

Authors

Gregory T. Casamento
212-812-8325
gcasamento@lockelord.com

Brian T. Casey
404-870-4638
bcasey@lockelord.com

Patrick J. Hatfield
404-870-4643
phatfield@lockelord.com

Vita E. Zeltser
404-870-4666
vzeltser@lockelord.com

www.lockelord.com

This *Client Alert* is provided solely for educational and informational purposes. It is not intended to constitute legal advice or to create an attorney-client relationship. Readers should obtain legal advice specific to their enterprise and circumstances in connection with each of the topics addressed.

If you would like to be removed from our mailing list, please contact us at either unsubscribe@lockelord.com or Locke Lord Bissell & Liddell LLP, 111 South Wacker Drive, Chicago, Illinois 60606, Attention: Marketing. If we are not so advised, you will continue to receive *Client Alerts*.

Attorney Advertising

© 2009 Locke Lord Bissell & Liddell LLP

The Expansion of Privacy and Data Breach Protection and Notification Laws: Changes are Coming Your Way

The overwhelming majority of states currently require that persons, companies or other entities that own, license, store or maintain personally identifiable information of an individual provide notice to that individual when the personally identifiable information has been breached.¹ These notifications do not come cheap, and, based on prior studies, the average data breach comes with a cost of \$54 per lost record in associated notification compliance costs.² Despite the comprehensive patchwork of breach notification laws designed to protect individuals whose personally identifiable information had been compromised and the associated costs of compliance, major data security breaches are commonplace.

News of employees engaging in the unauthorized review of employee personnel, customer or patient records, stories of stolen or lost laptops containing the names, addresses, Social Security numbers and credit card numbers of customers or employees, and criminal investigations of sophisticated hackers accessing customer or employee information through cyber-piracy serve as a sobering reminder that in the era of digitized personal information and portable electronic devices, data security breaches occur with alarming frequency. Thus, it comes as no surprise that the laws governing personally identifiable information safeguarding and data security breach notification requirements are expanding in scope and stringency as the federal, state and related governmental agencies attempt to respond to this reality and their constituents' concerns about the protection of personally identifiable information.

Massachusetts, for example, has taken a significant step to address data security – the Massachusetts Office of Consumer Affairs and Business Regulation recently enacted a regulation, effective January 1, 2010, (the “Massachusetts regulation”) setting stricter security standards for the protection of all Massachusetts residents' personally identifiable information and broader notification requirements for the breach of such information. These standards include specific encryption requirements for all persons that own, license, store or maintain personally identifiable information in both *electronic* and *paper* form about Massachusetts residents.³ The use of the term “Massachusetts Resident” in the regulation indicates that any company or entity, whether located in Massachusetts or not, that owns, licenses, stores or maintains a Massachusetts Resident's personal information is subject to the

Massachusetts regulations.⁴ While many states require pre-breach security measures and post-breach notification requirements to safeguard personally identifiable information, those measures are not as comprehensive as those that will become mandatory under the Massachusetts regulation.⁵

The U.S. Senate has also responded to the call for additional protections on personally identifiable information, though moving at a much slower pace than Massachusetts. A *proposed* federal bill sponsored by Sen. Dianne Feinstein (D-CA), titled the Data Breach Notification Act (“Senate Bill 139”), would require all federal agencies and persons engaged in interstate commerce who are in possession of data containing sensitive personally identifiable information to disclose any breach of such information. The federal bill provides that once it is passed into law, it “shall supersede... any provisions of law of any [s]tate relating to notification by a business entity engaged in interstate commerce or an agency of a security breach,” subject to some exceptions for victim protection assistance provided by state laws.⁶

Most recently, on April 30, 2009, the U.S. House *proposed* the Data Accountability and Trust Act (“House Bill 2221”),⁷ which contains certain information security safeguards aimed at protecting computerized data containing personal information and, like Senate Bill 139 requires a nationwide data security breach notification in response to a breach.

The Massachusetts regulation and the two proposed federal bills constitute a drastic expansion of security and notification obligations and requirements, and both are the bellwether for future laws and regulations in the data security management and breach notification areas.⁸ Therefore, the key requirements of the Massachusetts regulation and the proposed federal bills will be discussed in greater depth below to provide a better understanding of how to prepare to meet the upcoming data management security challenges associated with handling personally identifiable information.

