Legal Obligations When a Data Breach Invokes the Laws of Multiple Jurisdictions

New York Law Journal
July 12, 2019
By R. David Lane, Jr.

Many practitioners outside of the privacy and data security space may not appreciate the variety of incidents that can potentially give rise to data breach notification obligations.

By now, many attorneys are generally aware of the existence of data breach notification laws and may have even had the misfortune of receiving a data breach notice in the mail. The long string of high-profile breaches spanning back many years has raised awareness of the need to notify individuals whose personally identifiable information has been compromised in a data breach. One might envision the scenario of a hacker penetrating a system to steal sensitive business, financial or personal information, or a ransomware attack in which a threat actor encrypts a company's data for the purpose of extorting the company. In addition to the damage that can be done due to the loss of funds or private information, if the incident results in unauthorized access or exfiltration of personal information, legal obligations may arise to notify the individuals whose information was accessed or taken.

Yet many practitioners outside of the privacy and data security space may not appreciate the variety of other types of incidents that can potentially give rise to data breach notification obligations. Suppose an employee loses a device containing unencrypted personal information by theft or mistake. Or, an unauthorized individual might gain access to paper or electronic records containing an individual's personal information through criminal conduct or mere happenstance. Perhaps an employee inadvertently misdirects an email containing unsecured personal information to the wrong recipient. Other common incidents include a business email compromise incident, in which a threat actor gains access to a company employee's email account, possibly through an email phishing campaign, and hijacks and re-routes emails for the purpose of committing fraud. Each of these incidents requires an analysis as to whether it rises to the level of a reportable breach under applicable data breach notification laws.

Such an analysis begins by conducting an investigation as to the nature and scope of the incident and the types of data involved. In the case of an electronic system breach, it may require a thorough forensic investigation of the affected systems. Once a determination is made whether the data involved included individuals' personal information, the business will need to identify those individuals whose person information was impacted.

While the debate in Washington over a federal privacy law continues to gain momentum, to date, breach notification requirements are embodied within a patchwork of state and sector-specific laws.

All 50 states as well as the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have enacted data breach notification laws. When a data breach occurs, one must apply the data breach notification law of the jurisdiction in which each affected individual resides rather than the law of jurisdiction in which the breach occurred. While many state breach notification laws contain general similarities, many differences exist, adding complexity to the analysis.

State breach notification laws generally define a breach as an incident involving the unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information that the business owns or maintains. Some laws apply to both electronic and physical records. Others, such as New York's statute, apply to electronic records only. State breach notification laws typically define "personal information" as an individual's name in combination with other data sets, typically a social security number, driver's license number, or payment card or financial account number in combination with a required security code or password that allows access to the account. Some states also include other potentially identifiable data sets, such as health information, biometric information, date of birth, or an email address or username in combination with a password or security questions and answers to an online account.

Some state breach notification laws only require notification if the incident reaches a threshold level of harm to the affected individuals. Some laws require notification to the state regulator, often the Attorney General's Office, if a resident of that state is affected. Out of these states, some laws only require notice to the regulator if a threshold number of residents have been affected (e.g., 250, 500 or 1,000). Some state laws specify content requirements for the breach notice to either individuals or the state regulator. Additionally, some states require that notification to affected individuals take place within a specified period of time from discovery of the breach, such as within 30, 45 or 60 days. Other state laws do not specify a timeframe but require notification "in the most expedient time possible," or "without unreasonable delay." State breach notification laws around the country are often being amended, requiring practitioners to keep apprised of the latest developments.

In addition, there are sector-specific breach notification requirements under both federal and state law. For instance, the Health Information Technology for Economic and Clinical Health (HITECH) Act's Breach Notification Rule applies to HIPAA covered entities that have experienced a breach involving health information. The Gramm-Leach-Bliley Act contains breach notification requirements applicable to financial institutions. Some states also include sector-specific breach notification requirements, such as those applicable to insurance providers and financial services companies.

If an entity's breach affects the personal data of individuals who reside in other countries, it should consider the potential applicability of foreign breach notification laws. For instance, the General Data Protection Regulation (GDPR), which went into effect in the European Union on May 25, 2018, can have extraterritorial effect. The GDPR generally applies to the processing of personal data in the context of activities of an establishment of a controller or processor in the EU regardless of where the processing takes place, and to the processing of personal data of individuals

in the EU by a controller or processor not established in the EU when the processing concerns the offering of goods or services to individuals in the EU or monitoring the behavior of individuals that takes place in the EU. The GDPR contains a data breach notification requirement arising out of "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed." The regulation requires that a controller notify the competent supervisory authority of a personal data breach within 72 hours of discovery of the breach unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. The data controller must also notify affected individuals of a personal data breach when the breach is likely to result in a high risk to the rights and freedoms of natural persons.

Additionally, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), which went into effect on Nov. 1, 2018, requires organizations to provide breach notification to affected individuals and the federal privacy commissioner if a breach creates a "real risk of significant harm" to individuals. Data breach laws have been enacted in Latin America, Asia-Pacific, Africa and the Middle East as well.

Due to the myriad and sometimes conflicting legal requirements that may be triggered following a data breach invoking the laws of multiple jurisdictions, it is important for businesses and counsel alike to be aware of the potential legal implications in the event of a breach. Having cyber insurance coverage in place before an incident occurs and retaining counsel experienced in incident response upon discovery of an incident are vital steps in navigating a data privacy incident should it occur.

R. David Lane Jr. is a shareholder in the New York office of Marshall Dennehey Warner Coleman & Goggin where he is a member of the privacy and data security practice group. He may be reached at rdlane@mdwcg.com.