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

24 Hours: Government Likely to Require Notice of Ransomware Payments from Banks, Other Key Businesses

Article By:

Micah J. Fincher

Most banks and their service providers are familiar with the final rule governing notice for "notification incidents" and "cyber security incidents." With compliance due by May 1, 2022, the rule establishes standards and deadlines for service providers to notify banks of such incidents and for banks to notify their primary federal regulator "as soon as possible and no later than 36 hours" after the bank "determines" that a notification incident has occurred. (For more, see this summary.) However, a recently enacted law requiring new rulemaking by the Cybersecurity and Infrastructure Security Agency (or CISA for short) within the Department of Homeland Security could upend a key compromise made during the finalization of the banking rules.

On March 15, 2022, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (the Act). Subject to rulemaking likely to be finalized in 2024 or 2025, in general the Act will require "covered entities" to notify the CISA within 72 hours that it "reasonably believes" that a "covered cyber incident" has occurred and within 24 hours of any ransomware payment. CISA must publish proposed rules by or before March 15, 2024, and issue a final rule 18 months thereafter (i.e., by or before September 15, 2025, at the latest). Most of the Act's provisions go into effect only when the final rule is issued. Banking organizations should encourage their primary federal regulators to enter into agency agreements with CISA and study the CISA's proposed rules to ensure they qualify for the Act's exemptions.

Since the Act requires rulemaking to define "covered entity," it remains to be seen whether banking organizations will be included, but there is good reason to believe they will. Congress provided guidelines for the definition of "covered entity" based on the likelihood the entity "may be targeted by a malicious cyber actor," whether the compromise of the entity "will likely enable the disruption of the reliable operation of critical infrastructure," and the "consequences" of such compromise to "national security, economic security, or public health and safety." The Act also cites Presidential Policy Directive 21, which identifies "financial services" among 16 critical infrastructure sectors and designates the Department of the Treasury as its "Sector-Specific Agency." Banks and other financial service providers are therefore likely to be included in the definition of "covered entity," because they are frequently targeted by cyber criminals and their compromise could disrupt the critical infrastructure of the financial sector with adverse consequences to national and economic security.

While “covered cyber incident” must also be defined by rulemaking, the Act does define “ransom payment” and the types of ransom information that must be submitted to CISA within 24 hours of payment. “Ransom payment” is defined to include payments in cash, bitcoin, or other “virtual currency” that “has at any time been delivered as ransom in connection with a ransomware attack.” Within 24 hours of a ransom payment, the Act requires the following types of information to be submitted to the CISA:

1. A description of the ransomware attack, including the estimated date range of the attack, and the date of the ransom payment. Where applicable, the description should include the vulnerabilities, tactics, techniques, and procedures used to perpetrate the ransomware attack.

2. The name and identifying information of the covered entity that made the ransom payment (or on whose behalf the payment was made) with contact information that the CISA may use to contact the covered entity or its service provider.

3. Where applicable, any identifying or contact information related to the actor or actors reasonably believed to be responsible for the ransomware attack.

4. The ransom payment demand, including the type of virtual currency or other commodity requested, if applicable, and the ransom payment instructions, including information regarding where to send the payment, such as the virtual currency address or physical address to which the funds were requested to be sent, if applicable.

The Act includes certain exemptions. It requires other federal agencies to share with the CISA reports of cyber incidents, including ransom payments, within 24 hours of when they receive the report. So it provides an exemption for covered entities that are “required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe,” subject to certain requirements. That raises the question of whether existing rules for banks to notify their primary federal regulator of “notification incidents” within 36 hours would qualify as “substantially similar information” and a “substantially similar timeframe,” as required by the Act.

There are good reasons to believe the bank rules on notification incidents may not qualify in their current form. For example, incident notifications by banks do not require the ransom payment details required by the Act, although regulators could expressly ask for such information. The banking rules and Act also differ on how to calculate the time for incident notifications. Notably, in the course of finalizing the bank rule on notification incidents, regulators replaced a “good faith belief” notification standard of the proposed rule with a “determination” standard in the final rule. In other words, under the final rule, the 36-hour deadline for banking organizations to notify their primary federal regulator begins to run from when they “determine” that a notification incident has occurred, rather than merely having a “good faith belief.” The new law, by contrast, uses a “reasonable belief” standard: notification is required “not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.”

Ultimately, CISA will determine whether the bank rule on notification incidents requires “substantially similar information” in a “substantially similar timeframe.” That is because the Act’s exemption for entities that already have federal reporting obligations applies only when the CISA and the other federal agency have entered into a written agency agreement “to establish policies, processes, procedures, and mechanisms to ensure reports are shared with the [CISA]” as required by the Act. Without an agency agreement with the CISA, the entities regulated by the other federal agency

cannot qualify for the exemption.

The Act could also impact bank service providers. In addition to notification obligations they already have under banking rules, if the provider makes a ransom payment on behalf of a covered entity, then the Act requires the provider to “advise” the covered entity of its responsibility to report the payment. The Act also allows such service providers to provide such notification on behalf of the covered entity.

The Act’s principal enforcement mechanism is subpoena power granted to the CISA. If a covered entity fails to respond to the subpoena within 72 hours, the CISA may refer the matter to the Department of Justice to bring a civil action enforcing the subpoena. Continued non-compliance could result in civil contempt or sanctions, as in any other civil matter, to enforce a subpoena.

In summary, banking organizations should encourage their primary federal regulators to enter into agency agreements with CISA and study the CISA’s proposed rules to ensure they qualify for the exemption under the Act. An exemption will help avoid situations where banking organizations would otherwise be required to notify and coordinate with multiple federal agencies with differing rules while responding to a cyber incident.

National Law Review, Volumess XII, Number 118