. Heller****

*Federal bank regulators have proposed a rule that would require banks—including community banks and state banks insured by the Federal Deposit Insurance Corporation—to provide their federal regulators with "prompt notification" of specified "computer-security incidents."*

Cyberattacks against banks and against other businesses have increased in frequency and severity in recent years.[1] These types of attacks may use destructive malware or other malicious software to target weaknesses in banks' computers or networks. Some cyberattacks even may be able 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 also may be affected, which can severely affect the ability of the bank to recover operations.

Currently, a bank may be required to report certain instances of disruptive cyber-events and cyber-crimes through the filing of suspicious activity reports ("SARs") and generally must notify its federal regulator "as soon as possible" when it becomes "aware" of an incident involving unauthorized access to or use of sensitive customer information. Those general requirements may soon change into something much more demanding.

## THE PROPOSED RULE—IN GENERAL

The Office of the Comptroller of the Currency ("OCC"), Board of Governors of the Federal Reserve System ("Board"), and the Federal Deposit Insurance Corporation ("FDIC") (collectively, the "agencies") have issued a proposed rule that would require a bank to notify its federal regulator when it

---

* Michael J. Heller, a member of the Banking, Corporate, and Real Estate Practice Groups at Rivkin Radler LLP and a member of the Board of Editors of *The Banking Law Journal*, works extensively with bank clients on complex commercial loans, including Industrial Development Agency and Small Business Administration matters, and with private clients in real estate development and corporate transactions. He may be reached at michael.heller@rivkin.com.

[1] *See* Federal Bureau of Investigation, Internet Crime Complaint Center, "2020 Internet Crime Report," *available at* https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

believes in good faith that a significant "computer-security incident"[2] has occurred.[3]

The proposed rule would require notification as soon as possible, but no later than 36 hours after the bank believes in good faith that an incident had taken place.

Moreover, a bank service provider would be required to notify at least two individuals at an affected bank immediately after the bank service provider experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair services provided by the bank service provider for four or more hours.

The agencies' proposed rule makes clear that where a bank experiences a computer-security incident that may be criminal in nature, the agencies expect that the bank will contact relevant law enforcement or security agencies, as appropriate, after the incident occurs.

## PURPOSE OF THE PROPOSED RULE

The agencies state that the notification requirement in their proposed rule is intended to serve as an early alert to a bank's federal regulator and is not intended to provide an assessment of the incident.

Among other things, the agencies said that they believe that this notice could give the agencies earlier awareness of emerging threats to individual banking organizations and, potentially, to the broader financial system.

## PRIMARY REQUIREMENTS OF THE PROPOSED RULE

The proposed rule would establish two primary requirements, which the agencies said they believe would promote the safety and soundness of banking organizations and would be consistent with the agencies' authority to supervise these entities.

---

[2] As defined by the proposed rule, a "computer-security incident" is an occurrence that 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 that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. To promote uniformity of terms, the agencies said that they have sought to align this term to the fullest extent possible with an existing definition from the National Institute of Standards and Technology ("NIST"). *See* NIST, Computer Security Resource Center, "Glossary," *available at* https://csrc.nist.gov/glossary/term/dictionary.

[3] *See* www.fdic.gov/news/board/2020/2020-12-15-notice-sum-c-fr.pdf.

First, the proposed rule would require a banking organization to notify the agencies of a "notification incident."

In particular, a banking organization would be required to notify its 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 banking organization believes in good faith that a notification incident has occurred. The agencies state in the proposed rule that they do not expect that a banking organization would typically be able to determine that a notification incident has occurred immediately upon becoming aware of a computer-security incident. Rather, the agencies said that they anticipate that a banking organization would take a reasonable amount of time to determine that it has experienced a notification incident.

In this context, the agencies said that they recognize that banking organizations may not come to a good faith belief that a notification incident has occurred outside of normal business hours. As provided by the proposed rule, only once a banking organization has made such a determination would the requirement to report within 36 hours begin.