Massachusetts: Written Comprehensive Information Security Program Requirement

The new Massachusetts regulation, 201 CMR §§ 17.01 – 17.04, referred to as the “Standards for the Protection of Personal Information of Residents of the Commonwealth,” provides the minimum standards to

be met in connection with the safeguarding of personally identifiable information contained in both paper and electronic records. The regulation requires all persons that own, license, store or maintain personally identifiable information about a Massachusetts resident to develop, implement, maintain and monitor a comprehensive written information security program to safeguard that information.⁹

The program must be consistent with industry standards, and must contain administrative, technical and physical safeguards to ensure the security and confidentiality of personal information. Although the regulation provides that the information security program's scope will depend on the size, scope, and type of business at issue, the amount of available resources and stored data and the need for security and confidentiality, the regulation provides a list of specific elements the information security program must contain, including:

- (1) designating a specific employee to maintain the information security program,
- (2) identifying and assessing reasonably foreseeable internal and external risks,
- (3) developing security policies in connection with records that are transported outside the business premises,
- (4) imposing disciplinary measures for violations,
- (5) preventing terminated employees from accessing records by immediately terminating their access to physical and electronic records,
- (6) verifying that third-party service providers adhere to equally stringent security measures,
- (7) limiting the amount of sensitive personal information collected and retained,
- (8) identifying the electronic media that contain personal information,
- (9) placing reasonable restrictions on records containing personal information,

- (10) regularly monitoring the information security program,
- (11) reviewing the scope of the program at least annually, and
- (12) documenting all responsive actions taken.¹⁰

“...the fact that the regulation applies to records stored in both paper and electronic form should provide incentive for those waiting to convert paper records to electronic records.”

The regulation also contains computer system security requirements that require, among other measures, securing user authentication protocols such as user IDs and reasonably secure passwords, placing restrictions of access to the personally identifiable information to those with a need to know basis to perform job duties, education and training for employees, and similar security measures. The regulation also requires, to the extent technically feasible, encrypting all transmitted records containing personal information that will travel across public networks, encrypting all data containing personal information to be transmitted wirelessly, and encrypting all personal information stored on laptops or other personal devices.

The broad implications of the regulation to businesses or entities handling personally identifiable information cannot be understated. The technical requirements of the regulation go beyond any current state laws and will require companies to rewrite their IT playbook and specifically, their data security management and data breach response plans. Moreover, the fact that the regulation applies to records stored in both paper and electronic form should provide incentive for those waiting to convert paper records to electronic records. Finally, because the regulation applies to information about employees who are Massachusetts residents, even entities that do not engage in transactions with con-

sumers and are otherwise exempt from the requirements of the Federal Trade Commission's ("FTC") Red Flags Rule,¹¹ will need to adopt a written comprehensive information security program to meet the standards. These changes are significant and companies should plan, adopt and test their revised information security programs now, so that those programs meet the regulation's standards on January 1, 2010.

Federal Data Breach Notification Act

Senate Bill 139, the *proposed* Federal Data Breach Notification Act, requires any federal agency or business entity engaged in interstate commerce that uses, accesses, or collects sensitive personally identifiable information to (1) provide notice to any U.S. resident whose information may have been accessed or acquired following the discovery of a security breach; and (2) provide notice to the owner or licensee of any such information that the agency or business does not own or license. As noted above, the federal bill provides that once it is passed into law, it "shall supersede... any provisions of law of any [s]tate relating to notification by a business entity engaged in interstate commerce or an agency of a security breach," subject to some exceptions for victim protection assistance provided by state laws.¹²

Senate Bill 139 exempts: (1) agencies and business entities from notification requirements for national security and law enforcement purposes; (2) security breaches where the agency or business conducts a risk assessment that concludes there is no significant risk of resulting harm, provides the results of the risk assessment to the Secret Service and the Secret Service does not respond within 10 days with a written directive requiring notification; and (3) business entities that utilize a security program that blocks the use of sensitive personally identifiable information and provides notice of a breach to affected individuals.

Under certain circumstances, the Secret Service, the FBI, the Postal Inspection Service, and State Attorneys General must be notified of the data security breach. Senate Bill 139 includes appropriations for costs incurred by the Secret Service to investigate

and conduct risk assessments of security breaches. Certain violations are punishable by civil penalties, and the U.S. Attorney General and State Attorneys General may bring a civil action against any business entity that violates Senate Bill 139. Senate Bill 139 further amends the Fair Credit Reporting Act to require agencies to include a fraud alert in the file of a consumer that submits evidence of compromised financial information to a consumer reporting agency.

