BURR FORMAN LLP

Data Breach Notification Laws in the United States: What is Required and How is that Determined?

Articles / Publications
12.10.2021

Has your business considered what obligations you would have to notify people in the event of a cyber-attack that compromises some or all of your IT systems? Have you cataloged all the data you collect and where it is stored so that you can determine whose information is impacted by a breach? If not, you are certainly not alone. With the continuing increase in cyber-attacks and particularly ransomware, combined with laws that are imposing shorter and shorter notice deadlines, it is important for all businesses to understand the scope of their potential notification obligations in the event they fall victim to an attack.

Breach Notification Laws

Breach notification requirements obligate organizations that are collecting, storing, processing, or otherwise in possession of personally identifiable information to notify the individuals if the information is compromised in a security breach. In addition to notifying the identified individuals, many states require that the Attorneys General offices and the Credit Reporting Agencies be notified, depending on how many identified individuals in the state received notices. If you are missing contact information for some of the identifiable individuals, if the number of identified individuals is particularly high, or if the cost of the required notifications is excessive, you may have the option to, or be required to, provide substitute notice in lieu of or in addition to individual notices. In most cases, substitute notice requires notification to be placed prominently on your website as well as distributed through the

RELATED PROFESSIONALS

India E. Vincent, CIPP/US, CIPM

RELATED CAPABILITIES

Cybersecurity & Data Privacy

Data Breach Notification Laws in the United States: What is Required and How is that Determined?

media, in print, on television, and/or by radio.

In the United States, certain Federal Laws govern obligations to report data breaches in particular industries, including:

- The Health Insurance Portability and Accountability (HIPAA) Act provides notification requirements for a security breach that compromises protected health information held by a covered entity or its business associates.
- The Gramm-Leach Bliley Act (GLBA) requires covered financial institutions to notify customers whose non-public personal information is compromised by a security breach.
- The Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers recently issued by the FDIC which requires FDIC supervised banking organizations to notify the FDIC within 36 hours of determining that they have suffered a computer security incident (a) that materially disrupts or degrades the organization's ability to maintain banking operations or to deliver services to a material portion of its customers, (b) that materially disrupts or degrades the operations of one or more business lines that could result in a material loss of revenue or decrease in the organization's value, or (c) that could pose a threat to the financial stability of the country.

Beyond the federal laws, all 50 states have data breach reporting laws, and they all have different requirements for determining whether a breach has occurred and for the notices that are required. For data breach reporting statutes, most businesses have to comply with the law of a given state if they have a breach that compromises the personal information of a resident of that state. This means that businesses must consider the scope of the data they collect and store in order to determine whether they are likely to have obligations to report under the laws of a given state.

If your business has information on an individual residing in a given state, two key questions in assessing reporting requirements are the nature of the data involved and whether or not the incident meets the definition of a reportable breach.

What is Personally Identifiable Information?

Even though the definition of personally identifiable information differs from state to state, and the states use different terminology to define the data that triggers reporting obligations, personally identifiable information in general is information that does, or can be used to, identify, locate or contact an individual, alone or when combined with other personal or identifying information and is usually information known to create a significant risk of identity theft, fraud or other harm if compromised. When considering the differing definitions in the U.S. you can usually expect personally identifiable information that triggers a breach reporting requirement to include a person's first name or first initial and last name, together with one or more of the following:

Data Breach Notification Laws in the United States: What is Required and How is that Determined?

Identification Numbers such as a –

- Social Security Number,
- Passport Number,
- Driver's License Number,
- State Non-Driver's Identification Card Number, or
- Other government-issued ID number;

Account Numbers such as a –

- Financial account number,
- Credit card number, or
- Debit card number
- (sometimes requiring the account number be disclosed in conjunction with a security code, access code, or password that permits access to the account)

Personal Characteristics / Biometrics, including

- photographic images,
- fingerprints,
- iris scans,
- handwriting, or
- other unique characteristics;

Medical information or medical history

In many states, even if the data constitutes personal information triggering reporting requirements, there are exceptions to the reporting requirements if the data is already publicly available or when it is encrypted or de-identified, but not all states address those exclusions so clearly.

When determining your obligations to comply with a particular data breach notification law, a key requirement is to determine whether the information involved qualifies as personal information, personal data, or other protected form of data or information under the relevant state's data breach reporting law.

