SULLIVAN & CROMWELL LLP

S&C memo

November 22, 2021

Federal Banking Agencies Issue Final Rule Regarding Cyber Incident Notification Requirements

Final Rule Requires Banking Organizations to Notify Primary Federal Regulator of Certain Cyber Incidents Within 36 Hours, and Bank Service Providers to Notify Banking Organization Customers as Soon as Possible

SUMMARY

On November 18, 2021, the Board of Governors of the Federal Reserve System (the "Board"), the Office of the Comptroller of the Currency (the "OCC"), and the Federal Deposit Insurance Corporation (the "FDIC," and together, the "Agencies") issued a final rule (the "final rule") mandating the reporting of certain significant cybersecurity incidents to regulators.[1] The final rule, which reflects the Agencies' consideration and incorporation of industry comments on the notice of proposed rulemaking (the "proposed rule"), requires a banking organization to notify its primary banking regulator within 36 hours of any "computer-security incident" which has or is reasonably likely to disrupt or degrade its (i) ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base; (ii) business lines, including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or (iii) operations, including associated services, functions, and support, the failure or discontinuance of which would pose a threat to the financial stability of the United States. Bank service providers are required to notify at least one designated point of contact at affected banking organization customers as soon as possible after any computer-security incident which has or is reasonably likely to materially disrupt or degrade covered services for four or more hours.

BACKGROUND

As the Agencies noted in issuing the proposed rule, cyberattacks reported to federal law enforcement have increased in frequency and severity in recent years, including with respect to cyberattacks that have the potential to alter, delete, or otherwise render a banking organization's data and systems unusable. Although federally regulated banking organizations are required to file suspicious activity reports ("SARs") on reportable cyber-events and are subject to the Gramm-Leach-Bliley Act (the "GLBA"), pursuant to which Agency guidance requires them to notify their primary federal regulator "as soon as possible" upon becoming aware of an incident involving unauthorized access to, or use of, sensitive customer information, no regulation required them to report cyberattacks affecting their operations to their primary federal regulator. The final rule changes that situation by requiring notification within 36 hours of certain significant cybersecurity incidents.[2]

THE FINAL RULE

The final rule requires a banking organization to notify its primary regulator of a "computer-security incident" rising to the level of a "notification incident" "as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred."[3] A "computer-security incident" is defined 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."[4] A "notification incident" is defined as a "computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's (i) 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; (ii) 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 (iii) 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."[5] A banking organization is required to provide notice to either an agency-designated point of contact or the appropriate supervisory office by email, telephone, or such other method as the agency may prescribe.

The final rule requires bank service providers, by any reasonable means, "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."[6] If the banking organization has not designated a point of contact, the bank service provider must notify either the customer's Chief Executive Officer and Chief Information Officer or two other individuals of comparable responsibilities at the customer.[7] Further, scheduled maintenance and updates were exempted from the notification requirement so long as the banking organization was forewarned.[8]

Compliance with the final rule is required by May 1, 2022.[9]

OBSERVATIONS

As the Agencies note, the final rule reflects a number of changes to the proposed rule in response to industry comments, most of which aimed to scale back the potential scope of the proposed rule. The Agencies received 35 comment letters on the proposed rule from banking and financial organizations, third-party service providers, industry groups, and individuals.[10] According to the Agencies, while most comments supported the Agencies' stated goal of prompt reporting of significant cybersecurity incidents,[11] comments also noted that the proposed rule could be read broadly to encompass a wide range of less significant cybersecurity incidents.[12] Such a reading, in turn, could have had the unintended consequence of creating a significant reporting burden on banking organizations, and would not achieve the Agencies' stated goals. Accordingly, some comments suggested language to further tailor the rule to the specific, significant cyber incidents that are the Agencies' intended focus.[13]

The final rule adopts many of the commentators' suggested revisions, including as follows:

- The definition of "computer-security incident" was narrowed to include only occurrences resulting in actual, not potential, harm, and to exclude violations of internal organizational policies.[14]
- The definition of "notification incident" was limited to a computer-security incident that "has or is reasonably likely to materially disrupt or degrade" operations rather than a computer-security incident that "a banking organization believes in good faith could materially disrupt, degrade, or impair" operations.[15]
- The trigger for the 36-hour reporting window was changed to the time at which there is a determination by the banking organization, rather than simply a good faith belief, that a notification incident has occurred. Further, the methods of providing such notification have been expanded.[16]
- Bank service providers will be required to notify "a bank-designated point of contact" (rather than "at least two individuals" at the banking organization), and to provide such notice "as soon as possible" rather than "immediately."[17]
- Designated financial market utilities have been excluded from the definitions of banking organization and bank service provider.[18]
- The Agencies clarified in the final rule's preamble that the trigger for a notification incident stemming from a material disruption or degradation of business line(s), which upon failure would result in a material loss of revenue, profit, or franchise value, refers to losses that are "material to the organization as a whole" and not merely the business line(s) at issue.[19]
- The Agencies explained in the final rule's preamble that the rule requires only "simple notification" with no "specific content or format" requirement.[20]

In sum, while the final rule represents an additional notification requirement for banking organizations and their service providers, and more broadly reflects the Agencies' heightened focus on cybersecurity risks and incidents, the final rule is meaningfully narrowed in scope compared to the proposed rule. As such, it appears to better align with the Agencies' stated goal of "promot[ing] early awareness of emerging threats to banking organizations and the broader financial system."

* * *

ENDNOTES

1 Office of the Comptroller of the Currency, Federal Reserve System, and Federal Deposit Insurance Corporation, *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers* (Nov. 18, 2021), *available at* https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211118a1.pdf (the "Final Rule").

2 Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 2299 (Jan. 12, 2021); *see* Office of the Comptroller of the Currency, Federal Reserve System, and Federal Deposit Insurance Corporation, *Agencies Propose Requirement for Computer Security Incident Notification* (Dec. 18, 2020), *available at* https://www.federalreserve.gov/newsevents/pressreleases/bcreg20201218a.htm.

3 Final Rule at 70.

4 Final Rule at 69.

5 Final Rule at 69–70.

6 Final Rule at 70.

7 Final Rule at 70–71.

8 Final Rule at 71.

9 Final Rule at 55.

10 Final Rule at 9.

11 Final Rule at 9–10.

12 Sullivan & Cromwell LLP, *Federal Banking Agencies Propose Cyber Incident Notification Requirements* (Dec. 22, 2020), *available at* https://www.sullcrom.com/files/upload/sc-publication-federal-banking-agencies-propose-cyber-requirements.pdf.

13 *See, e.g.*, American Bankers Association, Bank Policy Institute, Institute of International Bankers, and Securities Industry and Financial Markets Association, *Letter re Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers* (Apr. 12, 2021), *available at* https://www.regulations.gov/comment/OCC-2020-0038-0024 (the "Associations Letter").

14 Final Rule at 19–21, 69.

15 Final Rule at 21–26, 69–70; *see* Associations Letter at 6–9.

16 Final Rule at 29–35, 70; *see* Associations Letter at 10–14.

17 Final Rule at 38–42, 70.

18 Final Rule at 13–19, 69; *see* Associations Letter at 19.

19 Final Rule at 25; *see* Associations Letter at 9.

20 Final Rule at 31; *see* Associations Letter at 13.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.