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

Tech Transactions & Data Privacy 2022 Report: Ransomware Reporting Requirements: A Look Forward into Evolving Security Incident Notification Rules

Article By:

Michael J. Waters

Colin H. Black

Tech Transactions & Data Privacy 2022 Report

Data breach notification laws in the United States have historically focused on notifying individuals, regulators and others in situations in which personal information has been accessed or acquired. Ransomware attacks, while incredibly disruptive, do not always involve data access or acquisition and, as such, are not always reported. As ransomware attacks increase in frequency and the severity of their impact, both law enforcement and industry regulators are seeking greater visibility into these incidents and, through the publication of new guidance and the amendment of notification laws, are starting to require increased reporting.

How Does Ransomware Work?

Ransomware refers to a particular kind of malicious software that utilizes encryption to limit access to the contents of an impacted device until payment is made to the threat actor in exchange for a decryption key.

Encryption is a legitimate utility for data security and works by transforming plaintext into ciphertext using an algorithm that generally has a single known solution. The ciphertext can only be converted back to plaintext by using the solution, often referred to as a decryption key. When used responsibly, encryption is an excellent way to protect the confidentiality of data both at rest and in transit.

Oftentimes, ransomware is not a highly complex malware; in some instances, a ransomware attack can even be achieved by leveraging built-in encryption utilities such as BitLocker. The simplistic and often legitimate uses for encryption software make ransomware extraordinarily difficult to detect until it is too late. Furthermore, threat actors are constantly exploring new attack vectors, making complete protection impossible.

State Breach Notification Laws

By default, all entities domiciled in the United States are subject to state privacy laws. California passed the first data breach notification law in 2003, and since then, every state in the U.S. has adopted its own breach notification statute. Furthermore, the applicability of each state privacy law is based not on the domicile on the entity but rather on the domicile of the impacted data subject. Thus, an entity that is domiciled in California but holds data on individuals all over the United States will generally be subject to the state privacy law in each state where an impacted individual is domiciled.

While the trigger for notification will vary from state to state, all state data breach notification statutes contain requirements that impacted individuals be notified in a manner consistent with the forum state's notice rules. In addition to notice to impacted individuals, many states also require notice to state Attorneys General, consumer credit reporting agencies (e.g., Experian, TransUnion, and Equifax), and law enforcement.

The mere fact that a ransomware incident has occurred does not necessarily trigger a notice obligation pursuant to state breach notification laws. Rather, most states require either the actual access to or exfiltration of personal information. By contrast, the automated encryption of data will not generally trigger a notification obligation in and of itself.

Sectoral Privacy Regulations

Privacy regulation in the U.S. is based on a sectoral model; simply put, different rules may apply depending on the industry in which the impacted entity operates. Sectoral regulations exist at both the state and federal levels as well as in self-regulated industries.

Common examples of federal sectoral privacy regulations include the Health Insurance Portability and Accountability Act (HIPAA) for healthcare providers, the Gramm-Leach-Bliley Act (GLBA) for financial institutions, and the Federal Educational Rights and Privacy Act of 1974 (FERPA) for educational institutions.

At the state level, certain industries are subject to additional regulations; for example, many state Departments of Insurance (DOI) require notice to the DOI in the event of a service interruption involving entities regulated by the DOI. These regulations are particularly severe, in some instances requiring notice as soon as forty-eight hours from the initial discovery of a security incident.

Finally, many industries require compliance with certain privacy frameworks that have not been promulgated by law. For example, most enterprises that accept payment cards (e.g., Visa or Mastercard) are required to comply in some capacity with the Payment Card Industry Data Security Standard (PCI-DSS), a body of security standards developed by major payment card processors. Similarly, entities that contract directly with or subcontract under the federal government may be required to comply with cybersecurity standards promulgated by the National Institute of Standards and Technology (NIST).

