Privacy, Data Security, and the Hospitality Industry: What Changing Laws Mean for You

By Lindsay B. Nickle
Wilson, Elser, Moskowitz, Edelman & Dicker, LLP
901 Main Street, Suite 4800
Dallas, Texas 75243
214-698-8093
Lindsay.Nickle@wilsonelser.com

The headlines are becoming almost commonplace: "Hackers Attack and Steal Records" or "Data Breach Confirmed—Customer Information Leaked to the Public." An increasing number of stories are hitting news sources about the theft or breach of personal information, which can leave a business organization with questions about the potential risks in the event the unthinkable happens to them.

Virtually every business organization deals with sensitive and protected data, and the hospitality industry is no exception. The very nature of hospitality mandates that customers provide hotels and restaurants with personal and financial information in connection with the provision of services. In addition, many customers are travelers from other jurisdictions, which means that data security issues for businesses in the hospitality section can become inordinately complicated very quickly. This paper is designed to provide an overview of key issues and potential legal ramifications for the hospitality industry related to data security.

I. Background Information

To understand data security obligations, an organization must first understand some basic key concepts. First, what data is it required to protect? Second, what is a data breach?

A. Protected Data

As a starting place, certain types of data are protected by law, and business organizations that collect, create, use, or share these types of data have legal obligation to protect the information from unauthorized disclosure. Generally speaking, by law, organizations are required to protect the security of certain personal information collected from customers and employees—commonly called Personally Identifiable Information or "PII." Forty-seven states, plus the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have enacted data protection statutes. These statutes typically define protected information as a combination of a person's name with one or more other identifiers—such as social security number, driver's license number, or certain financial account information. While the state law definitions have many commonalities, the statutes are far from uniform. For example, North Dakota includes dates of birth on the list of identifiers, and several states include medical or health insurance information in their definitions (Arkansas, California, Florida, Missouri, Montana, North Dakota, Nevada, Oregon, Puerto Rico, Texas, and Wyoming). Subtle differences in the statutes make understanding data security obligations a difficult proposition. Further, the laws are constantly in flux. Several states updated their data protection laws during 2015, adding additional elements to the components of protected information. For example, Montana and Wyoming amended their laws to protect name plus taxpayer identification number, and Connecticut and Oregon added

biometric data, which includes fingerprints or retinal scans. Several states, including Nevada and Rhode Island, have recently expanded protections to include email addresses or user names in combination with passwords or access codes. The continually changing laws make data security a complicated prospect for an organization to manage.

In addition, an organization must understand that it is the residence of the individual that controls the applicability of the law, rather that the location of the business organization. That means that in the hospitality industry, where customers are often travelers, the laws of the state where the customer lives governs what data the organization has an obligation to protect and the organization's response in the event the data is compromised.

In addition to the legal protections afforded to PII, federal law also protects individuals' health information. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") defines protected health information—or "PHI"—which, general described, is the information about an individual's medical history or treatment, as well as health insurance information, used to identify patients. Health care providers, insurers, and business associates have a legal obligation to protect PHI. While HIPAA regulations may not often have a direct impact in hospitality related fields, these laws are significant in the data security landscape and understanding that medical and health care information is protected by law is important to understanding the big picture of data security.

In addition to the myriad of laws that address data protection, contractual agreements can also impose obligations on an organization to keep certain data and information private and confidential. When businesses enter into vendor relationships, partnerships, or joint ventures, the contractual agreements that govern those business dealings may impose obligations on an organization to protect data received from, exchanged by, or created as a result of the relationship. Organizations should be aware of any data protection obligations they may have as a result of contractual agreements, and those obligations should be communicated to the personnel responsible for ensuring the security of the data governed by the contractual terms.

Once an organization understands that it has legal obligations to protect information it creates, collects, uses, and stores, the organization should take steps to determine what data it has, so that the organization can properly understand its data protection obligations. An organization needs to know what information it has to be able to know what information it needs to protect. Further, if an organization does not know what data or information it has, it can be difficult to know if information has been lost or what information has been lost. That reality can significantly complicate the response process.

B. Data Breach

When a data breach occurs, an organization has a number of responsibilities in response. Therefore, it is important for an organization to have an understanding of what constitutes a data breach. Generally speaking, a data breach is the intentional or unintentional access, acquisition, or disclosure of sensitive, protected, or confidential data to an unauthorized individual or individuals. It is important to note that the disclosure of data can be a breach even if the disclosure was unintentional. Accidents and negligence can cause breaches just as intentional or malicious conduct can.

While this is a general description of a data breach, data breach is actually another term with highly varied state law definitions. As with the definitions of data protection, the state law definitions there are similarities among the states' laws, but there is no uniformity. Therefore, if an organization's data is compromised, lost, or stolen, responding to the event may require the analysis of multiple state laws to determine whether the event meets the definition of breach and to determine how the organization must respond.

II. What Do You Do if You Have a Breach?

If your organization has a breach, what are the key issues? How will you know what to do in response, and what are the legal risks present when a breach has occurred? These are difficult questions to answer, particularly in the heat of the moment following the discovery of an event. One way to ensure the smooth navigation of a breach response is to utilize a breach coach. A breach coach is an attorney with experience in interpreting the various data security and privacy laws that govern how organization s must respond to data breaches. An experienced breach attorney can help avoid missteps and miscues that can further complicate the already stressful and complicated process of dealing with a breach event.

