Data Security: What You Don't Protect Can Cost You

Every business has a responsibility to keep the sensitive personal information of its customers and clients secure. No list captures exactly what information qualifies as "sensitive personal information" but it can include names, addresses, social security numbers, and credit card and banking information—the types of data businesses keep in their records from day-to-day operations. Failing to protect this information can lead to loss of customer confidence, bad publicity, and civil and criminal liability. To guard against these very real dangers, business owners and managers must take care to understand their risks and responsibilities in light of a complex, and changing, web of federal and state regulation.

Nature of the Threat

Buried somewhere in a company's server, the "cloud," and other digital storage mechanisms there often lies a vast amount of valuable customer information. Today's technology compiles this information in such a fashion that, absent proper safeguards, digital storage systems can become a veritable treasure trove for individuals looking to illegally access the sensitive personal information of others. Businesses of all sizes and types are potential targets.[1] Retail stores, energy companies, information and technology companies, insurance companies, gas stations, financial service providers, hotels, restaurants, and healthcare providers, among others, have all suffered data security breaches.[2]

Moreover, if recent history is any indication, businesses will continue to be affected by data security breaches in the years ahead. In 2011, there were 855 documented security breaches worldwide, compromising 174 million records.[3] Early markers show that 2012 was no exception: among business organizations, medical providers, governmental entities, and educational institutions there were at least 660 documented data breaches in the United States.[4]

State of the Law

In the United States, the legal obligations of businesses to protect data containing the sensitive personal information of their customers derive from two sources: (1) a series of limited but fairly well-defined federal laws; and (2) a tapestry of state law. The interaction between these different bodies of law outlines the legal responsibilities and potential risks facing businesses throughout the country.[5]

Federal Data Security Laws

There are a limited number of federal data security laws. In the private sector, those that exist focus on specific areas or industries. For example, entities that possess records of individuals' health information are subject to the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). Such entities include health plans, health care clearinghouses, health care providers, and the business associates of those entities. Likewise, the Gramm-Leach-Bliley Act (GLBA) established minimum data security standards for companies that offer financial products or services. Among other things, HIPAA, HITECH, and GLBA (and various regulations implementing these Acts) limit the use and disclosure of protected information, impose requirements to preserve the security, confidentiality, and integrity of protected information and, in certain circumstances, require notification of affected individuals when a breach occurs.[6] Failure to comply with these requirements can lead to civil and criminal liability.[7]

In addition, various governmental agencies, including the Federal Trade Commission, have implemented the Red Flags Rule, which applies to "financial institutions" and "creditors." The Red Flags Rule requires many businesses to implement a written program designed to detect the warning signs of identity theft in their day-to-day operations.[8] In cases of noncompliance, civil penalties and injunctive relief are available.[9]

The Tapestry Of State Data Security Laws

Businesses that fail to sufficiently protect the sensitive personal information of others may be held civilly or criminally liable under state law. Unsurprisingly, data security requirements and potential punishments vary from state to state.[10] Ohio, for example, enacted a statute requiring businesses to notify state residents when records containing the residents' sensitive personal information are breached, without consideration of the business's culpability, if any, in permitting the breach.[11] The Ohio Attorney General is expressly authorized to "bring a civil action" against persons that fail to act in accordance with the statute's requirements.[12]

In addition to requiring compliance with state statutes and regulations, some states also allow for private actions based on the common law theories of negligence, breach of contract, breach of fiduciary duty, and invasion of privacy. These private actions can include class actions. For example, in 2011, nearly 77 million records were compromised when an unauthorized person breached the security of the PlayStation Network, a Sony gaming system.[13] In 2012, nearly six million records

continued on page 5

1 Of the 855 security breaches documented by the Verizon Risk Team in 2011, 72% involved companies with 100 or fewer employees. Verizon Risk Team, 2012 Data Breach Investigations Report 11 (2012).

2 *Chronology of Data Breaches*, Privacy Rights Clearinghouse, http://www.privacyrights.org/data-breach/new (last visited January 22, 2013). The Privacy Rights Clearinghouse website collects information on data security breaches, separated by type of breach, type of organization affected, and year. *Id.*

3 Verizon, *supra* note 1, at 2; *see also id.* at 45 (listing the hundreds of millions of records compromised in recent years).

4 *Chronology of Data Breaches*, *supra* note 2.

