CLIENT ALERTS & INSIGHTS

Federal Agencies Issue New Breach Notification Rules for Banking Organizations and Banking Service Providers

DECEMBER 22, 2021

Authors: Ryan T. Sulkin

Banking organizations must notify the appropriate agency within 36 hours of certain computer-security incidents; and banking service providers must notify affected banking organizations as soon as possible in the event of an equivalent incident.

In November, the Office of the Comptroller of the Currency ("**OCC**"), the Federal Reserve Board ("**FRB**"), and the Federal Deposit Insurance Corporation ("**FDIC**") issued a new rule placing certain breach notification standards on banking organizations and bank service providers.

Just as cybersecurity incidents continue to increase (such as the SolarWinds hack that resulted in recent lawsuits), the financial services industry continues to see an increased frequency cybersecurity incidents with increased severity.

In the past year, the federal government has taken a more active role in cybersecurity and created new avenues, such as aggressively enforcing cybersecurity standards and contractual requirements on government contractors, to hold bad actors accountable or provide new rules for entities to follow in response to cybersecurity incidents.

For example, the Federal Trade Commission ("**FTC**") recently amended the Safeguards rule to include new specific cybersecurity requirements that financial institutions must employ.

In this case, the new rule sets up notification requirements for severe cybersecurity incidents in the financial services industry. In the face of the new requirements, entities falling within the scope of the rule will likely have to implement robust cybersecurity monitoring systems that monitor for more than just incidents involving data breach, but that monitor the underlying functionality of Information Technology ("**IT**") systems.

According to the three agencies, the notification requirements will provide regulators with better (1) awareness of emerging, larger threats to financial systems; (2) assessments of the threats and risks posed by an incident as well as facilitate proper steps to mitigate the threat; (3) ability to provide banks with assistance through the U.S. Treasury Office of Cybersecurity and Critical Infrastructure Protection, (4) inform future guidance and adjust supervisory programs.

The rule takes effect on April 1, 2022 and entities must be fully compliant by May 1, 2022.

Scope and Applicability

The new rule applies specific notification requirements on both “banking organizations” and “banking service providers.”

While all three agencies have different definitions for what constitutes a “banking organization,” the rule will apply to most banks (or similar entities) operating in the U.S. The rule’s definition for “banking service providers” is also broad; likely covering any entity providing financial services to a bank.

First, which entities are considered banking organizations depends on which federal agency is their primary regulator. First, the OCC defines banking organization as national banks, federal savings associations, and federal branches and agencies of foreign banks. Second, FRB defines banking organizations as all U.S. bank holding companies, savings and loan holding companies, state member banks, U.S. operations of foreign banking organizations, and all Edge and agreement corporations. Finally, the FDIC defines banking organizations as all insured state nonmember banks, insured state-licensed branches of foreign banks, and insured State savings associations.

Second, an entity is considered a banking service provider if it performs “covered services.” The definition of both “banking service provider” and “covered services” is the same across all three agencies.

Covered services include any service that is subject to the Bank Service Company Act. Such services include-among other activities-check sorting; deposit sorting; calculating or posting of interest; and credits or charges, preparing and mailing checks, statements or other similar documents. Covered services also includes any other bookkeeping, accounting, or similar services that are performed for a bank.

Neither “banking organizations” or “banking service providers” include any designated financial market utility. Such entities include businesses that have been deemed systemically important under the Dodd-Frank Act. Designated financial market utilities are separately regulated by the Securities and Exchange Commission (“**SEC**”) or the Commodity Futures Trading Commission (“**CFTC**”).

The rule broadly applies to banks and related service providers. However, the notice requirements are only triggered in certain circumstances.

A “computer-security incident” includes any event that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that is processed, stored, or transmitted on such system. This covers a broad range of potential incidents. However, notification is only required in severe incidents, or as the rule indicates, when a computer-security incident rises to the level of being considered a notification incident.

For a computer-security incident to rise to level of requiring notification (i.e., a notification incident) the event must either (1) materially disrupt or degrade a banking organization; or (2) be reasonably likely to materially disrupt or degrade a banking organization.

Material disruptions or degradations include any events that materially affect a banking organization’s (1) ability to operate, process, or deliver banking products and services to a material portion of their customers; (2) operations and services that upon failure would result in material loss of revenue, profit, or franchise value; or (3) operations and services that upon failure would pose a threat to the financial stability of the U.S.

In sum, while the rule will broadly apply to a number of entities, the obligations imposed by the new rule are only triggered by a subset of cybersecurity related incidents. However, entities within the scope of the rule will need to be monitoring the broad swath of cybersecurity related incidents that occur in order to determine whether they rise to a level necessitating notification.

Notification Requirements

The new rule creates two new notification requirements; one for banking organizations and another for banking service providers.

First, banking organizations must notify their primary federal regulator within 36 hours of determining a computer-security incident rises to the level of a notification incident.

Second, banking service providers must notify each affected banking organization customer, through at least one customer-designated contact, as soon as possible once the banking service provider determines they have suffered a computer-security incident that will materially dispute or degrade covered services for four or more hours.

If the banking organization customer has not previously provided a contact, the banking service provider must notify the banking organization's CEO and CIO (or those in comparable positions) through any reasonable means.

The banking service provider notification requirement does not apply to scheduled maintenance, testing, or updates that was previously communicated to a banking organization customer.

Practical Effects

Importantly, the scope of what is considered a "cybersecurity incident" is broader than what other laws-including U.S. state breach notification laws-impose on entities.

Traditional breach notification requirements apply to unauthorized access and disclosure of data. Here, the rule applies to potential IT system disruptions or access to the underlying IT systems. Therefore, new rule applies to far more than actual unauthorized access or disclosure of data.

That means entities within the scope of the rule will need to potentially expand their cybersecurity monitoring systems to track all cybersecurity incidents. These robust monitoring systems will need to track all disruptions to the underlying functionality of the IT systems. While the definition of a notification incident is narrow and specific, an entity will not be able to properly determine whether an incident rises to such a level unless they can track and monitor for all incidents.

Because entities are facing increased cybersecurity risks, the new rule's broad definition of "cybersecurity incident" will require entities falling within the scope of the rule to review their cybersecurity monitoring systems and account for the new notification requirements in their policies and procedures.

As compliance with new breach notification rules and regulations come into effect at both the state and federal level, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Ryan T. Sulkin at rsulkin@beneschlaw.com or 312.624.6398.

Lucas Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.