PUBLICATION

Faster and More Comprehensive Breach Notification Requirements Proposed for Banks

Authors: Matthew George White, Alexander Frank Koskey, III
January 13, 2021

The Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (FRB), and the Federal Deposit Insurance Company (FDIC), have issued a notice of proposed rulemaking (Proposed Rule) that would require a banking organization to provide its primary federal regulator with prompt notification of any "computer-security incident" that rises to the level of a "notification incident." The Proposed Rule would, among other things, require banks to notify their primary regulators of a triggering incident as soon as possible, and no later than 36 hours after learning that the incident occurred, and would require banking service providers to notify affected bank customers immediately after experiencing a security incident that disrupts or impairs services for four hours or more.

The Proposed Rule would fundamentally change a bank's current notification obligations under the Gramm-Leach-Bliley Act (GLBA) and the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (the Interagency Guidance) and the Interagency Guidelines Establishing Information Security Standards (the Interagency Guidelines) by attaching specific notification timelines, explicitly defining triggering events, and imposing delineated obligations on banking service providers. All covered banking organizations need to pay attention to this Proposed Rule as it has the possibility of fundamentally altering the ways in which banks will be required respond to data incidents.

Threat Landscape

It is undisputed that the frequency and severity of cyberattacks have increased in recent years. This has only been exacerbated by COVID-19, which has resulted in a marked increase in cyberattacks. Banks continue to be a prime target for such attacks. In fact, according to a recent report from cyber vendor VMware Carbon Black, attacks on financial institutions spiked by 238 percent between February and April 2020 alone. Not only are financial service providers a prime target, but according to Accenture and the Ponemon Institute, the costs to address and contain cyber attacks are greater for financial firms than for companies in any other industry. Those costs only continue to rise.

Current Regulatory Obligations

Currently, banking organizations may be required to report certain instances of disruptive cyber-events and cybercrimes through the filing of Suspicious Activity Reports (SARs), and are generally expected to notify their primary federal regulators "as soon as possible" when they become "aware of an incident involving unauthorized access to or use of sensitive customer information." Under the Bank Secrecy Act (BSA) reporting requirements, SARs are typically required to be filed within 30 calendar days (and sometimes 60 days). Pursuant to the Interagency Guidance and Guidelines, computer-security incidents that result in the compromise of sensitive customer information should be reported to an organization's primary regulatory as soon as possible. Finally, the Bank Service Company Act (BSCA) requires a banking organization to notify the appropriate federal banking agency of the existence of service relationships within 30 days after the execution of such service contracts or the performance of the service, whichever occurs first, but contains no notification requirements if the service is disrupted.

Summary of the Proposed Rule

The Proposed Rule would establish two primary requirements. First, a banking organization would be required to notify its primary federal regulator of any 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. Second, a bank service provider of a service described under the BSCA would be required to notify at least two individuals at affected banking organization customers immediately after experiencing a computer-security incident that it believes in good faith could disrupt, degrade, or impair services provided subject to the BSCA for four or more hours.

New Notification Requirements

As indicated above, the Proposed Rule would attach a specific notification timeframe to a bank's notification obligations. Currently, under the Interagency Guidance and Guidelines, a bank must notify its primary regulator of a triggering event as soon as possible. The Proposed Rule attaches a specific timeframe to the regulatory notification requirement of no later than 36 hours after a bank's learning that an incident has occurred. It is important to note that a 36-hour notification requirement is substantially shorter than many current state law consumer notification requirements, shorter than the New York Department of Financial Services' (NYDFS) 72-hour notification requirement under its Cybersecurity Regulation, and also shorter than the 72-hour breach notification requirement under the EU's General Data Protection Regulation (GDPR). This would force banks to make quick decisions about whether an event triggers this requirement, and if so, to very quickly make the regulatory notification.

In addition to this substantial change to the reporting timeframe, the Proposed Rule also enhances the definition of triggering events that must be reported. Specifically, the Proposed Rule 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 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. The Proposed Rule defines a ***notification incident*** as a computer-security incident that a banking organization believes in good faith could materially disrupt, degrade, or impair −

…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;

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 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.

The Proposed Rule also provides a non-exhaustive list of computer-security incidents that would be considered to be "notification incidents" including:

1. Large-scale distributed denial of service attacks that disrupt customer account access for an extended period of time (e.g., more than four hours);

2. 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;

3. A failed system upgrade or change that results in widespread user outages for customers and bank employees;

4. An unrecoverable system failure that results in activation of a banking organization's business continuity or disaster recovery plan;

5. A computer hacking incident that disables banking operations for an extended period of time;

6. Propagation of malware on a banking organization's network that requires the banking organization to disengage all Internet-based network connections; and

7. A ransom malware attack that encrypts a core banking system or backup data.

However, the Proposed Rule also states that banks would be expected to consider whether other significant computer-security events would constitute notification incidents.

The Proposed Rule does not delineate specific information required for the notice and does not include any prescribed reporting forms or templates. It does provide that notifications can be conveyed through any form of communication, whether written, oral, or through technological means (i.e., email or phone). However, notification under the Proposed Rule does not change a bank's obligation to report appropriate incidents via SAR filings.

Service Provider Requirements

Entirely new in the Proposed Rule are regulatory obligations on banking service providers to notify their customers of triggering events. In the past, many service providers have such obligations imposed pursuant to contracts with their customers, but the specifics as to the timeframes and triggering events have been left to negotiations between the parties. The Proposed Rule would now impose an overarching obligation on these service providers to notify at least two individuals at affected banking organization customers immediately after experiencing a computer-security incident that it believes in good faith could disrupt, degrade, or impair services provided subject to the BSCA for four or more hours.

Bank services that are subject to the BSCA include check and deposit sorting and posting, computation and posting of interest and other credits and charges, preparation and mailing of checks, statements, notices, and similar items, or any other clerical, bookkeeping, accounting, statistical, or similar functions performed for a depository institution, data processing, back office services, and activities related to credit extensions (as well as components that underlie these activities).

In terms of the notification itself, the Proposed Rule provides that service providers would be required to make a best effort to share general information about what is known at the time. It further provides that regulators would enforce the service provider notification requirement directly against service providers and would not cite a bank because a service provider fails to comply.

Conclusion

If passed in its current form, the Proposed Rule would substantially increase the regulatory reporting obligations with which banking organizations must comply. This would be the first substantial update to a bank's responsibility to report a cyber incident in the last 15 years. Indeed, the Proposed Rule would subject financial institutions to some of the strictest incident reporting obligations currently in existence in the United States. Banks and banking service providers should continue to follow this Proposed Rule and be ready to review and update their incident response plans, business continuity and disaster recovery plans, and vendor

management programs to comply with these enhanced requirements. As always, these plans should be regularly tested (including through tabletop exercises) to ensure these institutions remain ready to quickly, effectively, and compliantly respond to an incident.

Comments on the Proposed Rule must be received within 90 days of its publication in the Federal Register.

If you have any questions regarding this Proposed Rule, or any other aspect of your incident response planning, please contact the authors Matt White, CIPP/US, CIPP/E, CIPM or Alex Koskey, CIPP/US, CIPP/E, or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.