Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# Data Breaches: Will You Be Sued, And Can You Lower Risk?

*Law360, New York (April 25, 2012, 1:29 PM ET)* -- Statistics regarding data security breaches can be sobering. For instance, according to one widely reported study conducted by the Ponemon Institute, 90 percent of organizations have had at least one data breach in the last year. More troubling is that the study concluded that the majority of organizations (almost 60 percent) had two or more breaches over the year.

In light of headlines describing multimillion-dollar data security breach settlements, it is no surprise that businesses fear the worst. As a result, after a breach occurs understanding the likelihood that a lawsuit will be filed, and, if filed, the company's potential liability, is essential.

While quantifying risk is always difficult, it is even more so when it comes to data security breaches due to the ever-changing statutory, regulatory and judicial environment. Nonetheless, data collected as part of a recent joint study by the Heinz College of Public Policy and Information Systems, Carnegie Mellon University, and Beasley School of Law, Temple University, provides some measure of the litigation risks associated with security breaches.

**What Is The Chance Of Being Sued After A Security Breach?**

During the five-year period of 2005 through 2010, 230 federal complaints were filed by consumers (typically as class actions) attempting to recover damages following a data security breach. When that number is compared against the quantity of publicly reported breaches, it appears that 4 percent of all publicly reported data security breaches lead to federal litigation. Of course, this is only half of the picture as many of the most prominent data security cases to date were filed in state court. Nonetheless, the likelihood of receiving a federal complaint provides one of the first quantitative metrics concerning the general risk of data security breach litigation.

All breaches, of course, are not created equal, and a number of factors significantly impact the likelihood that a federal complaint will be filed.

*Plaintiffs Are Focused on the Loss of Financial Data*

Breaches that involve the loss of consumer financial data are six times more likely to lead to a federal lawsuit as compared to breaches that did not involve financial data. Financial data also is a far better predictor of suit than is the existence of other types of sensitive personal information such as health records, medical data or credit card information.

*Plaintiffs Focus on Improper Disposal of Data*

Breaches that were caused by a company, or a company's employee, improperly disposing of data were three times more likely to lead to a federal lawsuit as compared to breaches that resulted from other causes, such as the loss or theft of a device. Most likely this is due to the fact that numerous states specifically require companies to properly dispose of sensitive information. Accordingly, training employees on how best to destroy documents and hardware can be key to lowering risk.

*Plaintiffs Are More Likely To Bring Suit When They Can Show Actual Injury*

Although in many (if not most) data breach lawsuits, plaintiffs fail to allege actual financial harm, the existence of financial harm greatly increases the likelihood that suit will be filed. Specifically, the odds of a company being sued are three and a half times greater if consumers suffer financial harm. That said, there may be a recent trend among district courts to permit suits to proceed where out of pocket harm cannot be shown. As a result, this factor may be less of a differentiator going forward.

*Plaintiffs Look for Large Breaches*

Not surprisingly, the likelihood of receiving a federal complaint is far greater if a breach involves a greater number of consumers. For example, federal lawsuits focus on breaches that involved, on average, 5.3 million records. In comparison, the average number of records that are at issue in breaches that do not elicit federal lawsuits is 98,000.

**What Is the Range of Liability?**

The likelihood that a particular lawsuit, once filed, may lead to recovery or liability is dependent on a number of factual and legal factors. From a global perspective, however, defendants have obtained dismissal of approximately 50 percent of the data security cases that have been filed. The vast majority of suits that survive dismissal are settled.

While the settlement value of such suits varies widely, based upon the little public information that is available, individuals (e.g., class members) obtained an average of more than $2,500, whereas their attorneys average $1.2 million (but go as high as $6.5 million) in fees. In addition, several settlements involve cy pres relief in amounts up to $9.5 million.

**How Can Businesses Lower Risk?**

There are three proven methods of lowering the risks associated with data breaches.

*Breach Prevention*

The only surefire way to eliminate the risk of litigation and of liability is to prevent a data security breach from occurring in the first place. In addition to complying with state and federal laws that require most companies to institute procedures to secure sensitive information, as a best practice companies should:

1) Know Their Data: Identify all sensitive data that the company collects.

2) Minimize Data: Only collect what the company needs and securely dispose of data that is no longer needed to achieve business objectives.

3) Map Data: Understand how collected data is used, and with whom it is shared.

4) Prepare A WISP: Develop a written information security plan to address known risks and prepare for a breach.

5) Educate Employees: Train employees about the company's written information security plan.

6) Manage Data Vendors: Incorporate appropriate data transfer provisions in your vendor agreements and monitor compliance.

*Breach Response*

The sooner an incident is identified, its cause is determined, and mitigation measures are implemented, the greater the chance that a company can avoid litigation. As a practical matter, the actions taken in the first minutes and hours after discovering an incident can either cause or prevent the eventual filing of a complaint.

As a best practice, have a data breach protocol in place prior to a breach. The plan should lay out what to do in the event of various types of data breaches, including technology, administrative and legal resources that can be contacted immediately if needed to help handle the breach. Remember that breaches are far more likely to occur after hours, on the weekends or during holidays than during normal business hours. If your company lacks sufficient internal resources to respond to breaches 24 hours a day, find out if your external resources can fill the gap if needed.

For example, our firm's data security team has an attorney on-call 24 hours a day to advise clients and recommend steps in the first hours of a breach response that can decrease the likelihood that a suit will be initiated or that a lawsuit, if brought, could succeed.

*Litigation Defense*

After a breach occurs it is essential to anticipate possible causes of action. Although almost every data security breach complaint alleges that a company committed an unfair or deceptive act in violation of a state consumer protection statute, the legal landscape is constantly evolving.

Indeed, plaintiffs have asserted at least 85 unique causes of action that draw upon various state and federal statutes, tort and contract law. Understanding what may be alleged in a complaint is essential to developing at an early stage — often before litigation is filed — a litigation defense strategy.

--By David A. Zetoony and Jena M. Valdetero, Bryan Cave LLP

*David Zetoony is a partner in Bryan Cave's Washington, D.C., office, where he leads the firm's data privacy and security practice. Jena Valdetero is an associate in the firm's Chicago office.*