Published on *The National Law Review* https://natlawreview.com

Federal Data Breach Reporting Requirements Continue to Evolve

Article By:

Scott Ferber

Mark E. Schreiber

Cathy Lee

OVERVIEW

Complementing the patchwork of state data breach notification laws, a number of federal agencies recently have promulgated sector-specific reporting rules affecting a variety of companies, both directly and indirectly, with varying definitions of triggering incident and requirements on submission content. These include:

- Effective April 1, 2022, with a compliance date of May 1, 2022, **federally regulated banking organizations** must notify their primary federal regulator of any "computer-security incident" that rises to the level of a "notification incident"[1] within **36 hours** after the banking organization determines that an incident has occurred. In addition, federally regulated bank service providers must notify each affected bank organizations of such an incident "as soon as possible" after determining it has experienced such an incident.

- Effective December 31, 2021, **covered freight railroads, passenger rail and rail transit systems** must report a "cybersecurity incident"[2] to the US Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) within **24 hours** of identifying a covered incident.

- Effective September 15, 2021, **health apps and connected devices that collect or use consumers' health information** must notify affected consumers when their health data is breached,[3] as well as the Federal Trade Commission (FTC), within **60 days** of discovering the incident.

- Effective May 28, 2021, **designated critical pipeline owners and operators** must report a "cybersecurity incident"[4] to CISA within **12 hours** of incident identification.

In addition, President Joe Biden's May 12, 2021, Executive Order on Improving the Nation's Cybersecurity (14028) contains provisions that could affect data breach reporting requirements for Information Technology (IT), Operational Technology (OT) and Information and Communications Technology (ICT) service providers providing such services to the federal government. The Executive Order provides that:

- Within 60 days of the Executive Order's date, the Director of the Office of Management and Budget (OMB), in consultation with the Secretary of Defense, Attorney General, Secretary of Homeland Security and Director of National Intelligence, shall review the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement contract requirements and language for contracting with IT and OT service providers and recommend updates to such requirements and language to the FAR Council and other appropriate agencies. This includes recommending contract language designed to ensure appropriate reporting of cyber incidents and potential incidents relevant to any agency with which an IT/OT service provider has contracted—directly with such agency, as well as any other agency deemed appropriate.[5]

- Within 45 days of the Executive Order's date, the Secretary of Homeland Security, in consultation with the Secretary of Defense acting through the Director of the National Security Agency (NSA), the Attorney General, and the Director of OMB, shall recommend to the FAR Council contract language that identifies, among other things, the time periods within which ICT service providers must report cyber incidents[6] to the contracting federal agencies. The reporting timeline is to be based on a graduated scale of severity, **with reporting on the most severe cyber incidents not to exceed three days after initial detection**.[7]

Congress also has been considering a variety of data breach notification bills. For example, the National Defense Authorization Act (NDAA) had contained a provision that would have required critical infrastructure companies to report "cyber incidents" to CISA within 24 or 72 hours, but that provision did not survive the legislative process.

Based on the above, as well as other measures and messaging from the federal government, ever-increasing cybersecurity oversight of the private sector seems inevitable. The recent rules are also expected to have a cascading effect on other industries. For example, many of the companies covered by the recent rules provide products and services to—and receive products and services from—an array of other companies. The expectation for timely reporting of data breaches—at the very least contractually—is likely to accelerate greatly.

Facing this shifting landscape, it is important for organizations, regardless of sector, to take a fresh look at their cybersecurity programs, including breach reporting and incident response, and third-party contractual arrangements to ensure they are in harmony with these rising expectations and increasing obligations.

---

[1] Under the federal banking data breach notification rule, a "computer-security incident" is defined 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." *See* 12 C.F.R.

§ 53.2(b)(4); 12 C.F.R. § 225.301(b)(4); 12 C.F.R. § 304.22(b)(4). A "notification incident" is "a computer-security incident that has material disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's – (i) 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; (ii) 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 (iii) 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." *See* 12 C.F.R. § 53.2(b)(7); 12 C.F.R. § 225.301(b)(7); 12 C.F.R. § 304.22(b)(7).

[2] The rail system Security Directives broadly define a "cybersecurity incident" to mean an unauthorized event that "jeopardizes, disrupts or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system." A covered cybersecurity incident includes an event that is under investigation as a possible cybersecurity incident without final determination of the event's root cause or nature (such as malicious, suspicious or benign).

[3] Under the FTC's Health Breach Notification Rule, "breach of security" means "with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information without the authorization of the individual. Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information." 16 CFR § 318.2(a).

[4] The critical pipeline Security Directive broadly defines a "cybersecurity incident" to mean "an event that, without lawful authority, actually, imminently, or potentially jeopardizes, disrupts or otherwise impacts the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system." This includes an event that: "(1). Is under investigation as a possible cybersecurity incident without successful determination of the event's root cause or nature (such as malicious, suspicious, benign); and (2). May affect the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system."

[5] EO 14028 § 2(b). Within 90 days of receipt of such recommendations, the FAR Council shall review the proposed contract language and conditions and, as appropriate, shall publish for public comment proposed updates to the FAR. *Id*. at § 2(d).

[6] Covered incidents are those involving a software product or service provided to the agencies or involving a support system for a software product or service provided to such agencies. *Id*. at § 2(g)(i)(D).

[7] *Id*. (emphasis added).

National Law Review, Volume XI, Number 343

Source URL:https://natlawreview.com/article/federal-data-breach-reporting-requirements-continue-to-evolve