Notifying Clients and Customers of a Data Breach: When is a Breach Actionable?

by Rosaria A. Suriano and Matthew Dolan

The media reports of hacking and mammoth corporations experiencing data breaches have now become incessant. Despite the attention-grabbing headlines occasioned by some of America's largest corporations, small and mid-sized businesses are not being spared. In fact, small and mid-sized companies are more at risk and less prepared for data breaches. In a recent report, the security firm Symantec found that 30 percent of small businesses received a 'spear-phishing' email in 2013.[1] These seemingly innocuous-looking emails rely on social engineering tactics to specifically pique the interest of an intended target and induce that target to open an attachment. Once the attachment is released, the attackers can often access the entire company network, including any electronically stored confidential customer information.

Depending on the nature of the company's business and the state in which the company conducts that business, a number of legal duties and liabilities will arise in the event of a breach. It is imperative that a company, whether large or small, understand the legal ramifications of a breach and its obligations to its customers and clients.

The Law in New Jersey

Many states, including New Jersey, have enacted some form of legislation requiring private or government entities to notify individuals of security breaches of information involving their personally identifiable information.[2] N.J.S.A. 56:8-161 *et seq.*, applies to any company conducting business in New Jersey, which compiles or maintains computerized records that include personal information. "Personal information" is defined as "an individual's first name or first initial and last name linked with any one or more of the following data elements: (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."[3]

A "breach of security" is defined as unauthorized access, or authorized access for an illegitimate purpose, to personal information that compromises the security, confidentiality or integrity of the information.[4] Personal information that is encrypted to render it unreadable or unusable does not constitute a breach. Upon discovery of a breach, the statute requires companies to first notify the Division of State Police and then notify any customer who is a resident of New Jersey whose "personal information was, or is reasonably believed to have been, accessed by an unauthorized person."[5] The notification must be either written or electronic, with an exception permitting substitute notice in the event the cost of providing such notice would exceed $250,000, or the affected class of subject persons to be notified exceeds 500,000.[6]

Federal Law

At the federal level, there are no generally applicable notice requirements imposed upon companies in the event of a breach. However, notice requirements and penalties are included within a number of federal statutory schemes involving highly regulated groups such as medical and financial professionals. For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act require covered entities to notify all patients and insureds whose private health information is compromised by a security breach. Similarly, pursuant to the Gramm-Leach-Biley Act (GLBA), federal agencies such as the Federal Trade Commission (FTC) and the Financial Industry Regulatory Authority (FINRA) have issued guidelines that require financial institutions to notify customers whose non-public information has been subject to unauthorized use.

Under the HIPPA and HITECH rules and regulations, the definition of covered entities is quite broad, and

can include small business vendors such as insurance brokers and billing servicers who transfer and maintain private health information (PHI).[7] In the event of a breach, the penalties can be significant. Pursuant to 45 C.F.R. 160.404(b)(2), the Department of Health and Human Services (HHS) can impose penalties ranging from $100 to $50,000, based on the determined level of culpability. Recently, it has become apparent that the HHS is cracking down on violators, and small medical practices have not been spared.

In early 2013, a small hospice group in North Idaho was assessed a $50,000 penalty after a laptop containing the unencrypted private health information of 441 individuals was stolen from the premises.[8] Similarly, in Dec. 2013, a small physician practice group in Massachusetts settled with the HHS for a $150,000 penalty after an unencrypted thumb drive containing PHI on about 2,200 individuals was stolen from the vehicle of one its staff members.[9] In that case, the HHS determined the medical practice failed to implement policies and procedures to address the breach notification provisions of the HITECH Act.[10]

Cases Interpreting the Law

As of yet, there has not been any case law directly addressing an action by individuals against a company for failing to notify pursuant to New Jersey's notification statute, N.J.S.A. 56:8-161. Although some reported case law exists under similar theories of liability, they all reflect a common theme—the inability to demonstrate actual damages or cognizable loss.

