THE REVIEW OF
BANKING & FINANCIAL SERVICES
A PERIODIC REVIEW OF SPECIAL LEGAL DEVELOPMENTS AFFECTING LENDING AND OTHER FINANCIAL INSTITUTIONS

Vol. 38 No. 5 May 2022

THE BANKING AGENCIES' FINAL RULE ON COMPUTER-SECURITY INCIDENT NOTIFICATION REQUIREMENTS

Responding to the increasing frequency and severity of cyberattacks on the financial services industry, the federal banking agencies have issued a final rule regarding required notifications of such attacks. The authors discuss the rule in detail, beginning with the Agencies' stated goals and key definitions in the rule. They then turn to updating incident response plans for compliance, incident notification requirements, and issues surrounding service provider contacts and contracts.

By Avi Gesser, Johanna Skrzypczyk, Michael R. Roberts, Courtney Bradford Pike, and Andres Gutierrez *

On November 18, 2021, the Federal Deposit Insurance Corporation ("FDIC"), the Office of the Comptroller of the Currency ("OCC"), and the Federal Reserve Board ("FRB" or "the Board") (collectively, "the Agencies") announced the approval of a final rule that imposes new requirements on banking organizations and bank service providers for certain cybersecurity incidents. The Agencies issued the *Final Rule on Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers* ("Final Rule"), which went into effect on April 1, 2022 and requires banking organizations, as well as certain banking service providers, to comply by May 1, 2022. Importantly, on March 29, 2022, the Agencies each issued guidance to their supervisory institutions regarding logistics for notification.

This article discusses three key components of the Final Rule, specifically: (1) new considerations and requirements for notifiable computer-security incidents; (2) steps to take to update incident response plans ("IRPs"); and (3) issues to consider when reviewing service provider relationships, including relevant contacts and contractual obligations. The Final Rule offers an opportunity for banking organizations to refine and formalize their processes and communications regarding computer-security incidents.

IMPORTANT DEFINITIONS AND GOALS

The Agencies' Goals and Considerations

The Agencies explained that they issued the Final Rule due to the increasing frequency and severity of cyberattacks in the financial services industry. Cyberattacks can harm banking organizations' networks, data, and systems, and impair their ability to carry out normal operations, such as providing customers access to their accounts. Some of the existing notification requirements, according to the Agencies, were not

* *AVI GESSER is a partner, JOHANNA SKRZYPCZYK is counsel, and MICHAEL R. ROBERTS, COURTNEY BRADFORD PIKE, and ANDRES GUTIERREZ are associates at Debevoise & Plimpton LLP's New York City office. Their e-mail addresses are agesser@debevoise.com, jnskrzypczyk@debevoise.com, mrroberts@debevoise.com, cbpike@debevoise.com, and asgutierrez@debevoise.com.*

INSIDE THIS ISSUE

- ***LITIGATION TRUST CLAIMS: CONFIRMATION AND INVESTIGATION PITFALLS, Page 43***

RSCR Publications LLC Published 12 times a year by RSCR Publications LLC. Executive and Editorial Offices, 2628 Broadway, Suite 29A, New York, NY 10025-5055. Subscription rates: $650 per year in U.S., Canada, and Mexico; $695 elsewhere (air mail delivered). A 15% discount is available for qualified academic libraries and full-time teachers. For subscription information and customer service call 609-683-4450; fax 609-683-7291; write Subscriber Services, RSCR Publications, PO Box 585, Kingston NJ 08528; e-mail cri.customer.service@comcast.net; or visit our website at www.rscrpubs.com. General Editor: Michael O. Finkelstein; tel. 212-876-1715; e-mail mofinkelstein@gmail.com. Associate Editor: Sarah Strauss Himmelfarb; tel. 301-294-6233; e-mail sarah.s.himmelfarb@gmail.com. To submit a manuscript for publication contact Ms. Himmelfarb. ISSN: 1051-1741.

comprehensive enough and resulted in some untimely notifications. The Agencies also noted that they anticipate that the Final Rule will allow banking organizations and bank service providers time to assess incidents before making notifications, which will reduce notification of less material incidents and ensure that regulators are still receiving alerts as early as possible.

