SULLIVAN & CROMWELL LLP

December 22, 2020

Federal Banking Agencies Propose Cyber Incident Notification Requirements

Proposal Would Require Banking Organizations to Notify Primary Federal Regulator of Significant Incidents Within 36 Hours; Bank Service Providers to Notify Any Affected Bank Immediately

SUMMARY

On December 18, 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") released a notice of proposed rulemaking (the "proposal") regarding notification requirements for banking organizations and bank service providers related to significant cybersecurity incidents.[1] Under the proposal, a banking organization would be required to notify its primary banking regulator within 36 hours of a "computer-security incident" that it believes in good faith could materially disrupt, degrade, or impair (i) its ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base; (ii) any of its business lines, including associated operations, services, functions, and support, and would result in a material loss of revenue, profit, or franchise value; or (iii) any 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. Additionally, bank service providers would have to notify at least two individuals at affected banking organization customers immediately of significant computer-security incidents.

BACKGROUND

As the proposal notes, 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.[2] Although federally regulated

banking organizations are required to file 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 currently requires them to report cyberattacks affecting their operations to their primary federal regulator. As the Agencies note, the proposal aims to change that situation by requiring notification within 36 hours of certain cybersecurity incidents that could affect operations.

The Agencies provide several reasons why the notifications required under the proposal would be advantageous from a supervisory perspective, including: (1) earlier awareness of emerging threats to individual banking organizations and potentially the broader financial system; (2) better ability to assess the extent of the threat and take appropriate action in the case of a severe incident; (3) based on the Agencies' supervisory experiences, the ability to provide information to a banking organization that may not have previously faced a particular type of notification incident; (4) better ability 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 (5) enabling 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.[3]

Notably, outside the context of federal regulation, banking organizations are subject to a variety of additional data breach notification requirements. For institutions regulated by the New York State Department of Financial Services (the "DFS"), 23 NYCRR Part 500 ("DFS Part 500") requires notification to DFS within 72 hours of a determination that the covered entity has experienced a cybersecurity event that has "a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity" or that is required to be reported to "any government body, self-regulatory agency or any other supervisory body." Apart from banking regulations, all 50 states require notice to consumers of cybersecurity breaches affecting certain types of personal information, the nature of which varies by state. Many states require notice to state Attorneys General as well. Banking organizations are also subject to the EU's General Data Protection Regulation, which requires notice to supervisory authorities within 72 hours of certain types of cybersecurity incidents affecting individuals located in the EU, including non-EU citizens.

SUMMARY OF THE PROPOSAL

Under the proposal, a banking organization[4] would have to notify its primary regulator of a "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.[5] The proposal defines a "computer-security incident" as 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.[6] A "notification incident," which under the proposal would trigger the notification requirement, is defined as 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.[7] Banking organizations subject to the resolution planning rule under Section 165(d) of the Dodd-Frank Act can use their "core business lines" and "critical operations" identified in their resolution plans for purposes of clauses (ii) and (iii), respectively, of the definition of "notification incident." Those not subject to the resolution planning rule are not required to develop definitions of those terms for purposes of this proposed rule.[8] The proposal further notes that banking organizations that experience a computer-security incident that may be criminal in nature "are expected to contact relevant law enforcement or security agencies, as appropriate, after the incident occurs."[9]

- ***Examples of "Notification Incidents."*** The proposal provides a non-exhaustive list of events that would meet its definition of "notification incident":
  - large-scale distributed denial of service attacks that disrupt customer account access for an extended period of time (e.g., more than 4 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 proposal also gives the example of a limited distributed denial of service attack that is promptly and successfully managed by a banking organization as an incident that would likely *not* be a notification incident.[10]
- ***Form of Notification.*** Under the proposal, a banking organization could provide the required notification through "any technological means," such as email or telephone, to a designated point of contact identified by its primary federal regulator, such as an examiner-in-charge, local

supervisory office, or a cyber-incident operations center. The Agencies note in the proposal that the notification is intended to serve as an early alert to the primary federal regulator about a notification incident and is not intended to include an assessment of the incident. The notification does not require any specific information, and the proposal does not include a reporting form for notification.[11]

- ***Timing.*** A banking organization would have to notify its primary regulator as soon as possible and no later than 36 hours after it makes a good faith determination that a "notification incident" has occurred. The Agencies note in the proposal that they do not expect that a banking organization typically would be able to determine that a notification incident has occurred immediately upon becoming aware of a computer-security incident. Instead, they expect that a banking organization would take a reasonable amount of time to determine that it has experienced a notification incident. Furthermore, the Agencies state in the proposal that they "recognize banking organizations may not come to a good faith belief that a notification incident has occurred outside of normal business hours. Only once the banking organization has made such a determination would the requirement to report within 36 hours begin."[12]

Bank Service Providers

Finally, the Agencies note that banking organizations have become more dependent on bank service providers for essential services, such service providers are themselves subject to cyber risk, and the proposal is meant to address these increased risks.[13] As a result, under the proposal, a "bank service provider" would be required to notify at least two individuals at each affected banking organization customer 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 Bank Service Company Act (the "BSCA") for 4 or more hours.[14] For the purposes of the proposal, a "bank service provider" is a bank service company or other person providing services to a banking organization that is subject to the BSCA.[15] Such notification would not need to include an assessment of the computer-security incident; rather, the Agencies expect "a best effort to share general information about what is known at the time."[16] A banking organization would then need to determine whether the reported computer-security incident rises to the level of a notification incident and therefore requires 36 hours' notice to the banking organization's primary federal regulator.

