NSCP
THE NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS

MAY 2017 SPECIAL REPRINT

Currents

Data Breach! What to Know About Where to Go…

By Louis Dempsey

Regulators and law enforcement agencies aggressively pursue data breach cases focusing on the controls investment advisers and broker-dealers implement to prevent and detect a data breach. While significant emphasis is placed on the firm's preventative measures to detect and mitigate data breaches, there is little published to assist firms in the unfortunate instance where they may actually have been breached; this despite virtually every state having rules that require prompt reporting of such instances. In fact, how your firm deals with an attack may help mitigate the impact of regulatory action and criminal or customer litigation. Therefore, every firm should develop a robust response plan in the event of a breach that addresses the unique requirements of each jurisdiction in which it operates.

What is a Data Breach?

A data breach is an incident of unauthorized access to, or acquisition of, sensitive or confidential data. It may involve personally identifiable information ("PII") or personal health information. Although we most often think that a data breach involves only electronic data, we should also consider that PII is often contained in paper documents. Therefore, we must consider not only the protection of electronic PII, but also the destruction of documents that contain PII. Furthermore, breaches that occur at a third-party vendor, involving a firm's customer or proprietary data, may also be subject to state laws.

General State Requirements

In 2003, the state of California was the first state to enact a data breach notification law. Since that time, approximately 46 additional states have enacted laws addressing data breaches (Alabama, New Mexico and South Dakota are the exceptions). In general, state laws address the type of information that is covered, to whom notification of the breach must be reported, the timing of such notification, the assessment of potential harm, and civil liability in the event of a breach.

About the Author

Louis Dempsey is President at Renaissance Regulatory Services, www.rrscompliance.com. He can be reached at louisdempsey@rrscompliance.com.

What information is covered?

While the definition of PII in many states is similar to the SEC's Regulation SP, the reporting obligations typically go beyond what is required under the federal rules. States generally define PII as:

1. The customer's first and last name in combination with some other data elements, such as a social security number, driver's license or state identification card, passport or similar information that may be used to verify identity; or
2. A financial account, debit or credit card number, along with a security or access code or password that would provide access to the customer's account.

Reporting Obligations

The reporting obligations under state laws are triggered by the acquisition, or reasonable belief of acquisition, of PII by an unauthorized person. Once triggered, firms must consider their reporting obligations to customers, government agencies, and others.

Reporting to Customers

For those states that have data breach laws, notification to customers is generally required. Firms are expected to investigate the breach immediately to determine the scope of the breach, and to take measures to restore the integrity of the system. If, during the investigation, the firm determines that there is no reasonable likelihood of harm, due to encryption or redaction of the data, then customer notification may not be required.

State data breach laws typically address the timing, content, and method of delivery of the notice to customers.

1. Timing: In describing the timing of the notice, state laws use phrases such as "as expeditiously as possible", "without unreasonable delay", "immediately, but no later than 45 days from discovery of the breach", and "not later than 30 days after determination of the breach." Customer notification may be delayed upon request from a law enforcement agency if the agency believes notification would compromise or impede a criminal investigation.
2. Content: Notices to customers should include the name and contact information for the company, an explanation of what happened (including the date(s) of the breach), what information was involved, what the firm is doing to investigate and prevent a recurrence, and what the customer can do to protect his/her information going forward. Some states require that the notice include the toll-free numbers and addresses of the major consumer

reporting agencies. Some states go further still, like California[1] and Connecticut,[2] and require the company to offer identity theft prevention and mitigation services if social security numbers are involved.

3. Method of Delivery: Generally, state laws permit reports to customers to be sent by written notice or by e-mail.

Reporting to Government Agencies

Not all state data breach laws require firms to notify the government of a breach, but, for those that do, the requirements vary widely. Some states have a threshold for the number of residents impacted (e.g., greater than 500) and identify the agency that must be notified. The state of New York, for example, requires that if any New York residents are impacted by a data breach, then the firm must notify the State Attorney General, the Department of State and the Division of State Police as to the timing, content and distribution of the notices, and the approximate number of affected persons.[3] The State of California requires that if more than 500 state residents are impacted as a result of a single breach, a firm must electronically submit a sample copy of the notice to the California Attorney General. Copies are maintained in a searchable database on the California Attorney General's website.

Reporting to Consumer Reporting Agencies

As with reporting to government agencies, state laws may also require data breaches to be reported to consumer reporting agencies. It is important to know what the state's requirement are for reporting to these agencies, and critically, the timing. Firms do not want their customers finding out about a breach from some other entity.

Reporting to Third-Parties

If a firm or its vendors maintain documents or data for third parties, and that data contains PII, the holding firm must notify the third-party owner of the information immediately upon discovery of the breach. This would include PII maintained on behalf of affiliates, custodians, and advisers where a sub-advisory arrangement exists. For example, if a custodian broker-dealer maintains PII on the clients of its affiliated investment adviser, then the broker-dealer would notify the adviser of a breach. Similarly, if a sub-advisor is breached it would be required to notify the adviser who has the primary relationship with the customer. These obligations should be documented in contractual agreements between the entities and in each entity's compliance program.

Penalties for Non-Compliance with State Data Breach Laws

Companies should be aware that the laws to which they are subject are based on the location of the affected customers. Thus, in the event of a breach, the company may find itself being accountable to several states on a single breach. For this reason, your firm must assess the reporting requirements for each state in which it operates or has customers.

Many state laws provide for civil penalties in the event of violations of their data breach laws. The penalties may be based on several criteria, e.g., the number of residents in the state who were not notified of the breach or the number of days the notification was delayed. Additionally, in some states, the Attorneys General could bring an action to recover economic damages resulting from a violation.

Finally, some states require the firm providing the notice to offer identity theft prevention and mitigation services to the customers at no cost for at least one year.

Safe Harbor for Use of Encryption

Although there are significant potential costs for a breach, some state data breach laws provide an exemption for firms that use encryption. If the information is encrypted, redacted or truncated (e.g., last four digits of the social security number or credit/debit card), and the encryption key was not accessed or acquired by the hackers, the reporting requirements in the statutes would not apply. Of course, firms must ensure that the encryption methods are industry standard and that the hackers did not acquire the encryption keys through other means.

Resources

Knowing where to start is critical. The varying state requirements create a multitude of reporting obligations that firms must be aware of to avoid significant regulatory actions or litigation that could cripple a firm. Researching all of the state requirements can be onerous, but there are resources. We've listed below some resources that can help you to begin developing your data breach incident response plan.

The National Society of Compliance Professionals: **www.NSCP.org**

National Conference of State Legislatures Website (as of 2/24/2017): **http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx**

California Attorney General searchable database: **https://oag.ca.gov/ecrime/databreach/list**

Privacy Rights Clearinghouse Data Breaches: **https://www.privacyrights.org/data-breaches**

Data Disposal Laws: **http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx**

Conclusion

As government agencies and the public focus more aggressively on data breaches, it is important for investment advisers and broker-dealers to ensure that they assess the requirements for data breach disclosure in each jurisdiction in which they operate. It may not matter who your primary regulator is, as data breach laws are unique to each jurisdiction. Determining what the requirements are for each jurisdiction in which you operate is critical to developing your response plan and may reduce your risk exposure to regulatory, civil or criminal actions. ★

(Endnotes)

1. California Civil Code 1798.82(d)(2)(G), effective 1/1/2015
2. Connecticut General Statutes Sec.6. Section 36a-701b.(b)(2)(b), effective 10/1/2015
3. NY Gen. Bus. Law 899-aa.8.(a)