NOW & NEXT

Financial Institutions & Banking Disputes Alert

FEBRUARY 16, 2022

36 hours: What banks should know about the upcoming compliance deadline for reporting computer security incidents

By Christopher Queenin, Christopher M. Mason, and Jason C. Kravitz

New reporting requirements for banks follow trend of increasing federal oversight of computer security incidents.

What's the Impact?

- The deadline for full compliance is set for May 1, 2022
- The short reporting window means that businesses should promptly investigate and report cybersecurity incidents
- Businesses should consult with counsel now to determine if cybersecurity infrastructure and policies are sufficient to meet these new requirements

Over the past year, the federal government has continued to increase the pressure on private companies to report cybersecurity incidents and data breaches. In October, the Justice Department announced how it would use the False Claims Act to pursue companies that receive payments from the government and knowingly violate obligations to monitor and report cybersecurity incidents and breaches. At the end of December, the Department of Defense announced a revised set of cybersecurity standards for government contractors and subcontractors (dubbed Cybersecurity Maturity Model Certification 2.0).

Continuing this theme, financial institutions regulated by the Federal Deposit Insurance Corporation (the FDIC), the Board of Governors of the Federal Reserve System (the Fed), and the Office of the Comptroller Currency (the OCC) will now face new computer-security incident notification requirements in a rulemaking common to all three agencies. The new requirements for these financial institutions appear in a recently issued final rule (the Final Rule) with a May 1, 2022, compliance deadline.[1] Banks should make sure that they are carefully reviewing the new requirements and updating their policies (including risk assessments, information security programs, and incident response plans) as well as coordinating with their service providers about the new obligations they share.

The notification requirement in the Final Rule is notable for its very short reporting window—36 hours. This is even shorter than, for example, the 72 hours in Defense Department regulations, such as 48 C.F.R. § 252.204-7012(a) ("Rapidly report" means "within 72 hours of discovery of any cyber incident"), and similar time periods under the GDPR or some state laws. The intended purpose of this short time frame is to ensure an early alert to a bank's primary federal regulator of the occurrence of any significant computer-security incident so that the regulator can react to the threat before it becomes a broader, potentially systemic, issue.

Here are the highlights of the Final Rule:

- A bank must notify its primary federal regulator of any **"computer-security incident"** that rises to the level of a **"notification incident"** within 36 hours after the bank determines that such an incident has occurred.
- A bank service provider must notify at least one point of contact designated by its bank customer as soon as possible when the service provider determines that it has experienced a computer-security incident that is reasonably likely to disrupt or degrade services provided to the bank for four or more hours. If the bank has not provided the service provider with a designated point of contact, the service provider must notify the bank's CEO and CIO (or individuals with comparable responsibilities).
- The final rule takes effect on April 1, 2022, with a deadline for full compliance set for May 1, 2022.

What is a computer-security incident?

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." As we will see below, this covers far more than data breaches.

[1] The Final Rule is codified in each agency's own regulations. *See* 12 C.F.R. Part 304 (FDIC); 12 C.F.R. 225 (Board); 12 C.F.R. Part 53 (OCC).

What is a notification incident?

The agencies recognize that banks manage computer-security incidents every day, and are not requiring banks to report each such incident. Instead, only those computer-security incidents that rise to the level of a "notification incident" must be reported.

A "notification incident" is defined as a computer-security incident that is "reasonably likely" to materially disrupt or degrade a bank's:

- 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;
- business line(s), including associated operations, services, functions, and support, that upon failure would result in material loss of revenue, profit, or franchise value; or
- 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.

Because of this "reasonably likely" standard, a bank will not have to notify its regulator when adverse consequences *are merely possible or capable of* being imagined. Still, it is likely that minds will differ in some instances as to when a notification incident is reasonably likely to cause a material disruption or degradation. To that end, the Final Rule includes a non-exhaustive list of seven examples of what the agencies generally consider "notification incidents":

- Large-scale DDoS (distributed denial of service) attacks that disrupt customer account access for an extended period of time (*e.g.,* more than 4 hours);
- Widespread system outages experienced by a service provider used by a bank for its core banking platform to operate business applications, when the 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 bank's business continuity or disaster recovery plan;
- A computer hacking incident that disables banking operations for an extended period of time;
- Malware on a bank's network that poses an imminent threat to the bank's core business lines or critical operations, or that requires the bank to disengage any compromised products or information systems that support the bank's core business lines or critical operations from internet-based network connections; and
- A ransom malware attack that encrypts banking system or backup data.

Because this list is only illustrative, institutions must evaluate, on a case-by-case basis, whether an incident is significant enough to require notifying the bank's primary regulator. The Final Rule cautions that, if a bank is in doubt, it should err on the side of notification.

