Hughes Hubbard & Reed

Recent Developments – U.S. Data Breach Reporting Obligations

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

June 29, 2022 – In the past few months, the United States has strengthened requirements on businesses and banks to report or disclose data breaches. Recent developments include: (1) President Biden's signing of the Cyber Incident Reporting for Critical Infrastructure Act; (2) the Securities and Exchange Commission proposing new rules to enhance cybersecurity incident reporting and risk management; (3) federal banking regulators issuing a new rule requiring banking organizations and their service providers to report computer-security incidents; and (4) the Federal Trade Commission confirming that there is a de facto data breach notification requirement in the FTC Act.

Background

The United States does not have a national data breach notification law. At the federal level, there are some sector-specific laws that contain data breach notification requirements, such as the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which protects personal health information. HIPAA requires covered entities and their business associates to notify affected individuals of a data breach without unreasonable delay and in no case later than sixty days following discovery of the breach.

At the state level, all fifty states have data breach notification laws. These laws vary from state to state but each state's law generally protects that state's residents when their personal data is compromised in a data breach. Companies that suffer a data breach often have to comply with multiple state laws and, in particularly large data breaches, companies may have to send notices to affected individuals in nearly every U.S. state. Moreover, in addition to notifying affected individuals of a data breach, some state laws also require notice to the state attorney general's office or other authorities.

The Cyber Incident Reporting for Critical Infrastructure Act

On March 15, 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA"), which will impose reporting requirements on critical infrastructure providers. The Cybersecurity &

Infrastructure Security Agency ("CISA") must publish a Notice of Proposed Rulemaking within 24 months of CIRCIA's enactment and adopt final rules within another 18 months. Only then will CIRCIA's reporting obligations become effective.

CIRCIA's central reporting obligation will require "covered entities" to report "substantial" cyber incidents to CISA (but not to affected individuals) within 72 hours and to report payments made in response to ransomware attacks within 24 hours. "Covered entities," which will be further defined in the rulemaking, are entities falling into one or more of the sixteen "critical infrastructure sectors" defined in Presidential Policy Directive 21 (Critical Infrastructure Security and Resilience). These include chemicals, commercial facilities, communications, critical manufacturing, energy, financial services, healthcare, and information technology.

Covered entities will be required to report to CISA when (i) a cyber incident leads to substantial loss of confidentiality, integrity or availability of an information system or network or a serious impact on the safety and resiliency of operational systems and processes; (ii) business or industrial operations are disrupted by, among other incidents, a denial of service attack, a ransomware attack, or the exploitation of a zero day vulnerability (i.e., a vulnerability that has been disclosed but not yet patched); or (iii) the unauthorized access or disruption of business operations is due to loss of service facilitated through, or caused by a compromise of, a cloud service provider, managed service provider or other third-party data hosting provider, or caused by a supply chain compromise.

In making reports to CISA, covered entities will need to describe, among other things, the vulnerabilities that were exploited, the estimated date range of the incident, the impact on operations, and the categories of information accessed or acquired. In the case of ransomware incidents, information relating to the demanded payment will also need to be reported. Covered entities will need to submit prompt updates if substantial new or different information becomes available or if they make a ransom payment after submitting a report.

CISA will be required to review the reports to determine whether the incidents are connected to an ongoing cyber threat or security vulnerability and to use the reports, as appropriate, to identify, develop and disseminate anonymized cyber threat information and defensive measures. Notably, CIRCIA includes provisions restricting CISA from disseminating any personally identifiable information and protecting against the loss of trade secrets and attorney-client privilege. In addition, the reports that covered entities submit to CISA will be exempt from requests under the Freedom of Information Act.

CIRCIA will prohibit persons or entities from bringing lawsuits against a covered entity based solely on the covered entity's submission of a required report. However, the Act will permit lawsuits when the cyber incident is discovered through other means. If a covered entity fails to submit a mandatory report, CIRCIA will authorize CISA to send "requests for information" and, if the company fails to comply within 72 hours, subpoenas. Based on the information that it obtains, CISA may refer the matter to the Department of Justice for investigation and enforcement.

SEC Proposals

On March 9, 2022, the Securities and Exchange Commission (the "SEC") proposed rules and amendments to enhance and standardize cybersecurity incident reporting and risk management by public companies. The public comment period has now closed, although the rules have yet to be finalized and take effect.

In regard to reporting, the SEC proposes requiring public companies to disclose information on material cybersecurity incidents within four business days after determining that they have experienced such an incident. The SEC proposal would also require companies to update prior disclosures and report immaterial cybersecurity incidents that become material in the aggregate.

During the public comment period, companies and law firms criticized the four-day reporting requirement, advocating for more time to investigate an incident before having to report to investors and the public. The public commenters argued that premature reporting of incidents before all the facts are known can tip off hackers, interfere with law enforcement efforts and encourage lawsuits, particularly if the company's early statements turn out to be inaccurate.

In addition to reporting incidents, the SEC also proposes requiring companies to disclose their policies and procedures, if any, for identifying and managing cybersecurity risks. This would include disclosures regarding the board's oversight of cybersecurity risk and management's role and expertise in assessing and managing cybersecurity risk and implementing the company's cybersecurity policies.

Final Rule on Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers

U.S. banking regulators – including the Federal Deposit Insurance Corporation (the "FDIC"), the Office of the Comptroller of the Currency (the "OCC") and the Federal Reserve Board (the "FRB") – issued a Final Rule on Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers (the "Final Rule"), which became effective on April 1, 2022 and required compliance by May 1, 2022.

The Final Rule requires a banking organization to notify its regulatory authority of a "notification incident" "as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred." A "notification 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 and that has resulted or is reasonably likely to result in a material disruption to or degradation of a banking organization's (1) 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; (2) business line(s), the failure of which would result in a material loss of revenue, profit or franchise value; or (3) operations, the failure or discontinuance of which would pose a threat to the financial stability of the United States.

The Final Rule also applies to a banking organization's service providers, which are required to notify each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced 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 and that has resulted or is reasonably likely to result in a material disruption to or degradation of covered services for four or more hours.

The Federal Trade Commission's Confirmation of an Implicit Data Breach Notification Requirement in the FTC Act

On May 20, 2022, the Federal Trade Commission (the "FTC") confirmed its position that the FTC Act, which protects consumers from deceptive and unfair business practices, imposes a de facto requirement on businesses to provide notice of data breaches to affected consumers in a timely manner.

In its statement, the FTC cited recent actions it had taken against CafePress, SkyFone, SkyMed, and Uber alleging a failure to provide timely or adequate notices of data breaches. For example, the FTC alleged that Uber's statement that it would reasonably secure personal information was deceptive in light of Uber's alleged failure to provide notice of a data breach to affected consumers for more than a year.

Conclusion

Companies with an existing cybersecurity incident response plan should consider what updates, if any, should be made in light of these developments. A response plan should be prepared if one does not already exist. When a data breach occurs, a company needs to act quickly to identify and contain the attack, ensure business continuity, and comply with legal requirements. A good response plan ensures that this happens, helps avoid expensive mistakes, and protects the company from potential liability.

Related People

Seth D. Rothman

Kevin T. Carroll

Paul Marston

Related Areas of Focus

Data Privacy & Cybersecurity