The Agencies explained that they anticipate that the 36-hour notice requirement (described *infra*), which is viewed as the most onerous part of the Final Rule, will make sense in light of the simplicity of the notification required and the severity of the incidents that would require notification. Additionally, the Agencies believe that the 36-hour notice requirement provides additional benefits, including:

- promoting early awareness of emerging threats to banking organizations and the broader financial system that helps the Agencies react to these threats before they become systemic;

- enabling prompt notification of reportable incidents: if the notification incident is isolated to a single banking organization, helping the Agencies to facilitate requests for assistance on behalf of the affected organization to minimize the impact of the incident, which could prove helpful for small banking organizations with more limited resources; and for a notification incident that is one of many similar incidents occurring at multiple banking organizations, helping the Agencies to also alert other banking organizations of the threat, recommended measures to better manage or prevent the recurrence of similar incidents, or otherwise help coordinate incident response;

- helping facilitate prompt notifications about incidents, which could enable the Agencies to respond faster to potential liquidity events that may result from such incidents, allowing a faster regulator response that could mitigate, or entirely prevent, these adverse liquidity events, thereby enhancing the resilience of the banking system against notification incidents;

- allowing the Agencies to facilitate and approve requests from banking organizations for assistance through the U.S. Treasury Office of Cybersecurity and Critical Infrastructure Protection; and

- enabling the Agencies to receive information on notification incidents at multiple banking organizations and help enable the Agencies to conduct empirical analyses to improve related guidance, adjust supervisory programs to enhance resilience against such incidents, and provide information to the industry to help banking organizations reduce the risk of future computer-security incidents.

Key Definitions Under the Final Rule

Banking Organizations and Bank Service Providers. The Agencies each define "banking organizations,"[1] based on their regulatory purview and, importantly, each exclude designated financial market utilities ("FMUs") from their respective definitions.[2]

---

[1] The OCC defines a banking organization as, "a national bank, Federal savings association, or Federal branch or agency of a foreign bank." Final Rule, 86 Fed. Reg. 66424, 66442 (Nov. 23, 2021), https://www.govinfo.gov/content/pkg/FR-2021-11-23/pdf/2021-25510.pdf. The FRB defines a banking organization as, "a U.S. bank holding company; U.S. savings and loan holding company; state member bank; the U.S. operations of foreign banking organizations; and an Edge or agreement corporation." *Id.* at 66443. The FDIC defines a banking organization as, "an FDIC-supervised insured depository institution, including all insured state nonmember banks, insured state-licensed branches of foreign banks, and insured State savings associations." *Id.* at 66444.

[2] An FMU is "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)). The Final Rule defines "designated financial market utility" as having the same meaning as set forth at 12 U.S.C. § 5462(4), under which a "designated financial market utility" means a FMU that the Financial Stability Oversight Council ("FSOC") has designated as "systemically important" under section 804 (12 U.S.C. § 5463) of the Dodd-Frank Act. In determining whether a FMU is, or is likely to become, "systemically important," the FSOC is required by section 5463 to take into consideration the

Under the Final Rule, a "bank service provider"[3] does not include designated FMUs and is defined as a "bank service company or other person that performs covered services" subject to the Banking Service Company Act ("BSCA"). These "covered services" 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, which may include data processing, internet banking, or mobile banking services.[4]

However, the Agencies explained that FMUs that are not designated and meet the definition of "banking organization" or "bank service provider" are within the Final Rule's scope. The Agencies determined that excluding all FMUs would be overly broad and result in inconsistent regulatory treatment and possible confusion, as there is no defined list of FMUs, other than designated FMUs.

Computer-Security Incident. The Final Rule's definition of a "computer-security incident" intentionally deviates from the National Institute of Standards and Technology's ("NIST") standard definition in order to narrow the Final Rule's focus to incidents with the greatest chance of materially and adversely affecting banking organizations. The Final Rule defines a "computer-security incident" as an "occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits."

Notification Incident. The Final Rule's definition of a "notification incident" incorporates a standard that the Agencies explained will avoid having an overbroad Final Rule requiring notification for too many incidents, including those that were more speculative in nature than intended.[5] Moreover, the Final Rule's materiality standard also requires notification for all events that cause prolonged disruptions to customers' ability to access their accounts, whether the result of an accident or natural disaster or an intentional cyberattack. Despite the focus on actual damage, the notification requirement also covers incidents that are reasonably likely to cause material disruption or degradation, not only those that have already had those results. The Final Rule provides a non-exhaustive list[6] of examples of notification incidents, including:

- large-scale distributed denial of service attacks that disrupt customer account access for an extended period of time (e.g., 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 banking organization 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 on a banking organization's network that poses an imminent threat to the banking

footnote continued from the previous page…

following: (1) the aggregate monetary value of transactions processed by the FMU; (2) the aggregate exposure of the FMU to its counterparties; (3) the relationship, interdependencies, or other interactions of the FMU with other FMUs; (4) the effect that the failure of or a disruption to the FMU would have on critical markets, financial institutions, or the broader financial system; and (5) any other factors that the FSOC deems appropriate. 12 U.S.C. § 5463. The Agencies determined that excluding designated FMUs from the Final Rule is appropriate, as they are already subject to incident notification requirements in other federal regulations.