The text of Senate Bill 139, as currently drafted, is likely to undergo significant revisions, and as of the date of this alert, the proposed Act had been forwarded to the Senate Committee on the Judiciary. We will issue updated alerts on any major developments in connection with its status as we monitor this situation closely.

Federal Data Accountability and Trust Act

On April 30, 2009, House Bill 2221 was proposed with bipartisan sponsorship in the U.S. House of Representatives. The *proposed* bill requires the FTC to promulgate regulations requiring each person engaged in interstate commerce and that directly or through a third party owns or possesses data in electronic format containing personal information to establish and implement policies and procedures regarding information security practices for the treatment and protection of personal information, including destruction of such information. Additionally, the proposed bill contains data security breach notification requirements applicable to any person engaged in interstate commerce that owns or possesses data in electronic format containing personal information.

House Bill 2221 notification requirements are largely similar to those currently in force in most states, with some substantive modification. The bill requires notices of a data breach to be sent to all affected U.S. citizens or residents and the FTC. If health information is breached, the Secretary of Health and Human Services is to be notified. The bill also contains special provisions not otherwise found in state laws for telecommunications carriers, cable operators, information services and interactive computer services providers. Notifications are to be made in written form or

by email, under certain circumstances, as is currently permitted in most states. The notification must contain a description of the personal information acquired, a summary of the recipient's rights to free credit reports, and contact information for the company sending the notices, the credit reporting bureaus, and the FTC.

Importantly, House Bill 2221, as proposed, has several major limitations that are similar to limits already in existence in current laws and regulations. First, it exempts from the notification requirement persons who determine that there is no reasonable risk of identity theft, fraud, or other unlawful conduct resulting from the breach. Second, the bill provides that encryption of data in electronic form, and other technologies the FTC may later identify, establishes a presumption that no reasonable risk of identity theft, fraud or other unlawful conduct exists following a breach. The presumption may be rebutted by facts showing that the encryption may be compromised.

House Bill 2221, as proposed, grants enforcement authority to the FTC, and grants state attorneys general the right to bring civil actions against violators, with penalties up to \$5,000,000.

As the law of privacy and data security continues to evolve, it becomes clear that holders and users of personally identifiable information will need to plan ahead to respond to the challenges posed by a continuously evolving legal and regulatory landscape to meet these challenges.

For more information on information security breach or loss notification laws, preparing breach or loss remediation plans, legally compliant breach notices or any of the other issues discussed in this e-Matters Alert, contact the authors listed on the first page or any member of Lock Lord's Technology Transactions Group.

Endnotes

1 The definition of personally identifiable information varies by state, but at the federal level is often defined as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any — (A)

name, Social Security number, date of birth, official [s]tate or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; (B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (C) unique electronic identification number, address, or routing code; or (D) telecommunication identifying information or access device" See 18 U.S.C. § 1028(d)(7). A few examples of state laws protecting this information are: California - Cal. Civ. Code § 1798.82; Georgia - O.C.G.A. § 10-1-910 et seq.; Illinois - 815 Ill. Comp. Stat. 530/1 et seq.; Louisiana - La. Rev. Stat. § 51:3071 et seq.; La. Admin Code. tit. 16, pt. III, § 701; Massachusetts - Mass. Gen. Laws ch. 93H, §1 et al.; New York - N.Y. Bus. Law § 899-aa; Texas - Tex. Bus. & Com. Code § 48.001 et seq.; Washington, D.C. - DC Code Ann. § 28-3851 - 3853.

2 This figure accounts for unbudgeted out-of-pocket spending and includes free or discounted services offered; notification letters, phone calls, and emails; legal, audit and accounting fees; call center expenses; public and investor relations; and other costs. Ponemon Institute, LLC 2006 Annual Study: Cost of a Data Breach, http://www.computerworld.com/pdfs/PGP_Annual_Study_PDF.pdf, last accessed May 12, 2009.

3 The Massachusetts regulations, known as the "Standards for the Protection of Personal Information of Residents of the Commonwealth," defines personal information as "a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) [s]ocial [s]ecurity number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public." 201 CMR 17.02.

