Banking Regulators Finalize 36-Hour Data Breach Notification Rule

November 24, 2021

On November 18, 2021, federal banking regulators published a Final Rule that imposes new notification requirements on banking organizations for certain cybersecurity incidents.

Most significantly, the Final Rule requires that banking organizations notify their primary federal regulator within 36 hours after experiencing a material or potentially material cybersecurity event.

The Final Rule will go into effect on April 1, 2022, with a required compliance date of May 1, 2022.

The regulators—the Federal Deposit Insurance Corporation ("FDIC"), the Office of the Comptroller of the Currency ("OCC") and the Federal Reserve Board ("FRB") (together the "Agencies")—first published a proposed rule about ten months ago, which we covered on the Data Blog. Much of the proposed rule was carried over into the Final Rule, but there are a few key differences, which we identify below.

REQUIREMENTS FOR BANKING ORGANIZATIONS

A *banking organization* must notify its primary federal regulator of any *computer-security incident* that rises to the level of a *notification incident* no later than 36 hours after determining that a notification incident has occurred.

- A "banking organization" is defined to include national banks, state banks, federal and state branches of foreign banks, bank and thrift holding companies, and federal savings associations. Unlike the proposed rule, the Final Rule specifically exempts designated financial market utilities. The Agencies accepted comments noting that designated financial market utilities are already subject to incident notification requirements under 17 CFR 39.18(g), 12 C.F.R. Part 234, or SEC Reg SCI.

- A "computer-security incident" is an event that results in actual harm to an information system or the information contained within it. The Final Rule's requirement of actual harm represents a significant narrowing of the definition of a computer-security incident from the proposed rule, which had included (i) potential harm to information systems and (ii) violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. The proposed rule also incorporated the NIST definition of computer-security incident, but through the comment process it appears the Agencies recognized that using the broader NIST definition would likely result in many unnecessary and burdensome notifications.

- A "notification incident" is a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's operations:

  - affecting a material portion of its customer base;

  - resulting in a material loss of revenue, profit, or franchise value; or

  - posing a threat to the financial stability of the United States.

The Final Rule also adopted clearer standards for when the notification obligation is triggered:

- "Reasonably likely to" replaces "could" in the risk of harm assessment, which is a less sweeping standard that permits organizations to make reasonable assessments of the situation as opposed to being forced to consider abstract hypotheticals.

- Notifications are only required by the Final Rule after a "determination" that a notification incident occurred, while the proposed rule used a less concrete "good faith belief" standard.

Banking Organizations' Regulator Notifications

Notification to regulators need not take any specific form or include any specific information. Agency-designated points of contact can be notified by email, telephone or any similar method that the agency prescribes.

Notifications to regulators, and any information related to the incident, would be subject to the Agencies' confidentiality rules; however, the Agencies are still required to respond to individual FOIA requests on a case-by-case basis.

REQUIREMENTS FOR BANK SERVICE PROVIDERS

Under the Final Rule, a *bank service provider* must 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 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 customer for four or more hours. Banking organizations are responsible for then assessing whether they need to notify their regulator, using the standard for notification incidents above.

The timing requirement—as soon as possible when the bank service provider determines it has experienced a computer-security incident—seeks to strike a balance between the time needed for bank service providers to examine the nature of the incident and assess the materiality of the disruption and the urgency faced by affected banking organizations experiencing a service disruption.

In response to comments that bank service providers are typically bound by contract to notify banking organization customers of disruptions, the Agencies made clear that they did not expect or require these contractual provisions to be revised.

- "Bank service provider" is defined as "a bank service company or other person that performs covered services; provided, however, that no designated financial market utility shall be considered a bank service provider," where *covered services* are services performed, by a person, that are subject to the Bank Service Company Act (12 U.S.C. 1861–1867). The Agencies added a definition of covered services to the Final Rule, but rejected comments recommending narrowing the definition of bank service providers, stating that the risk to banking organizations is not limited to a narrow group of bank service providers as vectors.

Notifications to Banking Organizations

The notification to a bank-designated point of contact must be sent to "an email address, phone number, or any other contact(s), previously provided to the bank service provider by the banking organization customer" or, "if the banking organization customer has not previously provided a bank designated point of contact… the Chief Executive Officer and Chief Information Officer of the banking organization customer, or two individuals of comparable responsibilities, through any reasonable means."

The Final Rule's single point of contact replaces the proposed rule's requirement to notify "at least two individuals" at each banking organization customer.

Although the Final Rule's requirements are in some ways less onerous than the proposed rule, the 36-hour notification requirement will likely pose a significant challenge for banking organizations experiencing the strain of a significant cyber incident. Such a short notification window makes clear the importance of preparing for an incident—including through the development of policies for identifying and escalating incidents that may trigger the 36-hour notification, and testing those policies through tabletop exercises that present a realistic simulated incident.

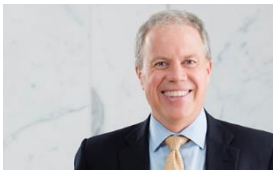
* * *

Please do not hesitate to contact us with any questions.

To subscribe to the Data Blog, please click here.

NEW YORK

Avi Gesser
agesser@debevoise.com



Gregory J. Lyons
gjlyons@debevoise.com

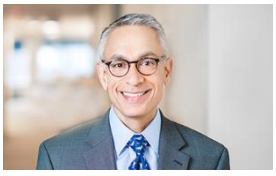
Johanna N. Skrzypczyk
jnskrzypczyk@debevoise.com

Alexandra N. Mogul
anmogul@debevoise.com

Erik Rubinstein
erubinstein@debevoise.com

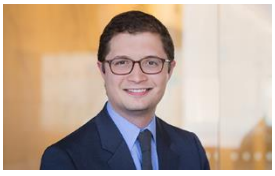
WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com



Satish M. Kini
smkini@debevoise.com

SAN FRANCISCO



Christopher S. Ford
csford@debevoise.com