[3] The Final Rule defines a bank service provider as a "bank service company or other person that performs covered services." 86 Fed. Reg. 66424, 66428 (Nov. 23, 2021), https://www.govinfo.gov/content/pkg/FR-2021-11-23/pdf/2021-25510.pdf.

[4] 12 U.S.C. §§ 1861-1863.

[5] The Final Rule defines a notification incident as a "computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade a banking organization's (1) ability 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; (2) business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or (3) operations, 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." *Id.*

[6] *Id.* at 66431.

organization's core business lines or critical operations, or that requires the banking organization to disengage any compromised products or information systems that support the banking organization's core business lines or critical operations from Internet-based network connections; and

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

While these examples are helpful for providing a sense of the breadth of notifiable incidents, banking organizations are still required to evaluate situations individually to determine whether any significant computer-security incidents they experience qualify as notification incidents. The Agencies noted that if there is any uncertainty during this assessment, banking organizations should contact the appropriate regulator. The Agencies explained that they understand that banking organizations may at times, in an abundance of caution, provide an ultimately unnecessary notification based on a mistaken determination, and they do not expect to take supervisory action in those instances. In such an instance, there is not a formal rescission mechanism — banking organizations can simply provide an update to their original notification.

UPDATING INCIDENT RESPONSE PLANS FOR COMPLIANCE

Even with the flexibility of the 36-hour notification requirement and the benefits it will bring, compliance will require banking organizations to be able to move quickly to ensure that potential incidents are escalated to the appropriate individuals for assessment and, if needed, notification. Companies that are subject to the Final Rule purview should consider a few steps to prepare for it, as well as documenting those steps in an updated incident response plan.

First, banking organizations should determine whether they are, either in their entirety or in part, subject to the Final Rule. In some instances, only certain entities within an organization may fall within the Final Rule's scope. Banking organizations should also start mapping where they may also be bank service providers, even if only to their own affiliated entities. For those entities that fall within the Final Rule's scope, companies should assess which data, information systems, and employees are associated with the covered entities. Once that assessment is complete, companies can update their incident response plans to ensure that the covered entities have the appropriate procedures in place for compliance, including those described below.

Second, the 36-hour turnaround time will pass quickly during a significant computer-security incident, so it will be important for companies to prepare as much as possible. Companies should identify which of the Agencies is their primary regulator that they would need to notify and confirm that they have the appropriate Agency-recommended contact information, discussed below, for their primary regulator in the event of a notification incident. The incident response plan should contain this contact information to avoid a mid-emergency scramble.

In addition to knowing whom to notify, banking organizations need to confirm the person who will ultimately be responsible for making the notification to the appropriate Agency. There may also be a few individuals who have to approve the notification before it is made to ensure that any case-specific information is properly included. Companies should consider whether more than one person should be designated for each role in case someone is unavailable or unreachable during the incident. These people should be listed in updated incident response plans not only to avoid confusion during an incident, but also to ensure that incidents are promptly escalated to the proper individuals. These individuals and their teams at covered entities should be trained to be able to identify when to escalate incidents and to whom.

Finally, banking organizations should consider drafting a sample Agency notification. This sample notification may be included with the incident response plan. Along with the draft text, the template should also indicate to whom the notification is going and the individuals who have been designated as the notifiers. Having this template drafted will save time during an incident, as notifications will not have to be created from scratch. Companies should consider adjusting these processes and templates with the following lessons learned from tabletop exercises and experiences with actual incidents.

COMPUTER-SECURITY INCIDENT NOTIFICATION REQUIREMENTS

Banking Organization Requirements

The Final Rule requires banking organizations to notify the appropriate Agency point of contact about a "notification incident through e-mail, telephone, or other similar methods" the Agencies may prescribe.[7] The notification has to be received "as soon as possible and

[7] *Id.* at 66442, 66443, 66444.

no later than 36 hours after the banking organization determines that a notification incident has occurred."[8] The Agencies have said that they assumed that banking organizations can take the time they need to assess an incident to determine whether it meets the Final Rule's notification standard before notifying their regulator. Accordingly, the 36-hour timeline does not start until the banking organization has actually determined that a notification incident has occurred.

