Banking Agencies Propose 36-Hour Data Breach Reporting Rules for Significant Incidents

December 18, 2020

On December 15, 2020, the Federal Deposit Insurance Corporation ("FDIC"), the Office of the Comptroller of the Currency ("OCC") and the Federal Reserve Board ("FRB") (together the "Agencies") issued a notice of proposed rulemaking ("Proposed Rule") that would significantly update the Agencies' guidance on data breach response. The Proposed Rule would impose prompt reporting requirements on banking organizations and their service providers with respect to certain data breaches and other cyber events.

Specifically, the Proposed Rule would require banking organizations to notify their primary federal regulators within 36 hours of becoming aware of a "computer-security incident" that rises to the level of a "notification incident." In addition to covering incidents involving unauthorized access to customer person information, it would apply to some events where data was rendered temporarily unavailable, such as ransomware and distributed denial-of-service attacks.

The rule would also require bank service providers to notify "at least two individuals" at an affected banking organization-customer immediately after experiencing a computer-security incident that it believes "in good faith could disrupt, degrade, or impair services provided for four or more hours." A 36-hour deadline appears to be one of the most rigorous timeframes of any U.S. breach reporting scheme.

Below we provide context for the Proposed Rule and outline its key features.

BACKGROUND

Banking organizations already are subject to reporting obligations of cyber events and data breaches under applicable federal and state laws. Notably, the new proposal would blow the dust off the federal interagency guidance—issued in 2005 and never before updated—that interprets the Gramm-Leach-Bliley Act and its Security Guidelines ("GLBA") to require banks to develop and implement a response program to address unauthorized access to, or use of customer information that could result in "substantial harm or inconvenience to a customer." This guidance only requires banking

organizations (as defined therein) to report incidents to federal banking regulators where certain customer personal data is exposed.

In addition, the Bank Secrecy Act requires banking organizations, and other financial institutions, to file suspicious activity reports ("SARs") under certain circumstances. In 2016, the Financial Crimes Enforcement Network ("FinCEN") issued an advisory instructing financial institutions with SAR filing obligations to file SARs for cyber-events and cyber-enabled crime. The SAR filing requirements are designed to detect cyber-related crimes and money laundering but not report cyber incidents more broadly. Further, 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.

At the state level, some banking organizations are subject to more recent and specific reporting requirements. For example, the New York State Department of Financial Services ("NYDFS") adopted a cybersecurity regulation in 2017, known as Part 500. Part 500 requires covered entities, including New York state-chartered banks and other financial organizations licensed by the NYDFS to conduct business, to implement an incident response plan as part of their cybersecurity program and to notify the NYDFS no later than 72 hours after determining that a cybersecurity event has (1) impacted the entity and notice is required to be provided to another regulator, or (2) a reasonable likelihood of materially harming a material part of the normal operation of the entity.

Banking organizations are also potentially subject to state breach notification laws that apply to businesses generally in all 50 states, although some of those requirements under state law can be satisfied by GLBA. California, for example, requires persons conducting business in California to notify California residents if their unencrypted personal information is acquired or is reasonably believed to have been acquired by an unauthorized person. If a single breach requires such a notification to more than 500 California residents then a business must submit a sample security breach notification to the California Attorney General. Many other states' laws are modeled on California's law.

OVERVIEW OF BANKING ORGANIZATION NOTIFICATION REQUIREMENT

The Proposed Rule would require banking organizations to notify their primary federal regulator of cyber incidents that amount to "notification incidents" no later than 36 hours after determining in "good faith" that a notification incident has occurred. The notification requirement is meant to serve as an "early alert" to regulators and is not

intended to provide an "assessment of the incident," which is all that can be reasonably expected in 36 hours.

Definitions of Banking Organizations

The Proposed Rule applies to "banking organizations," as defined by the applicable federal regulator. For foreign banks, the Proposed Rule would only apply to their U.S. operations. Further, under the Proposed Rule if a banking organization is the subsidiary of another banking organization subject to notification requirements (*e.g.*, a bank is a subsidiary of a bank holding company), the subsidiary banking organization is expected to alert its parent—in addition to notifying its primary federal regulator—of a notification incident "as soon as possible." The parent banking organization must then determine whether it also has suffered an incident that requires notification.

On the other hand, the Proposed Rule does not require subsidiaries or banking organizations not subject to the notification requirement (*e.g.*, nonbank subsidiaries of bank holding companies) to implement separate notification requirements. Instead, the Agencies expect that the parent banking organization of such subsidiary will appropriately notify its primary federal regulator if the incident at the subsidiary constitutes a notification incident for the parent.

Definition of Computer-Security Incident and Notification Incident

Under the Proposed Rule, a computer-security incident is an occurrence "that (i) results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information 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."

A "notification incident" is a type of 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."

