March 22, 2022

Expansive Federal Breach Reporting Requirement Becomes Law

Attorneys
Fran Faircloth
Edward R. McNicholas
Kevin J. Angle

On March 15, 2022, President Biden signed into law significant new federal data breach reporting legislation that could vastly expand data breach notice requirements far beyond regulated entities or entities processing personal data. Unceremoniously tucked as Division Y into the H.R. 2471 Consolidated Appropriations Act, 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) will require "covered entities" — organizations in certain critical infrastructure sectors—to report substantial cybersecurity incidents to the Department of Homeland Security within 72 hours after the organization reasonably believes the cyber-incident has occurred. Covered entities will also be required to report ransom payments within 24 hours of making a payment in response to a ransomware attack.

Forthcoming rulemaking by the Critical Infrastructure Security Agency (CISA) with the Department of Homeland Security (DHS) will materially define the scope of these requirements, including the scope of "covered entities" required to report, the definition of a "substantial" cybersecurity incident triggering the requirement, and the information that must be conveyed in any report to CISA. The reporting requirement extends to substantial cyber incidents impacting business and industrial operations as well as losses of the confidentiality, integrity, or availability of information systems and is not limited to data breaches affecting personal data. As such, CIRCIA will significantly expand the breadth of data breach reporting requirements across sectors for many commercial enterprises that have not focused on consumer privacy issues. Regardless of the rulemaking, a core requirement will remain: "A covered entity that experiences a covered cyber incident shall report the covered cyber incident to the [CISA] not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred."

Late last year, legislative proposals to require breach reporting at the federal level advanced in both the House and Senate to require breach reporting at the federal level either to CISA, the FBI, or both. No compromise was reached, however, which deferred the issue until this year. CIRCIA essentially adopts the prior House approach, requiring incident reporting to CISA by covered entities within critical infrastructure sectors. While the law was criticized by FBI Director Christopher Wray and Deputy Attorney General Lisa Monaco for shifting cyber-focus from the DOJ/FBI to DHS/CISA, CISA Director Jen Easterly praised its passage, calling it a "game-changer" that will give CISA a new tool to help "build a common understanding of how our adversaries are targeting U.S. networks and critical infrastructure." The new requirements have the potential to improve the flow of cyber threat information to the federal government, but they will also increase the burden on organizations struggling to rapidly respond to a criminal attack on their systems.

New Reporting Requirements, Many Details Still to Come

CIRCIA will require breach reporting by covered entities in critical infrastructure sectors within 72 hours for substantial cybersecurity incidents and a remarkably short 24 hours after payment of a ransom in response to a ransomware attack. Critical infrastructure sectors cover a very wide range of businesses, from the chemical or national security sectors, to financial services, to health care, critical manufacturing, and information technology. Not all organizations in these sectors, though, will be required to report, as the law does allow an exemption for "a covered entity required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe." The scope of covered entities and such exemptions will be determined through rulemaking by the Director of CISA (the "Director").

The law requires reporting by covered entities in two circumstances: First, covered entities will be required to report a "covered cyber incident" to the DHS within 72 hours of establishing a reasonable belief that such an incident has occurred. A "covered cyber incident" is defined generally as a "substantial" cyber incident, but the law gives the Director

rulemaking authority to further delineate the term's parameters. Notably, a covered cyber incident is not limited to incidents in which personal data is compromised, as with various state breach reporting laws, and will likely include a wide variety of attacks, such as ransomware, other sensitive information leaks, and, possibly, newly exploited vulnerabilities.

CIRCIA will also require reporting in the event that a covered entity makes a ransom payment as a result of a ransomware attack. The clock for such notification will run even faster, requiring notification to DHS no later than 24 hours after the payment is made. Of course, the timing for both reporting requirements is substantially shorter than under typical state notification laws, which generally require notice "without unreasonable delay" or within periods such as 30 to 45 days or longer. The notice period is broadly consistent with expedited time frames under the EU's GDPR (72 hours), the New York Department of Financial Services Cybersecurity Regulation (72 hours), and the SEC's newly proposed risk management rules for registered funds and advisers (48 hours). In addition to required reports, covered entities are also encouraged to make voluntary reports to CISA about incidents that do not meet the threshold reporting requirements spelled out in the CISA rules. These voluntary reports will receive the same protections from disclosure as mandatory notifications, described below.

Many of the specifics of the reporting requirements are subject to further rulemaking. The law does not stipulate, for example, what information will be required within any breach report, leaving those details to be fleshed out by the Director. It does state that the Director's rulemaking must include reporting of information such as the systems impacted, a description of the unauthorized access or other event, an estimated data range surrounding the incident, and the attack's impact on the operations of the covered entity. Whatever the details, covered entities will be required to update or supplement a previously submitted report if substantial new or different information becomes available until the covered entity reports that it has determined that the incident has been fully mitigated and resolved.

In addition to reporting the covered cyber incident or ransom payment, CIRCIA will also require the covered entity to preserve data "relevant" to the covered cyber incident or ransom payment. Again, rulemaking by the Director will be required to further define what data is or is not considered "relevant," but even with more specific rules, covered entities will likely be forced to make key decisions about preservation early in the process of responding to an incident.

Information Sharing and Enforcement

The law will require that DHS share certain information about threat indicators and security vulnerabilities disclosed through breach notifications; however, CIRCIA contains limitations regarding the confidentiality of the information and the privacy of individuals. Regulators will generally be prohibited from using information submitted to DHS through the new reporting procedures in any regulatory action, and the law includes protections against waiver of the attorney-client privilege, trade secret, or other protections that could otherwise result from submission of breach reports. The law establishes liability protections surrounding submission of the reports and restricts from discovery communications or materials created solely for the purpose of drafting or submitting such reports—a restriction whose boundaries creative plaintiffs' attorneys are likely to push.

One critical exception to these protections, though, exists if an organization fails to timely report and subsequently fails to cooperate with requests for information made by the Director. At that point, the Director is authorized to issue a subpoena and refer any information received pursuant to the subpoena to the Attorney General or another appropriate regulatory authority to pursue a civil action in federal court to obtain the information subject to potential contempt of court for a failure to provide information. Accordingly, while CIRCIA does not provide direct penalties for non-compliance, it nevertheless does incentivize timely reporting and cooperation through the threat of waiver of some of its liability shielding measures in the event of noncompliance. The law also does not appear to limit any securities, derivative, commercial, or consumer actions based on the underlying data breach itself.

Looking Ahead

There remain numerous details in CIRCIA that require further rulemaking. Among these details are fundamental questions such as which organizations will be required to comply. At this time, we know covered entities will be chosen from the sectors deemed critical under Presidential Policy Directive 21, but the Director will have the ability to further refine the scope of reporting entities. The final rules will also cover, among other things

- The definition of a covered cyber incident requiring reporting;
- The information that must be included in an incident report;
- The types of data that must be preserved, the length of time it must be preserved, and allowable uses for the data;
- Deadlines and other criteria for submitting incident reports;
- Procedures for third parties to submit reports; and
- Other procedural measures necessary to implement the reporting requirements.

Timing

CIRCIA affords the Director up to 24 months from the date of enactment to publish a notice of proposed rulemaking covering these topics, after consulting with other federal agencies including the Department of Justice. Any rule will become final no later than 18 months thereafter. This means that it will likely be several years before there are clear rules, and this clarity will likely come after both the mid-term and presidential elections. CIRCIA's breach reporting requirement will become effective on a date prescribed in these final rules.

* * *

If you would like to learn more about the issues in this Alert, please contact your usual Ropes & Gray attorney contacts.