Under the proposal, the Agencies would be able to enforce the notification requirements for bank service providers directly against the providers themselves, rather than indirectly through a banking organization customer.[17] However, the Agencies believe that the proposal would not impose significant compliance costs on bank service providers, based on their belief that such providers already have automated systems that alert customers when incidents requiring notification under the proposal occur.[18]

Request for Comments

The Agencies are seeking comments on the proposal, including 16 specific areas listed in the proposal. Those areas include whether computer-security incidents should require actual harm, whether the time frame should be modified, including whether it should be extended for smaller banking organizations, and whether the rule for bank service providers should provide for notice to all banking customers (as opposed

to only affected customers). Comments are due 90 days after the proposal is published in the *Federal Register*.

IMPLICATIONS

Although the proposal makes clear that the notification standard is intended to be a "high threshold" and "is not expected to add significant burden on banking organizations," the proposed definition of "notification incident" broadly includes not only incidents that have materially harmed operations, or that have "a reasonable likelihood" of doing so (the notification standard under DFS Part 500), but also those incidents that simply "could" have such an effect. As a result, the notification standard may apply broadly or be challenging to interpret in certain circumstances. As an example, this month, a vulnerability was identified in certain SolarWinds software, widely used by government agencies and companies, including banking organizations and their service providers, that potentially exposes users to a risk of serious compromise by a reported nation-state adversary. Since it is possible that such a computer-security incident "could" materially disrupt, degrade, or impair a banking organization's operations or business line, it would appear that use of this software by a banking organization or any of its key service providers could trigger a notification incident under the proposal even if it is not currently believed that the vulnerability has led to a compromise. This is particularly true given the challenge in determining quickly or easily whether any such compromise has occurred.

Separately, the proposal would require banking organizations to report notification incidents more quickly than any existing law or regulation currently requires. The proposal cuts in half the required time frame to notify the DFS under DFS Part 500, for example, which is currently one of the shortest prescribed time frames for notification of a reportable cybersecurity incident in the U.S. Although the Agencies have made clear that they understand banking organizations may not immediately be able to determine whether a notification incident has occurred, and that the 36-hour deadline would run from the time such a determination is made, in practice, these determinations can be difficult for any organization, public or private, to make with precision depending on the circumstances. The facts typically evolve (for better and for worse) in connection with a computer-security incident, and the determination that a notification incident has occurred may require input from disparate areas of the banking organization, including cybersecurity, operations, finance, legal and executive personnel, and possibly external technical experts. In other words, the particularly short proposed deadline for notification may suggest there is more precision about the moment such a determination occurs than may reasonably be possible in practice.

To the extent any uncertainty about the applicable deadline puts pressure on banking organizations to over-report or report more quickly than they would otherwise be comfortable doing based on their understanding of relevant facts, banking organizations could face additional pressure and challenges with respect to public disclosures and disclosures to other agencies. For example, as noted, DFS Part 500 requires covered

entities to report within 72 hours any cybersecurity incidents that have a "reasonable likelihood" of materially harming any material part of operations or are required to be reported to any government body, self-regulatory agency, or any other supervisory body. As a result, the proposal may have the effect both of shortening the effective time frame for disclosure to the DFS and effectively expanding the scope of what must be disclosed to the DFS from those events that have "a reasonable likelihood" of impacting operations to those that merely "could" have such an impact (as required under the proposal).

Finally, the proposal is significant for the context in which it arises. Federal banking regulators have not historically issued prescriptive cybersecurity rules or brought public enforcement actions in the wake of cybersecurity breaches. Instead, they have played a significant role in developing processes to enable banks to measure cybersecurity risk and preparedness, such as through the Federal Financial Institutions Examination Council's Cybersecurity Assessment Tool,[19] and in encouraging banks to focus on cyber risk management through exam findings and guidance, such as the OCC and FDIC's Joint Statement on Heightened Cybersecurity Risk[20] issued earlier this year. In the past six months, however, the Agencies have taken a markedly different approach, bringing a landmark enforcement action against Capital One in August 2020 in the wake of its cybersecurity breach, and now issuing a prescriptive proposed cybersecurity notification rule. These actions likely signal that the Agencies intend to continue to play a more active role in oversight and enforcement in connection with cybersecurity incidents.

* * *

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* (December 18, 2020), *available at* https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201218a1.pdf (the "Proposal").

2 Proposal at 7.

3 Proposal at 9-10.

4 The proposal defines a "banking organization" as (i) for the OCC, national banks, federal savings associations, and federal branches and agencies; (ii) for the Board, all U.S. bank holding companies and savings and loan holding companies; state member banks; the U.S. operations of foreign banking organizations; and Edge and agreement corporations; and (iii) for the FDIC, all insured state nonmember banks, insured state-licensed branches of foreign banks, and state savings associations. Proposal at 15.

5 Proposal at 12-13.

6 Proposal at 13.

7 Proposal at 13-14.

8 Proposal at 16-17.

9 Proposal at 8.

10 Proposal at 15-16.

11 Proposal at 18.

12 Proposal at 12-13.

13 *See* Proposal at 8-9.

14 Proposal at 18-19.

15 *E.g.*, Proposal at 44-45.

16 Proposal at 19.

17 Proposal at 19-20. Note that a banking organization's notification requirement may be triggered by receiving notification from a bank service provider of a computer-security incident that rises to the level of a notification incident. However, the bank service provider would not be required to assess whether the incident rises to the level of a notification incident for a banking organization customer. Proposal at 19.

18 Proposal at 24-25.

19 Federal Financial Institutions Examination Council, Cybersecurity Assessment Tool, *available at* https://www.ffiec.gov/cyberassessmenttool.htm.

20 Federal Deposit Insurance Corporation and Office of the Comptroller of the Currency, *Joint Statement on Heightened Cybersecurity Risk* (January 16, 2020), *available at* https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-5a.pdf.

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.