What is a Reportable Breach?

When assessing breach reporting obligations, you also must determine if the incident qualifies as a "security breach" or "data breach" under the relevant statute. In some states, a breach occurs when the personally identifiable information has been **accessed and acquired** by an unauthorized person, but in

other states, it is enough if the personally identifiable information is **accessed** by an unauthorized person. Some states allow exceptions to the notification requirements if you can document that there is low risk of harm to the identified individuals based on the circumstances of the breach. To rely on this type of exception to the notice requirement, the decision should be well documented, and the documentation must be maintained as specified in the statute. In addition, some states require that the Office of the Attorney General be notified of your determination to rely on this exception.

When considering breach notification obligations, organizations should consider not only the individuals who are their customers or patients but also the individuals who work for them. In addition, if the nature of your business includes collecting information about individuals other than your customers, vendors, or employees, you may have reporting obligations to those other individuals as well. Knowing and documenting what information the organization holds about which individuals, why you hold that information, and where that information is stored, can go a long way toward facilitating breach notification obligations should the situation arise.

A complete discussion of the notification requirements is beyond the scope of this article, but there are some key points to remember. The content requirements for the notices also vary by state, as do the requirements for how notices must be delivered. Do not just assume you can send the same notice to all individuals. Also be aware of the timing requirements for each state, which are usually measured from the time you had knowledge of the breach. While many of the states identify their timing requirements to be "without undue delay" be aware that many Attorneys General still evaluate the process undertaken by the organization to determine if notice was provided promptly. In some states that are penalties for providing late notice.

Exceptions to Breach Notification Requirements

Some states exempt certain businesses from compliance with the state's privacy law. Again these exemptions vary by state, but some of the typical categories are:

- Organizations complying with another law or regulation with requirements at least as thorough and restrictive as the state's privacy laws;
- Organizations regulated by a federal statute intended to meet the same objectives, such as HIPAA and HITECH, without regard to which standard is more restrictive;
- Organizations that hold the personally identifiable information subject to contractual confidentiality obligations, and comply with those contractual obligations; and
- Organizations that maintain and comply with their own procedures for protecting personal information pursuant to the laws, rules, regulations, guidance, or guidelines established by the organizations' state or federal regulators.

Data Breach Notification Laws in the United States: What is Required and How is that Determined?

Despite these exemptions, it is important to carefully consider the terms of the exemption. For example, if state law requires more protection for Protected Health Information than HIPAA does, HIPAA requires compliance with the state requirement. In that case, complying with HIPAA might exempt you from complying with the state statute, but then HIPAA on its terms would require you to comply with certain portions of the state statute. Consistent with the theme of privacy laws in the United States, sorting through the conflicting obligations requires careful analysis of the requirements.

Enforcement and Penalties

Just as the requirements of the various state statutes differ, the methods of enforcing these statutes and the penalties that can be assessed differ by state as well. Most states authorize their Attorney General to enforce the statutes, but some states also have options for private causes of action seeking damages for failure to properly protect information or failure to properly notify individuals under the breach notification requirements.

The remedies available for failure to comply with data breach notification laws include injunctions to prevent further violations, monetary penalties, and reasonable costs. The range of the monetary penalties varies significantly, and while some states include caps for the total penalties that can be assessed either per consumer or per incident, other penalties can reach well into six figures particularly when the violations impact 10,000 or more residents.

Beyond the injunctive or monetary penalties, organizations should also consider the negative publicity that accompanies failure to protect the personally identifiable information of its employees, customers, or other parties. Such a determination can cause consumers to lose confidence in the organization and cause other organizations or individuals to seek greater contractual assurances that the organization will comply with the privacy laws. In addition, if you are seeking insurance coverage for future incidents, you may find that it is harder or at least more expensive to obtain such coverage. Litigation risks in states with a private cause of action also open the door for class action lawsuits or other claims for damages arising as a result of the breach.

Closing Thoughts

While data breach reporting requirements vary by state, knowing which state laws apply to your business and identifying common requirements and standards across those states can help streamline your breach reporting requirements in the event of a breach. Maintaining a solid understanding of the data you collect, store, process, and ultimately dispose of makes it easier to assess reporting requirements resulting from any particular breach and can go a long way to reducing the costs associated with a data security incident.