Trends in Ransomware Reporting Requirements

Based on trends observed in 2021, we can make some predictions about the future of ransomware breach reporting requirements. First, we expect that data breach reporting timelines will continue to shorten. By way of example, the FDIC, Federal Reserve, and Department of the Treasury issued a rule in November with compliance beginning May 1, 2022, that requires banks and their service providers to notify their primary federal regulator within thirty-six hours of a computer security incident

that is reasonably likely to disrupt the bank's operations. Notably, this rule does not predicate notice on data access or acquisition, meaning that entities may have to quickly notify their regulators of ransomware events even if there has not been such access or acquisition.

Second, many breach notification frameworks permit notice upon discovery of a breach, in other words, notice will not be triggered until the entity should reasonably know there has been access to personal information. However, some regulators are beginning to place greater emphasis on the discovery of an incident.

While the distinction is narrow, the implications are significant. In the case of ransomware incidents, businesses can be taken offline for weeks, and in many incidents, are unable to restore access to sensitive information. Even if access to data is restored, it can take weeks to determine the nature and scope of the incident and determine which individuals, if any, had sensitive personal information exposed. In many instances, victims of ransomware are forced to choose between reporting on a speculative basis due to a lack of information or risking sanction by a regulator or private action for failure to effectuate timely notice.

Notwithstanding the difficulties associated with making expeditious notice to the appropriate individuals and regulators, we are continuing to see "point of incident" notification triggers grow in popularity. For example, in 2017, the National Association of Insurance Commissioners (NAIC) issued a model rule requiring notice to the state insurance commissioner within 72 hours of the discovery of a cybersecurity event, which includes the disruption or misuse of an information system. Since its release in 2017, the NAIC model rule has been adopted in approximately ten states, however, we anticipate that additional states will be adopting the rule, either in part or in its entirety, in 2022.

Finally, we expect that we will soon be seeing additional requirements regarding the payment of a ransom. Historically, from a legal perspective, the only substantive impediment to payment of a ransom has been the OFAC sanctions list. While paying a threat actor is never palatable, paying a ransom for immediate decryption may be required in some circumstances, such as when there is a risk of bodily harm as in the case of a healthcare provider. Entities are generally free to pay a ransom so long as the threat actor has not been specifically blacklisted by OFAC.

However, as ransomware has entered the public discourse, greater attention is being given to the aftermath of ransomware incidents. The Biden administration has recently expanded its use of sanctions to target cryptocurrency marketplaces that effectuate payment to threat actors. Law enforcement routinely seeks information regarding ransomware negotiations and payment in its postmortem investigations of ransomware incidents and the Department of Treasury has stated that it will consider whether an organization notified and cooperated with law enforcement in deciding how to proceed against entities that inadvertently make payment to an individual or entity on the OFAC list.

In light of the growing ransomware threat, we anticipate that we will see additional and more formal reporting requirements relating to ransomware events and the payment of ransoms. Presumably, such data would aid law enforcement in its effort to apprehend threat actors and perhaps recapture ill-gotten funds.

Recommendations for Businesses

The best way a business can protect itself from ransomware is to create a robust culture around

cybersecurity. Security is an ongoing exercise; while no system is impregnable, the vast majority of ransomware incidents we see leverage a combination of the same five or so vulnerabilities, such as open remote desktop protocol ports, unpatched or out-of-date software and Layer 8 failures. Security controls should be constantly assessed for vulnerabilities, configuration errors and proper function.

Second, many businesses do not realize the sprawling nature of data in their control until an incident has occurred. Sensitive information should be segmented appropriately, and if at all possible, encrypted both in transit and at rest. Developing a detailed data flow, both for internal and vendor data, is a critical step in ensuring an expeditious response in the event of a ransomware incident.

Finally, a robust incident response plan is critical, and in many instances, required. The incident response plan should include, at a minimum, procedures for backup validation, key incident response contacts and procedures for the preservation of forensic artifacts. As breach notification rules become more stringent, an incident response plan is invaluable in ensuring a compliant response and restoration.

National Law Review, Volume XII, Number 40