5 Businesses can also assume additional data security obligations by agreement.

6 *See* Gina Stevens, Congressional Research Service, Data Security Breach Notification Laws 11-17 (2012).

7 *See, e.g.*, 42 U.S.C. § 1320d-5.

8 *See, e.g.*, 16 C.F.R. § 681.1.

9 *See Fighting Fraud with the Red Flags Rule*, The Federal Trade Commission, http://www.ftc.gov/bcp/edu/microsites/redflagsrule/faqs.shtm#E (last visited January 22, 2013).

10 *See, e.g., Stevens, supra* note 7, at 4.

11 Ohio Rev. Code. § 1349.19.

12 *Id.*

13 13 Liana B. Baker & Jim Finkle, *Sony PlayStation Suffers Massive Data Breach*, REUTERS (Apr. 26, 2011), http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426.

continued from page 4

were exposed after LinkedIn's security was breached.[14] Both of these breaches resulted in class-action lawsuits against LinkedIn and Sony.[15]

Given the tapestry of state law, businesses should (1) be familiar with the regulations of the different states in which they do business[16] and (2) consider the potential for private rights of action in various jurisdictions, including class-action lawsuits.

Further Federal Data Security Legislation

Several bills were introduced in the 112th United States Congress, including: the Personal Data Privacy and Security Act of 2011 (S. 1151); the Data Breach Notification Act of 2011 (S. 1408); and the Personal Data Protection and Breach Accountability Act of 2011 (S. 1535). This legislation would have increased the number of businesses subject to uniform federal regulation and imposed substantial penalties for noncompliance. Although not enacted, this legislation suggests that Congress may attempt to further alter the legal landscape in the coming years.

Conclusion

Acquiring and storing the sensitive personal information of customers is a standard part of business for the simple reason that it allows businesses to increase the quality of the services they provide. But the value and sensitivity of this information also makes these businesses vulnerable to breaches of their data security. As a result, business owners must be proactive in understanding not only the laws that govern their businesses today, but also the consequences they might face tomorrow if their data security is breached.

Robert J. Hanna
Tucker Ellis LLP
216.696.3463
robert.hanna@tuckerellis.com

Jesse W. Thomas
Tucker Ellis LLP
216.696.5573
jesse.thomas@tuckerellis.com

Paul L. Janowicz, Law Clerk
Tucker Ellis LLP

14 Nicole Perlroth, *Lax Security at LinkedIn is Laid Bare*, The New York Times (June 10, 2012), *http://www.nytimes.com/2012/06/11/technology/linkedin-breach-exposes-light-security-even-at-data-companies.html?_r=1&pagewanted=all*.

15 Among other things, the class-action complaints alleged breaches relating to failure to adequately safeguard consumer data and/or failure to timely notify appropriate entities and consumers. *See Johns v. Sony Computer Entertainment America LLC, et al.*, Case No. 3:11-cv-02063, CM/ECF No. 1 (N.D. Cal.); *Szpyrka v. LinkedIn Corp.*, Case No. 5:12-cv-03088, CM/ECF No. 1 (N.D. Cal.).

16 Determining whether a company "does business" in a state and is subject to the laws of that state can be a difficult legal question, especially in light of recent advances in technology and e-commerce. The simple fact that a business does not own or operate a physical location in a state is not conclusive. Other factors, such as whether a business advertises in or ships product to a particular state, may also be considered in determining whether it is subject to that state's laws.

Welcome New Members

Jeffrey Barlow, Swagelok Company
Jason Blake, Reliability First Corporation
Carolyn Blake, Brakey Energy
John Bridges, MCPc, Inc.
Kathleen Fenner, KeyBank
Kristen Gest, Parker-Hannifin Corporation
Robert Hackley, CTPartners
Mathew Hicks, Federal Equipment Company
Gerri Kornblut, Dwellworks, LLC
Joseph Leonti, Parker-Hannifin Corporation
Katarina Mijic-Barisic, Cuyahoga Community College
John Molnar, Parker-Hannifin Corporation
Alexandra Price, Hyland Software, Inc.
Ryan Quinn, Nordson Corporation
Michelle Raymond, Babcock & Wilcox Power Generation Group, Inc.
Kiana Russell Zeigler, Cleveland Clinic Foundation
Brian Stack, Tremco Incorporated
Jason Sussman, The Lubrizol Corporation
Halle Terrion, TransDigm Inc.
Rinda Vas, American Greetings Corporation