



the quintessential source of information and education on professional liability

RECENT DEVELOPMENTS IN STATE PRIVACY AND DATA SECURITY: ASSESSING NEW BUSINESS RISKS

By Joseph J. Lazzarotti



Joseph J. Lazzarotti is an employee benefits attorney who coordinates the HIPAA and Workplace Privacy Practice Group at Jackson Lewis LLP, in the firm's White Plains, NY office. He may be contacted at lazzarottij@jacksonlewis.com or 914-328-0404.

This article discusses some of the federal and state legislative and regulatory developments affecting the privacy and data security of personal information. Businesses will need to take steps to deal with these new developments. For those businesses that use insurance as one tool to manage risk in this area, underwriters will need to consider how to assess the risk posed by policyholders. For that reason, the article also points to factors following from the legislative and regulatory developments discussed which underwriters should weigh in assessing its risk tolerance with respect to a particular policyholder.

Over the past few years, there has been a significant increase in state legislative and regulatory activity focused on protecting the privacy and security of personal information. A driving force behind these efforts has been the explosion in the number of identity theft cases. Instances of stolen laptops and PDAs, unauthorized entries into electronic databases and similar attacks on personal data are becoming more frequent and affecting more individuals.¹ This trend will only increase as advances in technology lead to (i) new and better tools that move and store information and (ii) the

adoption of less traditional methods of doing business, such as working from a “virtual” office.

Because businesses are massive repositories for and frequent transmitters of many forms of personal information, including the personal information of customers, vendors and employees, they will need to address this increasing exposure. While all businesses that access, use, maintain, disclose or destroy personal information should have reasonable policies and procedures to protect the privacy and data security of that information, they also should consider what insurance options are available to mitigate their exposure in the event of an unauthorized breach of personal information.

In many states, there is significant exposure, including the risk of class-action litigation, for businesses that violate these provisions.² For businesses with operations in more than one state, the risk of liability compounds. Thus, as state legislatures finally start to catch up with the rapid advancement of technology facilitating the crime of identity theft, businesses need to manage new risks relating to the privacy and data security of the personal information they maintain.

PRIVACY AND DATA SECURITY MEASURES

Both the federal and state governments have passed laws seeking to deter persons from committing identity theft by imposing stiff civil penalties and criminal sanctions. They also have passed laws intending to

limit the opportunity for the crime to be committed in the first place. While this article focuses on state law, examples of relevant federal laws are discussed below.

At the federal level, regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)³ provide one of the first sets of comprehensive privacy and data security protections. While far-reaching, these regulations have limited application in that they apply to certain health information maintained by certain “covered entities” – covered health plans (which include health insurance issuers), health care providers, and health care clearinghouses.⁴ However, the regulations create a comprehensive framework for protecting sensitive information that generally can be applied to many types of information. For this reason, these regulations may become the standard by which others, including courts, measure a business’ privacy and data security policies.

Other federal laws directed at enhancing the privacy and data security of personal information include the Gramm-Leach-Bliley Act of 1999,⁵ the Telephone Records and Privacy Protection Act of 2006 (HR 4709, signed by President Bush on January 12, 2007) and the Veterans Benefits, Health Care and Information Technology Act of 2006 (S. 3421, signed by President Bush on December 27, 2006). Under HR 4709, the practice known as “pretexting,” or obtaining phone records under false pretenses, is illegal and subject to civil and criminal sanctions. As part of requiring the Veterans Affairs Department to improve its

data security policies, S. 3421 requires the VA to include data security provisions in all service-provider contracts, such as requiring that the contractor notify the VA of any breach. While other bills are pending and expected to be taken up in the 110th Congress, more has been done at the state level to more broadly deal with privacy and data security issues.

The states generally have taken a “cocktail” approach to preventing identity theft, attacking the problem from a number of directions, such as (i) protections for social security numbers, (ii) notification requirements in the event of unauthorized breaches of personal information, (iii) affirmative obligations to safeguard personal information, and (iv) requirements related to destroying personal information that is no longer needed.