A. Identify the Type or Types of Data Involved

If the organization discovers a data security event, take steps to determine the type or types of data involved. For example, were names and social security numbers compromised? What about driver's license numbers or credit or debit card information? The type of information involved can have an impact on the response.

Sometimes the process of identifying what has been compromised or lost is a simple process. Other times it requires a deeper investigation, which can include the internal IT department or external computer forensic investigators. Forensic examination can help determine not only what occurred, but how many individuals may have been impacted, as well as the types of data involved. If an external forensic investigation is necessary, the attorney breach coach should oversee the process of retaining the forensic firm and assist with scoping the project. In this way, investigation costs can be controlled and as much of the investigation as possible can be afforded protection by the attorney-client privilege.

B. Identify the Applicable Statutes and Regulations

As indicated above, it is the residences of the impacted individuals that control the applicable laws for purposes of determining the appropriate response to a breach. Therefore, during the process of compiling information about the involved individuals, an organization must take note of the states where the individuals live, and because the hospitality industry involves travelers, the list of individuals can quickly implicate a large number of jurisdictions. While the state laws might be similar, the subtle differences mandate an appropriate analysis of each involved state's responsive obligations when crafting the organization's response strategy.

C. Confirm Whether there are Contractual Obligations

In addition to the state law concerns, an organization's vendor contracts may obligate an organization to notify a business partner in the event of a data breach or other security incident, and the contract may impose very tight timelines. Vendor contracts should be reviewed during the preparation of the response strategy to ensure that contractual obligations are met during the notification process.

III. Notification Requirements

A. Individual Notification

Typically, following the data breach, and organization will be required to send individual notification letters to the people whose information was lost or compromised. Each of the data protection statutes include a notification provision, but again, the provisions are far from uniform. There are many different timelines in play, and some states even place different requirements on the content of the notification letters. Therefore, the location of the individual to whom the letter will be sent can impact the content and the timing of the notification. Further, while sending individual letters is the most common form of notification, some states permit notification by telephone or email, as appropriate. Also, many states provide a substitute notification measure if the cost of individual notification is prohibitive. Further, some of laws require that notification of an event be made to the media as well.

Despite the lack of uniformity regarding notification, the general requirements of the notification letters are customary. With some express statutory exceptions (most notably, Massachusetts) the notification letter should tell the recipient generally what happened and what type of information was compromised. It should also explain what individuals can do to protect themselves and explain how the organization plans to assist. In addition, the letter should also discuss what the organization has done in response to the event and what is being done to prevent future events.

It is easy to see why responding to an event involving individuals from more than one state can quickly become confusing tangle of legal interpretation.

B. Regulatory Notification

In addition to the legal requirement that impacted individuals be provided with notification, several states require notification to regulators, most notably, state Attorneys General. As will all data protection and notification provisions, there is no uniformity here either. Different provisions have different deadlines for notification. Further, some provisions are not triggered until a threshold number of impacted individuals is met. If Attorney General notification is required, the Attorney General's office will want to see how potential harm to individuals was mitigated and how future occurrences will be avoided. Regulators often want to see copies of notification letters or substitute or media notifications. In addition, organizations can expect potential follow up questions or investigations after notification. Attorneys General have the authority to issue fines and penalties against an organization in response to a data breach. They can also impose fines if an organization fails to provide notification of a breach to individuals or regulators when it should have.

IV. Litigation Risk

In understanding the legal risks and ramifications of data breach, it is important to understand not only that the process of navigating the investigation and notification in response to a data breach is a minefield, but data breach also presents a very real risk of potential litigation. It is not uncommon in the aftermath of a data breach to see class-action lawsuits filed on behalf of individuals whose information was involved. Common causes of action include negligence, defamation, fraud, breach of contract, violation of right to privacy, and state law deceptive or unfair practices claims. While there may be legal arguments that could defeat these claims, staggering litigation costs are a very real risk.

Federal regulators can also pursue actions against organizations as a result of data breaches, and the FTC has regularly pursued actions in response to breach events, relying upon their authority under section 5 of the FTC Act to regulate conduct that constitutes an unfair or deceptive practice. The FTC can assess significant fines as a result of data breaches, and consent orders often result from these actions. The consent orders frequently require years of audits, self-reporting requirements, and on demand reporting, in addition to monetary payments.

V. Conclusion

Obviously, data breach presents significant legal risk to an organization, and the aftermath of data breach can quickly become a very complex matter to deal when. When a potential breach is discovered, an organization must quickly and effectively conduct an investigation and begin navigating a quagmire of legal requirements that lack uniformity and cohesion while also continuing to operate business. Every decision must be made quickly with the business's goals in mind, as well as the risk management perspective of potential litigation and regulatory investigation. It is often confusing and cloaked in crisis. Having experienced and qualified assistance during a breach response can avoid pitfalls and mistakes, and time and effort spent in risk management and pre-preparation can help an organization survive what might otherwise be chaos.