The proposed rule would apply to the following banking organizations:

- For the OCC, "banking organizations" would include national banks, federal savings associations, and federal branches and agencies;
- For the Board, "banking organizations" would include all U.S. bank holding companies and savings and loan holding companies, state member banks, and the U.S. operations of foreign banking organizations; and
- For the FDIC, "banking organizations" would include all insured state nonmember banks, insured state-licensed branches of foreign banks, and state savings associations.

Second, the proposed rule would require a bank service provider of a service described under the Bank Service Company Act ("BSCA")[4] to notify at least two individuals at an affected banking organization customer immediately after experiencing a computer-security incident that the bank service provider

[4] Bank services that are subject to the BSCA include "check and deposit sorting and posting, computation and posting of interest and other credits and charges, preparation and mailing of checks, statements, notices, and similar items, or any other clerical, bookkeeping, accounting, statistical, or similar functions performed for a depository institution," as well as components that underlie these activities. *See* 12 U.S.C. 1863–64. Other services that are subject to the BSCA include data processing, back office services, and activities related to credit extensions, as well as components that underlie these activities. *See* 12 U.S.C. 1864(f).

believes in good faith could disrupt, degrade, or impair services provided subject to the BSCA for four or more hours.

The agencies explained that, as technological developments have increased in pace, banks have become increasingly reliant on bank service providers to provide essential technology-related products and services. According to the agencies, the impact of computer-security incidents at bank service providers can flow through to their banking organization customers. Therefore, in order for a banking organization to be able to provide relevant notifications to its federal regulator in a timely manner, the agencies said that they believe that the banking organization needs to receive prompt notification of computer-security incidents from its service providers.

## WHEN WOULD NOTIFICATION BE REQUIRED?

The proposed rule makes clear that not every "computer-security incident" would require a banking organization to notify its federal regulator; only those that rise to the level of a "notification incident" would require notification. Other computer-security incidents, such as a limited distributed denial of service attack that is promptly and successfully managed by a banking organization, would not require notice to the appropriate agency.

The proposed rule contains the following non-exhaustive list of events that would be considered a "notification incident" and, therefore, that would require notification:

- Large-scale distributed denial of service attacks that disrupt customer account access for an extended period of time (for example, more than four hours);
- A bank service provider that is used by a banking organization for its core banking platform to operate business applications is experiencing widespread system outages and recovery time is undeterminable;
- A failed system upgrade or change that results in widespread user outages for customers and bank employees;
- An unrecoverable system failure that results in activation of a banking organization's business continuity or disaster recovery plan;
- A computer hacking incident that disables banking operations for an extended period of time;
- Malware propagating on a banking organization's network that requires the banking organization to disengage all internet-based network connections; and

- A ransom malware attack that encrypts a core banking system or backup data.

## THE NOTICE

Interestingly, the proposed rule states that the proposed notification requirement is intended to serve as an early alert to a banking organization's federal regulator about a notification incident and is not intended to include an assessment of the incident. As such, no specific information is required for the notice, and the proposed rule does not include any prescribed reporting forms or templates that might help minimize the reporting burden.

The agencies said that they recognize that a banking organization may be working expeditiously to resolve the notification incident—either directly or through a bank service provider—at the time it would be expected to notify its federal regulator. The agencies added, however, that they believe that 36 hours is a reasonable amount of time after a banking organization believes in good faith that a notification incident has occurred to notify its federal regulator, particularly because the notice would not need to include an assessment of the incident.

Moreover, the agencies said that they expect only that banking organizations would share general information about what is known at the time.

Under the proposed rule, the notice could be provided through any form of written or oral communication, including through any technological means (e.g., email or telephone), to a designated point of contact identified by the banking organization's federal regulator (e.g., an examiner-in-charge, local supervisory office, or a cyber-incident operations center). The notification, and any information provided by a banking organization related to the incident, would be subject to the agencies' confidentiality rules, according to the agencies.

Under the proposed rule, a bank service provider would be required to notify at least two individuals at affected banking organization customers immediately after it 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.

Importantly, the proposed rule indicates that a bank service provider would not be expected to assess whether the incident rises to the level of a notification incident for a banking organization customer—the banking organization would be responsible for making that determination because a bank service provider may not know if the services provided are critical to the banking organization's operations. If, after receiving such notice from a bank service provider, the

banking organization determines that a notification incident has occurred, the banking organization would be required to notify its federal regulator in accordance with the proposed rule.