In *Pinero v. Jackson Hewitt Tax Service Inc.*, a Louisiana plaintiff brought an action against Jackson Hewitt alleging, in part, violations of the Louisiana Database Security Breach Notification Law for the mishandling of her confidential personal information.[11] The court dismissed the plaintiff's claim, finding her alleged damages were not based on actual injury but merely speculation regarding future injury or identity theft.[12]

Similarly, in *Giordano v. Wachovia Securities, LLC,* the plaintiff alleged a number of theories of liability against Wachovia after a Wachovia report containing confidential customer information was lost in the mail.[13] The New Jersey District Court dismissed the plaintiff's claim, finding the costs associated with credit monitoring to protect against possible future harm were merely speculation and insufficient to confer standing. Like *Giordano* and *Pinero*, federal courts across the country have uniformly held that the time and money spent on credit monitoring does not constitute a present injury but rather a future one that has not yet materialized.[14]

Despite plaintiffs' difficulties in establishing a cognizable loss, businesses must still remain vigilant, as the risk of liability remains.

Can a Security Breach Trigger a Claim under the Consumer Fraud Act Allowing for Treble Damages and Legal Fees?

New Jersey's notification statute is subsumed within the powerful provisions of New Jersey's Consumer Fraud Act (CFA), at N.J.S.A. 56:8-1 *et seq.* Pursuant to N.J.S.A. 56:8-166, "willfully, knowingly, or recklessly" violating the data breach notification law is an unlawful practice and a violation of the CFA. Under the CFA, a business can be exposed to penalties as well as civil suits, entitling the plaintiff to treble damages and costs.[15]

To prevail under the CFA, a plaintiff first must establish a violation of N.J.S.A. 56:8-161 *et seq.* The plaintiff would have to establish that the company willfully, knowingly, or recklessly failed to notify the plaintiff after the plaintiff's personal information was compromised. Second, the plaintiff must establish an "ascertainable loss."[16] As discussed, the mere possibility of some future identity theft is not enough. However, a scenario where a plaintiff's personal information is used to make fraudulent purchases or withdraw funds from an account is conceivable and will quantify the loss.

In New Jersey, alleged losses under the CFA need not be substantial. To the contrary, the New Jersey Supreme Court has affirmed the ascertainable loss requirement as satisfied in instances where each plaintiff sustained a loss of $39.99[17] and where the damages consisted of only an alleged $20 overcharge for a vehicle registration fee.[18] Consequently, a relatively minor loss may be sufficient. Moreover, even if the impermissible purchases are ultimately refunded, case law suggests a plaintiff could still establish an ascertainable loss as long as he or she brings a claim before the refund occurs.

In a 2011 unpublished Appellate Division opinion, *Cowger v. Cherry Hill Mitsubishi*, the Appellate Division reversed the trial court's decision and held that a car dealership that failed to timely return a plaintiff's $500 deposit for test-driving a car violated the CFA.[19] Although the money was returned one day after the complaint was filed, and within 24 days after the deposit, the court found the plaintiff had demonstrated

an ascertainable loss because she filed the matter before the money was returned. The court held the CFA does not require the alleged loss to continue after the filing of the complaint.

Picture the scenario as follows: Consumer credit card information is stolen from a local retailer. The local retailer knew its computer system was hacked but failed to notify all of those affected. Shortly thereafter, many consumers began to notice fraudulent purchases on their accounts. Those consumers contacted their banks but were told the investigation into whether or not the purchases were fraudulent could take up to 90 days, and a refund would not be issued until the conclusion of the investigation. Consequently, the next day the consumers filed a CFA claim against the retailer from whom they had made purchases shortly before the fraudulent transactions appeared. Will the consumers prevail? Based on the court's liberal interpretation of the penalty provisions under the CFA, it appears as if they may.