For purposes of determining whether a computer-security incident falls under the definition of notification incident, "business line" is defined as "products or services offered by a banking organization to serve its customers or support other business

needs." The Agencies note that all banking organizations are expected to have a "sufficient understanding of their lines of business to be able to notify the appropriate agency of notification incidents that could result in a material loss of revenue, profit, or franchise value to the banking organization." The Proposed Rule also includes a non-exhaustive list of events that would meet the definition of "notification incident," such as a failed system upgrade or change that results in widespread customer or employee outages.

Timing of Notification Requirements

As noted above, the Proposed Rule requires banking organizations to notify their primary federal regulator within 36 hours of a "good faith determination" that a notification incident has occurred. In that regard, the Agencies recognize that the banking organization would not be able to determine whether an event meets the notification incident standard immediately upon becoming aware of the incident, particularly outside of normal business hours. As a result, banking organizations may take a "reasonable amount of time" to determine whether a computer-security incident meets the notification incident standard. Once a banking organization has made a determination that a computer-security incident meets the notification incident standard, then the 36-hour clock begins to run.

Contents and Format of Notification

The Proposed Rule neither prescribes the contents to be included in the notice nor requires that notification be given in any particular format. Any form of written or oral communication, via any technological means (e.g., email or phone call) or other means (*e.g.*, live conversation) to a designated point of contact identified by the applicable primary federal regulator is sufficient. Any information provided by the banking organization related to the notification incident is subject to the Agencies' confidentiality rules, meaning that confidential supervisory information will be protected.

IMPACT OF PROPOSED RULE

The Agencies do not believe that the Proposed Rule will impose significant burdens on banking organizations. They estimate that roughly 150 incidents rising to the level of "notification incidents" may occur on an annual basis, and believe that the communications leading to the determination of a "notification incident" would occur regardless of the Proposed Rule. Moreover, the notice requirements for banking organizations should not include the level of detail required for an SAR, though the Agencies expect banking organizations that experience a potentially criminal computer-

security incident to contact relevant law enforcement or security agencies after the incident occurs.

The Proposed Rule affects state reporting requirements as well. For example, Part 500 requires banking organizations to report to the NYDFS if reporting of a cybersecurity event is required to another regulator, such as one of the Agencies. In light of NYDFS's broad definition of "cybersecurity event," any "notification incident" will almost certainly qualify as a "cybersecurity event." Thus, any such notification incidents reported to the FDIC, OCC or FRB must also be reported to the NYDFS if the banking organization is subject to NYDFS supervision, though subject to the NYDFS's 72-hour timeframe.

SERVICE PROVIDER NOTIFICATION REQUIREMENT

The Proposed Rule also imposes reporting requirements on "bank service providers," defined as companies or persons providing services that are subject to the Bank Service Company Act to banking organizations. Specifically, if the bank service provider has a good faith belief that a computer-security incident could disrupt, degrade or impair services, including back office services, provided to a banking organization for four or more hours, the bank service provider would be required to immediately report the incident to any affected banking organization-customers. Additionally, bank service providers must notify at least two individuals at an affected banking organization, to ensure notice is received. The Agencies would aim to enforce these notification requirements directly against bank service providers. Indeed, any failure by a bank service provider to comply with the Proposed Rule would not be cited against the banking organization.

* * *

Overall, these notification requirements could impose significant obligations on banking organizations and their service providers. The greatest challenge may be figuring out how to meet the 36-hour standard. Further, there is a risk that increased regulatory visibility into potential cyber breaches may lead to increased scrutiny on banking organizations' cyber practices. The Agencies seek comment on the proposal and outline some detailed questions for commenters. For example, the Agencies seek comments on the definitions as drafted, whether the 36-hour notification timeline should be adjusted, whether the "good faith" standard for banking organizations and bank service providers to notify the appropriate party is appropriate, among other questions. Comments must be submitted no later than 90 days after the publication of the Proposed Rule in the Federal Register.

Please do not hesitate to contact us with any questions.

To subscribe to the Data Blog, please click here.

NEW YORK


Jeremy Feigelson
jfeigelson@debevoise.com


Avi Gesser
agesser@debevoise.com


Gregory J. Lyons
gjlyons@debevoise.com


Jim Pastore
jjpastore@debevoise.com


David L. Portilla
dlportilla@debevoise.com


Zila Reyes Acosta-Grimes
zracosta@debevoise.com


Alex Henry
ahenry@debevoise.com


Alexandra N. Mogul
anmogul@debevoise.com


Courtney Bradford Pike
cbpike@debevoise.com


Amy Aixi Zhang
aazhang@debevoise.com

WASHINGTON, D.C.


Luke Dembosky
ldembosky@debevoise.com


Satish M. Kini
smkini@debevoise.com