GreenbergTraurig

Alert | Data, Privacy & Cybersecurity

January 2022

Federal Banking Regulators Issue 36-Hour Cybersecurity Breach Notification Requirement

This GT Alert covers the following:

- Multiple bank regulators have issued a final rule providing for a 36-hour regulatory breach notification requirement.
- This is the shortest breach notification requirement in the United States.
- The Rule does not apply to all data security incidents, just incidents that “materially disrupt or degrade.”
- Rule takes effect in April 2022.

Beginning in April 2022, banking organizations and bank service providers will be subject to the shortest regulatory breach notification reporting time frame of any law to date – 36 hours.

The Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (Board), and the Office of the Comptroller of the Currency (OCC) (collectively, the “Agencies”) have issued a final rule to establish cybersecurity breach notification requirements for banking organizations and bank service providers (Rule).

The Rule contains a 36-hour regulatory notification requirement for incidents that rise to the level of "notification events." This timeline is shorter than any U.S. state data breach notification law and surpasses even the tightest time frame on U.S. books – 72 hours under the New York State Department of Financial Services and certain state insurance laws. Banking organizations will need to act quickly to make notifications to their primary regulators once they determine a "Notification Event" has taken place.

While the timeline is constricted, the clock doesn't start until the banking organization "determines that a notification incident has occurred." This contrasts with other breach notification laws that set timeframes based on when an organization becomes aware of an incident. In the summary of the Rule, the Agencies stated that they anticipate banking organizations will take "a reasonable amount of time" to determine whether a Notification Event has occurred, and the 36-hour time frame will begin only after such determination has been made.

Additionally, the Rule also makes clear that not every data security incident is a Notification Event. "Notification Events" are computer security events that materially disrupt or degrade, or are 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 discontinuation of which would pose a threat to the financial stability of the United States.

The Agencies have also provided a list of examples of likely notification events, which include:

- Large-scale distributed denial of service (DDOS) attacks (*see* December 2021 Data Privacy Dish blog post) that disrupt customer account access for an extended period of time (e.g., more than four hours).
- A bank service provider used by a banking organization for its core banking platform to operate business applications experiencing a widespread system outage, and recovery time is undeterminable.
- A failed system upgrade or change that results in widespread user outages for customers and banking organization employees.
- An unrecoverable system failure that results in activation of a banking organization's business continuity or disaster recovery plan.
- A computer hacking incident that disables banking operations for an extended period of time.
- Malware on a banking organization's network that poses an imminent threat to the banking organization's core business lines or critical operations or that requires the banking organization to disengage any compromised products or information systems that support the banking organization's core business lines or critical operations from internet-based network connections; and
- A ransom malware attack that encrypts a core banking system or backup data.

The definition of Notification Event and the provided examples indicate the Agencies are targeting the type of security incidents with a significant impact on banking operations and are not focusing on less threatening incidents. The inclusion of ransomware attacks, regardless of how long encryption lasts, as a type of Notification Event is significant, given the rise in such incidents over the last few years.

In addition to this notification for banking organizations, the Rule also obligates bank service providers to notify "at least one bank designated point of contact at each affected banking organization customer" as soon as possible once 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, its covered services for four hours or more. A computer-security incident is defined more broadly than a Notification Event to include any 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.

The Rule takes effect April 1, 2022, with full compliance required by May 1, 2022. Banking organizations and bank service providers should begin reviewing their incident response and business continuity plans now to ensure compliance.

Authors

This GT Alert was prepared by:

- Jena M. Valdetero | +1 312.456.1025 | valdeteroj@gtlaw.com
- Jessica D. Pedersen | +1 312.456.1001 | pedersenj@gtlaw.com

Albany. Amsterdam. Atlanta. Austin. Boston. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Germany.¬ Houston. Las Vegas. London.* Los Angeles. Mexico City.+ Miami. Milan.» Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Sacramento. Salt Lake City. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv.^ Tokyo.¤ Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.

*This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. ¬Greenberg Traurig's Berlin office is operated by Greenberg Traurig Germany, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. *Operates as a separate UK registered legal entity. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. »Greenberg Traurig's Milan office is operated by Greenberg Traurig Santa Maria, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ∞Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. ¤Greenberg Traurig's Tokyo Office is operated by GT Tokyo Horitsu Jimusho and Greenberg Traurig Gaikokuhojimubengoshi Jimusho, affiliates of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ~Greenberg Traurig's Warsaw office is operated by GREENBERG TRAURIG Nowakowska-Zimoch Wysokiński sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in GREENBERG TRAURIG Nowakowska-Zimoch Wysokiński sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2022 Greenberg Traurig, LLP. All rights reserved.*