The notification does not have to include any specific information other than providing that a notification incident has occurred, as it is meant to serve as an early alert to the banking organization's primary federal regulator. There is no prescribed form or template for notifying the Agencies, though, as noted, it will be helpful for banking organizations to have their own template they can turn to during an incident. As mentioned, the notification requirements allow for flexibility; the Agencies noted that they anticipated that new technology may develop such that new methods of communication would be more practical and recognized that a communication channel may be impacted by an incident, so the Final Rule allows for multiple types of contact methods, as discussed below.

On March 29, the Agencies each issued guidance that provided instructions for banking organizations' compliance with the Final Rule's notification requirement, specifically regarding contact methods for notification incidents. Below we provide an overview of the key text of the guidance from the Agencies' releases, which apply to banking organizations and bank service providers regulated by the Final Rule.

FDIC, *Computer-Security Incident Notification Implementation*, Financial Institution Letter ("FIL") No. 12-2022 (Mar. 29, 2022)[9]

- FDIC-supervised banks can comply with the rule by notifying their case manager of an incident.
- FDIC-supervised banks can comply with the rule by notifying any member of an FDIC examination team if the event occurs during an examination.
- If a bank is unable to access its supervisory team contacts, the bank may notify the FDIC by e-mail at: incident@fdic.gov.

FRB, *Contact Information in Relation to Computer-Security Incident Notification Requirements*, Supervision and Regulation Letter 22-4 / Consumer Affairs Letter 22-3 (Mar. 29, 2022)[10]

- A banking organization whose primary regulator is the Board, must notify the Board about a notification incident by e-mail to incident@frb.gov or telephone at (866) 364-0096.
- The Board may identify other methods by which banking organizations may provide notice of cyber incidents in the future.
- If there is any doubt as to whether a notification incident occurs, a banking organization should provide notification via the above methods.
- If a bank service provider is in doubt as to whether a material disruption or degradation in services provided to a banking organization customer for four or more hours may have a material adverse impact on a banking organization customer, the Board encourages the bank service provider to contact the banking organization customer or its own legal adviser.
- The Board reiterated that the bank service provider notification requirement does not apply to any scheduled maintenance, testing, or software update previously communicated to a banking organization customer.

OCC, Information Technology: OCC Points of Contact for Banks' Computer-Security Incident Notifications, OCC Bulletin 2022-8 (Mar. 29, 2022)[11]

- A bank must notify the OCC after the bank determines that a notification incident has occurred,

[8] *Id.*

[9] The Federal Deposit Insurance Corporation, *Computer-Security Incident Notification Implementation*, Financial Institution Letter No. 12-2022 (Mar. 29, 2022) *available at* https://www.fdic.gov/news/financial-institution-letters/2022/fil22012.html#:~:text=On%20November%2023%2C%202021%2C%20the,notification%20requirements%20(Final%20Rule)%20for.

[10] The Board of Governors of the Federal Reserve System, *Contact Information in Relation to Computer-Security Incident Notification Requirements*, SA 22-4 / CA 22-3 (Mar. 29, 2022), *available at* https://www.federalreserve.gov/supervisionreg/srletters/SR2204.htm.

[11] Office of the Comptroller of the Currency, *Information Technology: OCC Points of Contact for Banks' Computer-Security Incident Notifications*, OCC Bulletin 2022-8 (Mar. 29, 2022) *available at* https://www.occ.treas.gov/news-issuances/bulletins/2022/bulletin-2022-8.html.

and the OCC must receive this notice as soon as possible and no later than 36 hours after the bank's determination.

- To satisfy the notification requirement, the bank may e-mail or call its supervisory office, submit a notification via the BankNet website, or contact the BankNet Help Desk starting on May 1, 2022.

- Banking organizations should register for BankNet well in advance of a notification incident.

- If there is any doubt as to whether a notification incident occurs, a banking organization should contact its supervisory office.

- If a bank service provider is unsure whether it has experienced a computer-security incident that meets this threshold, the OCC encourages the bank service provider to contact the affected banking organization customer(s) or the service provider's own legal counsel.