Under the proposal, bank service providers would be expected to continue to provide a banking organization customer with prompt notification of these material incidents. The agencies said that they believe that it is practical for a bank service provider to immediately notify at least two individuals at their affected banking organization customers after experiencing a computer-security incident of the severity described in the proposed rule because the notice would not need to include an assessment of the incident, and the agencies observed that there are effective automated systems for currently doing so. The agencies added that bank service providers would be expected to make a best effort to share general information about what is known at the time.

Additionally, the proposed rule provides that regulators would enforce the bank service provider notification requirement directly against bank service providers and would not cite a banking organization because a service provider fails to comply with the service provider notification requirement.

## PERCEIVED BENEFITS OF THE PROPOSED RULE

In the proposed rule, the agencies cite a number of benefits that they believe would accrue to banking organizations and the financial industry as a whole under their proposal.

For one thing, according to the agencies, notification may assist the agencies in determining whether an incident is isolated or is one of many simultaneous identical or similar incidents at multiple banking organizations. If a notification incident is isolated to a single banking organization, the federal regulator may be able to facilitate requests for assistance to the affected organization, arranged by the U.S. Treasury Office of Cybersecurity and Critical Infrastructure Protection ("OCCIP"), to minimize the impact of the incident. In the agencies' opinion, this benefit may be greatest for small banking organizations with more limited computer security resources.

If the notification incident is one of many simultaneous identical or similar incidents at multiple banking organizations, the agencies said that they also may alert other banking organizations of the threat, as appropriate, while protecting confidential supervisory information, recommend preventative measures in order to better manage or prevent reoccurrence of similar incidents, or otherwise help coordinate the response and mitigation efforts. In the agencies' view, receiving notification incident information from multiple banking organizations also would allow regulators to conduct analyses across entities to

improve guidance, to adjust supervisory programs to limit the reoccurrence of such incidents in the future, and to provide information to the industry to help banking organizations protect themselves against future computer-security incidents.

Another benefit perceived by the agencies is that the proposed rule may help reduce losses in the event a notification incident is so significant that it jeopardizes a banking organization's viability, as the proposal would provide additional time for the agencies to prepare to handle a potential failure as cost-effectively and non-disruptively as possible.

The agencies conceded that they do not have the information to quantify the potential benefits of the proposed rule because the benefits depend on the breadth and severity of future notification incidents, the specifics of those incidents, and the value of the assistance approved by the agencies, among other things. Nevertheless, the agencies indicated that they believe that the benefits of the proposed rule would exceed the costs—which the agencies said they believe would be "*de minimis*" for both banking organizations and bank service providers.

It is worth noting that the agencies estimate in the proposed rule that, upon occurrence of a notification incident, an affected banking organization might incur up to three hours of staff time to coordinate internal communications, consult with its bank service provider, if appropriate, and notify the banking organization's federal regulator. The agencies explained that this may include discussion of the incident among staff of the banking organization, such as the chief information officer, chief information security officer, a senior legal or compliance officer, and staff of a bank service provider, and liaison with senior management of the banking organization.

The agencies estimate the same amount of time would be necessary for a bank service provider to comply with the notification requirement, anticipating that a provider would need approximately one hour to determine that a computer-security incident meets the notification criteria and two hours to identify the customers affected by the service disruption and provide notification that an incident has occurred.

## CONCLUSION

The proposed rule has not yet been finalized and changes certainly are possible. Among other things, it is conceivable that the definition of "computer-security incident" might be modified, perhaps to include only occurrences that result in actual harm to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits.

The final rule also might alter the definition in the proposed rule of "notification incident," the 36 hour timeframe for notification could be made longer or perhaps even shorter, and the notification required by the proposed rule might expand to require a joint notification to all of the agencies.

It also is worth noting that some states already have their own reporting requirements, such as the 72 hour deadline imposed by the New York State Department of Financial Services for a cybersecurity incident; many reporting requirements are tied specifically to customer data breaches.

Nevertheless, one thing is clear: Banks (and their service providers) should become familiar with the proposed rule and begin high level discussions, including with counsel, about complying with it before it becomes final.