Federal government issues new cybersecurity incident reporting rule for banks and bank service providers

James J. Giszczak, Dominic A. Paluzzi, Colin M. Battersby, Hussein Jaward, CIPP/US | Monday, November 22, 2021

On November 19, 2021, the federal government published a Final Rule ("Rule") imposing new cybersecurity incident notification obligations upon certain banks and bank service providers. Specifically, banking organizations covered by the Rule must give notice to their primary regulator as soon as possible and not later than *36 hours after determining certain cybersecurity incidents have occurred*, even if the banking organization is not aware of any unauthorized access of acquisition of sensitive customer information. Similarly, bank service providers also have a new notification obligation to their bank organization clients. Discussion of the Rule and how to prepare for it follows.

Banking organization guidelines

The Rule applies to certain banking organizations (collectively, “banks”) including:

- National banks
- Federal savings associations
- Federal branches and agencies of foreign banks
- U.S. bank holding companies and savings and loan holding companies
- State member banks
- U.S. operations of foreign banking organizations

- Edge and agreement corporations
- Insured state nonmember banks
- Insured state-licensed branches of foreign banks
- Insured state savings associations

The Rule does not apply to financial market utilities designated under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act.

The Rule requires banks to alert their primary federal regulator as soon as possible and no later than 36 hours after determining a notifiable computer security incident has occurred. A notifiable computer security incident is an occurrence that:

- 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; **AND** that has
- materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization'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 a 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.

The Rule offers several example incidents that would trigger notification obligations but note that these examples are not exhaustive. These incidents occur at large and small banks every day:

- 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 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 ransomware attack that encrypts a core banking system or backup data.

The Rule further stipulate that banks should err on the side of caution and notify regulators if there is any doubt as to whether a notifiable incident has occurred. While the primary regulator may require other means of notification, the Rule indicates a preference for submitting the required notification via e-mail or telephone to the applicable agencies' supervisory office or designated agency contacts. The notification does not have specific content requirements, but the government hints that it expects organizations to share all that is known about the incident at the time of notification. Notwithstanding the seemingly lax notification form requirements, McDonald Hopkins' experience suggests that any cybersecurity incident regulatory notification will invite additional government inquiries and scrutiny into the nature and scope of the incident.

Bank service provider guidelines

Bank service providers, or companies that perform services for some banks subject to the Bank Service Company Act (except for designated financial market utilities), also have new notification obligations under the Rule. The Rule requires a service provider to notify at least one bank-designated point of contact at an affected organization as soon as possible when the service provider determines it has experienced:

- an occurrence that 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

AND 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.

If the bank has not previously provided a bank-designated point of contact, such notification must be made to the bank's Chief Executive Officer and Chief Information Officer or two individuals of comparable responsibilities.

The purpose of such a notification is, in part, to allow notified banks to determine whether they in turn have their own notification obligations to satisfy, as described above.

The Rule's relationship with other laws, regulations, and contracts

Importantly, the Rule supplements but does not replace other data privacy and cybersecurity laws and regulatory requirements that banks and service providers are already subject to. These include obligations imposed by the Gramm-Bleach-Bliley Act, the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, state data breach notification and security laws, biometric information privacy laws, omnibus consumer privacy laws, and private contracts governing cybersecurity incident response. To illustrate this, when discussing service providers' obligations, the Rule explicitly recognizes that many service providers already have contractual notification obligations in place with their bank clients. As such, the Rule notes that the newly imposed obligations are wholly independent of any contractual notification obligations banks and their service providers already have in place and that service providers must comply with the new Rule even when existing contractual obligations differ from the Rule. The government would likely take the same position with respect to other laws and regulations previously mentioned, and not just private contracts.

The Ryke establishes yet another regulatory regime that business organizations—in this case, certain banks and service providers—are to be aware of in order to avoid liability associated with ever-increasing cybersecurity incidents. The Rule takes effect April 1, 2022, and banks and service providers must comply beginning the following month. McDonald Hopkins anticipates that additional state and federal regulations specifically targeting banks and their service providers' cybersecurity incident response practices are forthcoming.

Preparing to comply with the Rule

Banks and services providers should consider taking steps to begin to comply with the Rule. These steps include establishing or updating their Written Information Security Program (WISP), cybersecurity incident response plans, other information security policies and procedures, and contracts governing information security practices. Additionally, banks and services providers should also consider training employees on their Rule-compliance efforts.

Attorneys from McDonald Hopkins' national Data Privacy and Cybersecurity Practice Group are available to counsel banks and bank service providers on new and existing laws and regulations governing cybersecurity incident response.

James J. Giszczak

Dominic A. Paluzzi

Colin M. Battersby

Hussein Jaward, CIPP/US