CADWALADER

Cabinet **News and Views**

Informed analysis for the financial services industry

Strengthening Cybersecurity Notification Requirements

By **Keith M. Gerver**
Associate | White Collar Defense and Investigations

Last week, the U.S. Senate passed S. 3600, the Strengthening American Cybersecurity Act, which represents a significant step forward in the establishment of a national data breach notification law for certain critical infrastructure businesses and marks, for the first time, that businesses will be required to report when they have made ransomware payments.

Here are five key takeaways from the bill:

- Under the bill, a "covered entity" will be required to report certain cyber incidents they experience to the Cybersecurity and Infrastructure Security Agency ("CISA") within 72 hours of when the "covered entity reasonably believes that the covered cyber incident has occurred," and any ransom payments they make as a result of a ransomware attack not later than 24 hours after the payment has been made.

- The bill delegates to the CISA Director the responsibility to determine via notice-and-comment rulemaking which businesses in any of the 16 critical infrastructure sectors identified in Presidential Policy Directive 21 (to include, among others, commercial facilities, financial services, and healthcare and public health) are covered entities.

- Only "*substantial* cyber incidents" must be reported, and the bill delegates to the CISA Director the responsibility to define via rulemaking what those incidents are. At a minimum, they must be cyber incidents that *actually* jeopardize information on information systems or the systems themselves.

- If the CISA Director has reason to believe that a covered entity has failed to make a required report and has not responded (or responded adequately) to a request for information, the bill gives them the authority to issue a subpoena to compel disclosure. If the covered entity does not respond to the subpoena, then the CISA Director may refer the matter to the Attorney

General to bring a civil action to enforce it.

- Covered entities that submit required reports enjoy liability protection from any action brought against the covered entity solely based on the submission of a required report.

The House of Representatives attempted, but failed, to include similar language in the annual defense authorization bill that it passed in December 2021. Nevertheless, after years of discussion and debate over the creation of a mandatory federal data breach reporting regime, the volume and tempo of cyberattacks against critical infrastructure businesses appears finally to have reached a level where opposition in private industry has significantly softened. We should expect to see legislation signed into law this year.