Bank Service Provider Requirements

The Final Rule requires bank service providers to "notify at least one bank-designated point of contact at each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours."[12]

The "bank-designated point of contact" can be an e-mail address, phone number, or other contact method that the banking organization has provided to the bank service provider. However, if that point of contact was not provided, the notification should be made to the Chief Executive Officer and Chief Information Officer of the banking organization customer, or two individuals of comparable responsibilities, through any reasonable means. It is also important to note that the notification requirement does not apply to any scheduled maintenance, testing, or software update previously communicated to a banking organization customer, unless the scheduled maintenance, testing, or software update exceeds the parameters communicated to the banking organization and meets the Final Rule's notification standard. Finally, the requirement only applies to affected customers, not all of the service provider's customers. This language minimizes the risk of confusion that could occur if a bank service provider had to notify all of their bank customers regardless of whether or not they were affected.

This notification is important because banking organizations have become increasingly dependent on their service providers for essential services. Like their customers, service providers are vulnerable to computer-security incidents, and providing timely notification is critical so incidents can be appropriately addressed quickly. That said, bank service providers are not required to assess whether an incident meets the notification incident standard for a banking organization, but they should make their best effort to share what is known with their customers. Much like the notification requirement for banking organizations, this standard also allows time for bank service providers to assess the nature of the incident before providing customers with notification. Thus, bank service providers will be able to provide more context and likely decrease the timeframe of their customers' assessments. Further, the Agencies will not "cite" the banking organization if a bank service provider fails to comply with the notification requirement. Both the OCC and the FRB suggest that if a bank service provider is in doubt as to whether a notifiable incident has occurred, they should contact the banking organization customer or its own legal adviser.[13]

SERVICE PROVIDER RELATIONSHIPS

Contacts

As noted, the Final Rule requires a bank service provider to notify "at least one bank-designated point of contact at each affected banking organization customer" after determining that it has experienced a notifiable computer-security incident. The Agencies explained that they expect that banking organizations and their service providers will work together to designate the methods of communications that work for both parties. To that end, the first step that banking organizations

[12] *Id.* at 66442, 66443, 66444.

[13] Office of the Comptroller of the Currency, *Information Technology: OCC Points of Contact for Banks' Computer-Security Incident Notifications*, OCC Bulletin 2022-8 (Mar. 29, 2022) *available at* https://www.occ.treas.gov/news-issuances/bulletins/2022/bulletin-2022-8.html; The Board of Governors of the Federal Reserve System, *Contact Information in Relation to Computer-Security Incident Notification Requirements*, SA 22-4 / CA 22-3 (Mar. 29, 2022), *available at* https://www.federalreserve.gov/supervisionreg/srletters/SR2204.htm.

should take is to identify which organizations are service providers under the Final Rule and provide that confirmation to them. From there, the parties should designate the appropriate points of contact for notification during an incident, which should include considering whether more than one person should be in that role in case someone is unavailable. The Agencies said that they expect the notification process will be best achieved if the parties work together to establish a communication method that is feasible all around and is designed to ensure the banking customer receives timely notice. Then, the parties should discuss updating their notification procedures to ensure compliance with the Final Rule.

Contracts

While updating their notification procedures, banking organizations and bank service providers should consider revisiting their contracts and making updates to provisions that are relevant to the Final Rule's requirements. The Agencies made clear that notification requirements are independent of any contractual provisions and that they did not expect or require contractual provisions to be updated, as bank service providers must comply with the Final Rule despite what any contracts with their banking organization customers require. The Agencies noted that they would not "cite" a banking organization if a bank service provider fails to meet its notification requirement. However, parties may find it helpful to ensure that their contracts reflect the obligation to be compliant with the Final Rule. The parties should review their contracts against the Final Rule's requirements to ensure that the provisions are stringent enough to meet the Final Rule's notification requirements for service providers — i.e., that notification is required immediately when there is or is likely to be a significant disruption to services for four or more hours.

Moreover, banking organizations and their service providers should consider the examples of notification-incidents that the Final Rule provides to determine whether any definitions, such as those for "data security incident" or "cyber event," should be updated or broadened. Parties may also want to consider adding "degradation" of services as a definition, if it is not already included, to fully capture the scope of the Final Rule. Contracts should also include the mutually agreed-upon methods of communication and notification procedures. This contractual review may be particularly helpful for banking organizations that provide sector-critical services, as they may want to consider enhancing the contractual notification requirements to allow them to make same-day notifications if possible. The Agencies do not expect that these reviews will be burdensome based on their experiences with conducting contract reviews during examinations.

Despite its seemingly daunting requirements, organizations should keep in mind that the Final Rule is meant to encourage them to review and, for the most part, formalize the processes and communications that they are likely already using. Where updates are required, organizations can rest assured that if they prepare to meet the Final Rule's tight timeline, they are likely in good shape to meet other notification requirements. ■