Social Security Number Protections

Many states have enacted measures to limit the use of social security numbers (SSNs). For example, beginning on January 1, 2008, businesses in New York will be prohibited from using or disseminating SSNs in certain instances, such as (i) printing an individual’s SSN on mailings or on any card or tag required to access products, services, or benefits, and (ii) requiring an individual to transmit his or her SSN over the Internet unless the connection is secure or the social security number is encrypted.⁶ Additionally, those possessing SSNs must implement safeguards necessary or appropriate to preclude unauthorized access to social security numbers and to protect the confidentiality of such numbers.⁷ Limited exceptions to these protections include a use or dissemination of an SSN that is mandated by federal or state law.⁸ Similar protections exist in a number of other states including, but not limited to, California, Connecticut, Illinois, Missouri and Texas.⁹

Breach Notification

Another measure taken by at least 34 states requires businesses to provide a notice when there has been an unauthorized breach of personal information maintained by the business.¹⁰ Unauthorized breaches triggering such notices are legion, many of which have hit the insurance industry – examples in 2006 include: (i) Aetna – laptop stolen from employee’s car exposes health records of policyholders’ employees; (ii) Humana – drug benefit applications stolen from

insurance agent’s unlocked car include personal information; in a separate incident, insurance employee called up customer information through a hotel computer and then failed to delete the file; (iii) AIG – computer server is stolen containing personal information including medical and disability information; (iv) Sentry Insurance – lead programmer-consultant for carrier stole personal information including SSNs on worker’s compensation claimants and sold the information on the Internet.¹¹ These incidents are not surprising given the mobility of today’s workforce and the volume of personal information to which many have ready access.

The protections under these laws extend to all residents in the state and protect “personal information,” typically defined as the first name or first initial and last name of an individual in combination with the individual’s (i) social security number, (ii) driver’s license number, (iii) state identification number, or (iv) financial account, debit or credit card number in combination with any required security code, access code, or password that would permit access to an individual’s account. If a notice obligation is triggered under a security breach notification law, notice generally must be provided to the affected residents of the state as soon as possible and without unreasonable delay. Accordingly, businesses should be aware of the notice requirements in the state(s) in which they are operating and be prepared to act quickly in the event of an unauthorized breach.

Affirmative Obligations to Protect Personal Information

In an increasing number of states it is not enough to be prepared to react to an unauthorized breach and provide the appropriate notice. Instead, businesses need to be proactive in safeguarding personal information. For example, the California Civil Code provides that: A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.¹² Because the California measure applies to a broad range of personal information, companies doing business in California will need to apply their

procedures and practices to a significant portion of the information they use, disclose and maintain with respect to customers, employees and others.

Data Destruction Requirements

Many companies struggle to determine how long to retain certain information. Retaining the information for too short a period may result in a violation of a particular record retention requirement, such as under applicable e-discovery rules or the Internal Revenue Code, or hamper a company’s ability to resolve a particular dispute or defend itself in litigation. However, retaining information for too long a period may not be considered reasonable with regard to protecting against unauthorized access to information. In addition, when companies finally do destroy information, state law requirements may affect the methods for doing so.

In a number of states, when businesses destroy records containing personal information they must ensure that the personal information is unreadable. For example, businesses in Texas that dispose of such records must modify the records by shredding, erasing, or any other means so that the personal information is unreadable or undecipherable.¹³ Similar laws apply in other states such as New York and California.¹⁴

UNDERWRITING THE RISKS OF PRIVACY AND DATA SECURITY VIOLATIONS

As insurance companies expand their product lines to include coverage for businesses relating to privacy and data security, underwriters will need to assess the risk of those seeking such coverage. In addition to understanding the enforcement provisions of the applicable laws, such as the availability and amount of penalties and damages under a particular law, by asking some of the questions below, an underwriter likely will be better able to determine how serious a particular applicant is about privacy and data security and, therefore, the level of risk in the policy.

- Does the business have a designated officer/committee dedicated to privacy and data security?
- What is the volume and nature of personal information accessed, used, maintained and disclosed by the business?