Importantly (and unfortunately, for the regulated entities) the Final Rule does not supersede or replace any other breach notification laws. The agencies considered whether existing laws and reporting standards would meet the goals of the Final Rule and concluded that they would not. Thus, a notification incident could trigger multiple different laws.[2] The agencies also expect that a bank that experiences a computer-security incident that may be criminal in nature will, as appropriate, contact relevant law enforcement or national security agencies.

When must a bank report the notification incident?

A bank must report a notification incident within 36 hours of "determin[ing] that a notification incident has occurred." This 36-hour notification requirement is shorter than most other data breach laws.

However, the 36-hour clock only starts once a bank "determines" that a notification incident has occurred. Many other breach notification laws, by contrast, start once an organization *begins* investigating or "becomes aware" of a breach. For example, the 72-hour clock under the GDPR starts once an organization "become[s] aware of a breach." GDPR, Art. 33. The use of the term "determines" in the Final Rule potentially gives a bank some additional cushion of time to examine the nature of the incident and assess whether it rises to the level of a notification incident. But this time will be limited by the circumstances and the default position of the Final Rule is that if a bank is in doubt as to whether it is experiencing a notification incident, it should notify its primary regulator. (The agencies, therefore, also recognize that a bank may file a notification from time to time based on a good-faith, but mistaken, determination that a notification incident has occurred when one actually has not.)

What liability could a bank or its service provider face for failing to report a notification incident?

Aside from regulatory enforcement, as with any data security incident, there is a risk of class action litigation by affected customers (and *qui tam* actions under the False Claims Act if the institution receives federal payments) if a bank fails to promptly report an incident that must be reported under the Final Rule. This is true even though the Final Rule does not include its own private right of action in favor of bank customers. Clever plaintiffs' counsel will have no trouble advancing theories based, for example, on unfair and deceptive practices theories whether or not such claims are ultimately sustained.

---

[2] As just one example, the same incident in New York that might trigger reporting to a federal regulator would likely also require state notification under the New York State Department of Financial Services Cybersecurity Requirements for Financial Services Companies (which requires notification if an incident has "a reasonable likelihood of materially harming any material part of the normal operation(s)" of covered financial institutions, 23 NYCRR 500.17).

What steps should banks and service providers take in light of the May 1, 2022, compliance deadline?

Banks and their service providers should take certain actions now in anticipation of the May 1, 2022, compliance deadline. These actions include the following:

- A bank should review and update its internal policies and procedures—and especially its incident response plan—to ensure compliance with the Final Rule. Among other things, the bank should identify which employees (and positions—because employees change) are the point of contact for bank personnel, service providers, and federal regulators vis-à-vis computer-security incidents. The bank should also update the contact information for the appropriate federal regulator (the FDIC, OCC, or Fed) for reporting notification incidents.
- Similarly, a bank should educate relevant employees on the requirements of the Final Rule. This includes training for relevant employees on how to identify and escalate suspected computer-security incidents to appropriate bank personnel. It also includes training for any employee designated as the point of contact for service providers on how to promptly respond to an incident, determine whether the bank must notify its primary federal regulator that a notification incident has occurred, and on what other appropriate measures relating to the incident must be taken.
- A bank and its service providers should review and update their service agreements and adjust key performance requirements. All service agreements should include a bank-designated point of contact (along with contact information) so that the service provider can notify the bank as soon as possible if the provider determines it is experiencing a computer-security incident that has materially disrupted or degraded (or is reasonably likely to materially disrupt or degrade) covered services provided to the bank for four or more hours.
- A bank should continue to monitor any guidance issued from its primary regulator. The FDIC, in particular, has stated that it will soon provide its supervised institutions with additional advice on compliance with the notification requirement.

What is the takeaway?

Financial institutions already deal with too many multiple and overlapping reporting and notification requirements. The Final Rule does not help relieve this complexity. But its prompt notification regime will help contain incidents that might otherwise spread or repeat. Furthermore, if an incident is isolated by prompt reporting, the Final Rule provides that regulators may be willing to assist the reporting institution in mitigating the impact of the incident. Such assistance may be especially helpful to smaller institutions and community banks that have more limited resources. And finally, while the timing requirement in the Final Rule may be onerous in and of itself, there is little doubt that prompt action in response to cyber incidents is highly likely to be one of the most effective ways to reduce the ultimate costs of those incidents to an institution.

What's Next?

Continuing the trend of federal involvement in regulating data breaches, on February 9, 2022, the Securities and Exchange Commission (SEC) voted to propose a new rule regarding cybersecurity risk management for investment advisors and registered investment companies, including business development companies. The SEC's proposed rule would require that investment advisors and funds implement written policies and procedures to address cybersecurity risks, and notify the SEC within 48 hours of concluding that a significant cybersecurity incident has occurred or is occurring.

Nixon Peabody will continue to monitor developments. For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Christopher Queenin
617.345.1080
cqueenin@nixonpeabody.com

Christopher M. Mason
212.940.3017
cmason@nixonpeabody.com

Jason C. Kravitz
617.345.1318
jkravitz@nixonpeabody.com