New Jersey Law Journal

VOL. 213 - NO 11 MONDAY, SEPTEMBER 9, 2013 ESTABLISHED 1878

IN PRACTICE

INTERNET LAW

A Primer on N.J.'s Data Breach Notification Law

What to do if the security of customers' personal information is compromised

By Andrew P. Bolson

In recent years, media coverage of data breaches has become ubiquitous. Hardly a week goes by before another company announces that its customer information has been leaked or stolen. No company is immune. Banks; hospitals; universities; federal, state and local governments have all experienced data breaches. See "Chronology of Data Breaches, Privacy Rights Clearinghouse," www.privacyrights.org/data-breach/new. In 2012, there were at least 14 reported breaches in New Jersey that affected thousands of customers, with surely many more unreported incidents. While any breach has the potential to be dangerous and disruptive to customers, in truth, not all breaches will result in identity theft. However, once customers' personal information is no longer secured, identify theft becomes a real concern.

The primary remedy for a breach of customer information is timely notice. The hope is that if customers are aware that their information has been breached, action can be taken to avoid the most serious repercussions caused by identity theft. Recognizing the importance of being timely notified of a breach, in 2005, New Jersey joined a growing list of states that have passed a data breach notification law.

New Jersey's statute, N.J.S.A. 56:8-161 et seq., requires that companies conducting business in New Jersey disclose breaches that affect New Jersey customers. A breach occurs when a customer's personal information "was, or is reasonably believed to have been, accessed by an unauthorized person." N.J.S.A. 56:8-163(a). Upon discovering the breach, the first step is to notify the Division of State Police, in the Department of Law and Public Safety, for investigation or handling. Thereafter, once permitted by law enforcement agencies, customers must be notified "in the most expedient time possible and without unreasonable delay." N.J.S.A. 56:8-163(a).

The notification must be made through written notice, through electronic notice or by substitute notice if the cost of providing notice would exceed $250,000. N.J.S.A. 56:8-163(d). Substitute notice consists of sending an email to customers, posting notice on the company's website and providing notification to the major news media. N.J.S.A. 56:8(d)(3). If a company has a notification procedure in place, the company satisfies its statutory requirement by following its own notification procedures. N.J.S.A. 56:8-163(e). If a breach affects more than 1,000 customers at one time, the company must also provide notice to national consumer reporting agencies. N.J.S.A. 56:8-163(f).

Not all breaches in New Jersey trigger the notification procedure. Notification is only required when there has been a "breach of security," which occurs when customer information is accessed by an unauthorized person or used by an authorized user for an illegitimate business purpose. N.J.S.A. 56:8-161. A breach of security does not occur if the customer information wrongly accessed is encrypted or if the information does not constitute "personal information."

In order to be personal information that triggers the notification statute, under N.J.S.A. 56:8-161, the breached data must consist of a person's "first name or first initial and last name" along with the person's:

1. Social Security number;
2. Driver's license number or state identification card number; or
3. Account number or credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.

However, if a name and a Social Security number were contained in

Bolson is an associate at Rubenstein, Meyerson, Fox, Mancinelli, Conte & Bern PA in Montvale.

separately breached data sets, the information would still be personal information if the data can be linked together. Before rushing to notify customers, companies must understand whether a breach of security warranting notification has occurred.

When a company does discover a breach of security requiring notification, it should immediately implement its own procedures or follow the statutory guidelines. "Willfully, knowingly or recklessly" violating the data breach notification law is an unlawful practice and a violation of New Jersey's Consumer Fraud Act (CFA). N.J.S.A. 56:8-166. The CFA empowers the New Jersey attorney general to investigate breaches and to impose penalties. N.J.S.A. 56:8-3; N.J.S.A. 56:8-3.1. In addition, the CFA allows for a private right of action for those persons who can establish they have experienced an ascertainable loss. N.J.S.A. 56:8-19. Thus far, in New Jersey, plaintiffs, in the few reported data breach cases, have been unsuccessful at establishing their damages.

In *Holmes v. Countrywide Financial Corp.*, No. 5:08-CV-00205-R, slip op. at 2 (W.D. Ky. July 12, 2012), Matthew and Danielle Holmes, two New Jersey residents, were among some 2.5 million persons who were impacted by a security breach at Countrywide. Concerned that their stolen information was the reason they were turned down for a car loan, the Holmes purchased credit monitoring for $14.95 a month. In January 2009, the Holmes instituted a class-action lawsuit against Countrywide. While the Holmes' complaint was joined with similar lawsuits and heard by the federal district court in the Western District of Kentucky, the Kentucky court applied New Jersey law to analyze their claims. Specifically, the *Holmes* court examined whether charges for credit monitoring created a sufficient ascertainable loss for purposes of the CFA.

The court ultimately found that costs for credit monitoring are not recognizable damages because "[l]itigants under the state's laws may not recover for future harm where an injury has not materialized." Similarly, in the other New Jersey district court cases that have examined the question of credit monitoring — namely, *Reilly v. Ceridian*, 664 F.3d 38, 46 (3d Cir. 2011), and *Giordano v. Wachovia Sec.*, No. 06-476 (JBS), 2006 U.S. Dist. LEXIS 52266, at *12 (D. N.J. July 31, 2006) — the courts have found that fees associated with credit monitoring do not amount to an ascertainable loss for the purposes of a consumer fraud violation.

Despite plaintiffs' difficulty in proving an ascertainable loss, New Jersey businesses should not ignore their responsibilities under the state's data breach notification law. By providing timely notification, companies are effectively immunized from any further liability under the CFA and from the state attorney general's office. For this reason, the mere threat of a regulatory investigation and the possibility that a plaintiff eventually might succeed in proving an ascertainable loss, or establishing another viable cause of action under an alternate theory, should be sufficient incentive for a company to follow the law and provide the required notification.

Still, the cost of notification will likely cause some companies to try and avoid their regulatory responsibilities. This is likely especially true of small businesses who may not have the resources to deal with a large-scale breach. Companies can minimize their costs through purchasing insurance products specifically designed for data breaches. These insurance products provide peace of mind to companies who regularly deal with personal information. Depending on a particular policy and provider, insurance may pay for the cost of defending lawsuits, for the costs of responding to any regulatory investigations, for the cost of the notification itself and for the costs of an array of other expenses that may arise. Since commercial insurance policies differ greatly and are often negotiated, companies must determine their needs before deciding which policy to consider.

For varying reasons, companies now hold vast amounts of information about their customers. Unfortunately, once customers' information is breached, it is difficult for a company to retrieve and secure what has been lost. Recognizing the reality of data breaches in our modern age, the New Jersey legislature has instituted a statutory scheme to prevent the greatest threat caused by data breaches, namely, identity theft. Companies of all shapes and sizes doing business in this state must be aware of New Jersey's data breach notification law, and be ready to comply with its requirements if and when breached. ■