4 See 201 CMR 17.01 ("This regulation implements the provisions... relative to the standards to be met by persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts...").

Offices

Atlanta
 Austin
 Boston
 Chicago
 Dallas
 Houston
 London
 Los Angeles
 New Orleans
 New York
 Sacramento
 San Francisco
 Washington DC

The Expansion of Privacy and Data Breach Protection and Notification Laws: Changes are Coming Your Way (cont'd.)

- 5 For example, Since October, 2008, Nevada's breach notice law requires all Nevada businesses to encrypt all electronic transmissions (other than faxes) of a consumer's personal information if the information is sent outside the secure system of the business. Nev. Rev. Stat. 570.970 (2005).
- 6 S. 139, 111th Cong. §10 (2009).
- 7 H.R. 2221, 22th Cong. (2009).
- 8 As will be discussed more fully in an upcoming LLB&L Client Alert, the health information technology section of the American Recovery and Reinvestment Act of 2009 that President Obama signed on Tuesday, February 17, 2009 (the "HITECH Act") contains numerous provisions affecting health privacy and security, electronic health information and updates to the Health Insurance Portability and Accountability Act (HIPAA). Among these changes were new notification requirements for breaches of privacy, security or integrity of personal health information (PHI). On April 16, 2009, the Federal Trade Commission issued the proposed Health Breach Notification Rules regarding breach notification requirements for vendors, their related entities and third party service providers when electronic health information is breached. Once finalized, these rules would apply to breaches that are discovered on or after September 18, 2009. On April 17, 2009, the Department of Health & Human Services issued guidance regarding technologies and methodologies that can be used to render PHI unusable, unreadable, or indecipherable to unauthorized individuals and, in effect, provides covered entities and their business associates with an optional safe harbor from the new data security breach notification requirement. HIPAA covered entities and business associates, as well as the new entities that are covered under the new FTC rules, should be prepared to comply with breach notification requirements that are being finalized.
- 9 201 CMR 17.01.
- 10 201 CMR 17.03(3).
- 11 The FTC's Red Flags Rule, which will be enforced by the FTC as of August 1, 2009, require entities subject to the FTC's jurisdiction to adopt written identity theft prevention policies – or, essentially, pre-breach security measures.
- 12 S. 139, 111th Cong. §10 (2009).

About the Authors

Gregory A. Casamento is a partner in Locke Lord Bissell & Liddell's New York office. He focuses his practice on business, commercial, insurance and intellectual property litigation and technology transactions. Mr. Casamento has significant experience litigating trademark infringement claims, technology, contract and restrictive covenant disputes, and insurance issues for his clients before both State and Federal Courts. His experience also includes advising clients on e-Matters issues, including, e-signature, e-discovery, e-admissibility and e-records management.

Brian T. Casey is a partner in the Atlanta office of Locke Lord Bissell & Liddell. As co-leader of Locke Lord's Insurance Practice Group, and a member of the firm's (a) Corporate(b) Capital Markets and (c) Healthcare Practice Groups, Mr. Casey focuses on (i) corporate, (ii) merger & acquisition, corporate and structured finance and other transactional, and (iii) regulatory matters for corporate clients in the insurance, financial services and health care industries. His clients include insurance companies, insurance holding companies, managing general agents and insurance agencies, third party and claims administrators, banks and other financial institutions, investment banks and reinsurance companies.

Patrick J. Hatfield is a partner in the Corporate Department in the Atlanta office and co-chairs the Firm's Technology Transactions Group. Throughout his legal career, Mr. Hatfield has focused on financial services, intellectual property and technology, gaining valuable experience as in-house counsel, including 10 years as senior counsel and vice president to a leading provider of IT and outsourcing services to the global financial services industry (NYSE:PMS) now part of Computer Sciences Corporation. Mr. Hatfield has handled a wide range of IT, outsourcing, acquisition and joint venture arrangements in the global financial services industry. His experience includes handling licensing, outsourcing and mergers & acquisition transactions in the United States, Europe, South Africa, Australia, and Asia.

Vita E. Zeltser is an associate in the Corporate Department in the Atlanta office of Locke Lord Bissell & Liddell. Ms. Zeltser focuses on general corporate and corporate governance matters, preparation and negotiation of commercial contracts, commercial lending and debt financing, and mergers and acquisitions.