Protecting Client/Customer Information

Due to the potential liability in the event of a breach, it is necessary for businesses to recognize their legal duties and take preventative measures to protect themselves before a breach occurs. Preventative measures must include the implementation of written security procedures and encryption of confidential customer information. Companies should implement procedures requiring employee passwords be changed regularly and educating employees about the dangers of opening suspicious email attachments. More importantly, companies should outline actions to be taken in the event of a breach. Timely notification of customers or law enforcement entities, as required under the law, could ultimately preclude legal liability.

Encryption is key. Hiring a security professional that can encrypt sensitive computer information could prevent the use of unlawfully obtained information. More importantly, some states, including New Jersey and New York, include safe harbor provisions within their notification laws for encrypted information. For example, under the New Jersey statute personal information rendered unreadable or unusable by way of encryption does not qualify as a breach.[20]

Conclusion

With the ever-increasing incidents of hacking and subsequent security breaches, it has become necessary for companies to stay informed of their duties under the law and work to prevent incidents from occurring in the first place. Those organizations subject to federal rules, regulations and penalties should pay particular attention to their obligations under the law. Still, even if not covered by a federal statutory scheme, all New Jersey businesses must remain conscious of potential risks. A data breach could equate to direct monetary losses, loss to reputation and legal liability. Although there have not been any reported CFA claims under New Jersey's statute to date, the potential for a CFA claim exists. Accordingly, it would be wise for attorneys to counsel their business clients on their duties under the law and the benefits of a security plan. ■

Rose Suriano is a partner with Meyner and Landis, LLP, and represents companies in business disputes, commercial litigation, non-compete agreements and business-related claims. Matthew Dolan is an associate with Meyner and Landis, LLP, and formerly a law clerk to the Honorable Edward M. Coleman, presiding judge, Chancery Division-General Equity, Somerset County.

Endnotes

1. Internet Security Threat Report 2014, Symantec Corporation, Volume 19, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.
2. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. (According to the National Conference of State Legislatures, 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted some form of legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information).
3. N.J.S.A. 56:8-161.
4. *Id.*

5. N.J.S.A. 56:8-163(a).
6. N.J.S.A. 56:8-163(d).
7. *See generally* 45 C.F.R. § 160.103.
8. HHS Jan. 2, 2013, press release, http://www.hhs.gov/news/press/2013pres/01/20130102a.html.
9. HHS Dec. 26, 2013, press release, http://www.hhs.gov/news/press/2013pres/12/20131226a.html.
10. *Id.*
11. *Pinero v. Jackson Hewitt Tax Service Inc,.* 2009 WL 43098 (E.D. La. Jan. 7, 2009).
12. *Id.* at *4.
13. *Giordano v. Wachovia Securities, LLC*, No. 06-476 (JBS), 2006 WL 2177036 (D.N.J, .July 31, 2006).
14. *Shafran v. Harley-Davidson, Inc.,* No. 07 CIV. 01365 (GBD) 2008 WL 763177 (S.D.N.Y. March 20, 2008); *Kahle v. Litton Loan Servicing, LP,* 486 F. Supp. 2d 705, 712-13 (S.D. Ohio 2007); *Guin v. Brazos Higher Educ. Serv. Corp.*, 2006 WL 288483, at *6 (D. Minn. Feb. 7, 2006); *Stollenwerk v. Tri-West Healthcare Alliance*, 2005 WL 2465906, at *5 (D. Ariz. Sept. 6, 2005); *Hendricks v. DSW Shoe Warehouse*, 444 F. Supp. 2d 775, 782-83 (W.D. Mich. 2006).
15. *See* N.J.S.A. 56:8-13 (penalties) and N.J.S.A. 56:8-19 (treble damages and costs).
16. N.J.S.A. 56:8-19.
17. *Lee v. Carter-Reed Co., L.L.C.*, 203 N.J. 496, 529 (2010).
18. *Bosland v. Warnock Dodge, Inc.*, 197 N.J. 543, 559 (2009).
19 *Cowger v. Cherry Hill Mitsubishi, Inc.*, 2011 WL 848133 (App. Div. March 14, 2011).
20. N.J.S.A. 56:8-161.