- To what extent does the business maintain personal information electronically? Has the business conducted an internal audit/risk assessment designed to (i) identify information maintained in the organization that is subject to privacy and data security laws; (ii) map the flow of that information throughout the organization; and (iii) assess the risks of unauthorized access and disclosure? When was that assessment conducted? How frequently are assessments conducted?
- Is the company more or less likely to use devices and technology that facilitate remote/wireless access to personal information?
- Are members of the business' workforce more likely to access personal information while traveling, working from home, making sales calls, etc.?
- Does the business employ encryption technology?
- In what states does the entity do business?
- Has the company had prior breaches of its electronic systems? How were those instances handled?
- Does the business have a written plan to address privacy and data security – including policies and procedures regarding when personal information may be received, created, accessed, used, modified, disclosed, discarded? When was it created, updated?

- Has the business identified which workforce members have access to personal information?
- What steps has the business taken to create awareness in the organization regarding the importance of privacy and data security? How often are workforce members trained? Is training documented? Does the business have confidentiality agreements with workforce members?
- How prepared is the business to deal with a breach to its personal information, including steps to mitigate harm caused by the breach?
- Does the business offer data protection services to workforce members, such as credit monitoring, I.D. theft insurance, I.D. theft repair services?
- How often does the business re-evaluate its privacy and data security policies and procedures?
- Does the business have a comprehensive record retention/destruction policy?

This list is by no means exhaustive, but it raises some of the key issues related to the privacy and data security environment in an organization. As this area develops, businesses and insurance carriers alike will need to develop ways to better assess and minimize the risk of harm to one of the most vital assets in business today – information.

FOOTNOTES

- ¹ The site <http://www.privacyrights.org/ar/ChronDataBreaches.htm> provides a chronological list of reported data breaches since February 2005. According to this site, during this time more than 100 million records have been affected.
- ² See, e.g., *Mannacio v. General Electric Co., et al.*, Cal. Super. Ct., CV-065227 (Dec. 5, 2006).
- ³ 45 CFR Parts 160, 162 and 164.
- ⁴ 45 CFR § 160.103
- ⁵ 15 USC § 6801 *et seq.*
- ⁶ N.Y. Gen. Bus. § 399-dd(2).
- ⁷ N.Y. Gen. Bus. § 399-dd(4).
- ⁸ N.Y. Gen. Bus. § 399-dd(3).
- ⁹ Cal. Civ. Code § 1798.85; Conn. Gen. Stat. § 42.470; 815 Ill. Comp. Stat. § 505/2QQ; Mo. Rev. Stat. § 407.1355; Tex. Bus. & Com. Code Ann. § 35.58.
- ¹⁰ See, e.g., Cal. Civil Code § 1798.82 *et seq.* (effective July 1, 2003); Conn. Gen. Stat. Ann. § 36a-701b *et seq.* (effective Jan. 1, 2006); Fla. Stat Ann. § 817.5681 *et seq.* (effective July 1, 2005); 815 Ill. Comp. Stat. Ann. 530/1 *et seq.* (effective Jan 1, 2006); N.J. Stat. Ann. § 56:8-163 (effective Jan 1, 2006); N.Y. Gen. Bus. § 899-aa *et seq.* (private entities), N.Y. State Tech. § 208 *et seq.* (state entities) (effective Dec. 7, 2005); Tex. Bus. & Com. Code Ann. § 48.001 *et seq.* (effective Sept. 1, 2005).
- ¹¹ These incidents, among others, are reported at <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.
- ¹² Cal. Civ. Code § 1798.81.5.
- ¹³ Tex. Bus. & Com. Code Ann. § 35.48.
- ¹⁴ N.Y. Gen. Bus. § 399-h and Cal. Civ. Code § 1798.81.

This article originally appeared in the 2007 April PLUS Journal. For more information, contact PLUS at 800-845-0778 or 952-746-2580.

The mission of the Professional Liability Underwriting Society is to enhance the professionalism of its members through education and other activities and to responsibly address issues related to professional liability. PLUS was established in 1986 as a non-profit association with membership open to anyone interested in the promotion and development of the professional liability industry.



As a nonprofit organization that provides industry information, it is the policy of PLUS to strictly adhere to all applicable laws and regulations, including antitrust laws. PLUS *Journal* is available free of charge to members of the Professional Liability Underwriting Society. Statements of fact and opinion in this publication are the responsibility of the authors alone and do not imply an opinion on the part of the members, trustees, or staff of PLUS.

The Journal is protected by state and federal copyright law and its contents may not be reproduced without written permission.