Privacy and EIM Alert

Data Breach Laws Become Even Stricter For All Companies With California Or Massachusetts Customers Or Users

BY ROBERT D. BROWNSTONE AND DAVID MARTY

MARCH 7, 2012

Fenwick
FENWICK & WEST LLP

INTRODUCTION

How can a 21st century U.S. company do its best to comply with data-security-related obligations imposed by the various laws of 46 states? (Only Alabama, Kentucky, New Mexico, and South Dakota have not enacted laws requiring companies to provide notice of a data breach.) A company can implement practices and procedures designed to achieve maximum compliance with the laws adopted by the two states widely acknowledged to impose the strictest obligations: California and Massachusetts. In 2012, in different ways, these two states' respective regulatory schemes addressing data breaches have become even stricter.

I. California: Incident-Response Requirements Stricter as of January 1, 2012

A. Background

Over the past decade, California has enacted, and then amended incrementally, notice-of-breach laws designed to prevent identity theft. The first of such laws, enacted in 2002, is commonly referred to as S.B. 1386. California's notice-of-breach statutes, including S.B. 1386, apply to all companies that conduct business in California (as well as to state and local governmental agencies). From day one those statutes, including Cal. Civ. Code § 1798.82, have protected every California resident's electronic personally identifiable financial information (PII) by requiring notice to the affected individuals whose sensitive PII stored in unencrypted form is hacked, lost or otherwise compromised (a "data breach").

The geographical location of that information is irrelevant, as is whether the PII possessor outsources storage to a service provider. Thus, the protection cuts a broad swath in the borderless universe of 21st century e-commerce in which most every company stores, or outsources storage of, information on consumers from all over the country. As with the notice-of-breach laws in most other states, California's statutes have always had an automatic notice trigger once certain PII – a name coupled with other sensitive confidential information – has been compromised. There is no requirement that the company owning the data first assess the extent of the risk of identity theft created by the data breach.

In 2008, A.B. 1298 expanded the scope of the California notice-of-breach laws to encompass a California resident's "medical information" and "health insurance information." Acknowledging modern heightened confidentiality concerns – such as medical and health-insurance identity theft – the post-2008 version of the California notice-of-breach laws applies even in situations in which HIPAA, the primary federal statutory regime directed at protecting personal health information, does not apply.

B. New as of January 1, 2012: Two Additional Incident-Response Requirements

1. Attorney-General Notification

Despite its overall strict statutory scheme as to data breaches, until recently California law did not require that notices of large-scale data breaches also be sent to the state Attorney General ("state AG"). Effective January 1, 2012, however, California joined 18 other states that *do* have such a requirement. S.B. 24, signed into law late last year by Governor Jerry Brown, includes a directive that whenever a data breach encompasses the personal financial and/or health information of more than 500 individuals, the state agency or company maintaining the compromised data must also notify the state AG.

2. Specificity as to Breach's Facts and Circumstances

In addition to requiring state AG notification for data breaches that affect more than 500 individuals, S.B. 24 added a number of specific factual items that must appear in *every* notice of breach, regardless of the number of individuals affected. Effective January 1, 2012, every notice of a data breach must include these details:

- "[a] list of the types of personal information that were or are reasonably believed to have been the subject of a breach;"
- "[i]f . . . possible to determine at the time the notice is provided, then any of the following: . . .the date [,] . . . estimated date . . . or date range within which the breach occurred;" and
- "[a] general description of the breach incident, if that information is possible to determine at the time the notice is provided."

At its option, the company that suffers the data breach may also include in the notice "[i]nformation about what the person or business has done to protect individuals whose information has been breached [and] . . . [a]dvice on steps that [each such individual] may take to protect himself or herself.

C. Practical Consequences and Tips

For various reasons, of course it behooves every organization to do its best to protect its customers/users/subscribers – and its employees – from identity theft. From a risk-management perspective, no company wants to be in the position of having to address the consequences of a data breach. Those ramifications typically include: statutory penalties; incident-response costs; large monetary outlays to cover statutory fines and/or customary voluntary remedies such as credit-rating freezes for the individuals whose PII was compromised; and a publicity/PR hit in the court of public opinion.

In light of S.B. 24, the mandated incident-response may now also include notifying the state AG. In addition, S.B. 24's "general description" requirement is likely to render the contents of every (large or small) breach notification quite embarrassing. Having to explain how a breach occurred could, in effect, result in a company reluctantly having to provide its customers with insight into the deficiencies of the company's information security practices that allowed a data breach to occur.

Any entity maintaining California residents' PII in electronic form should not wait to address information security until it is in reactive, apologizing incident-response mode. Regardless of its size or its type of business, every company can take various technological and practical measures proactively to decrease the risk of a data breach occurring. For example, employing data encryption – especially on portable devices and media – will not only protect the underlying information but also preclude the triggering of a statutory notification duty if the data is ever compromised.

II. Massachusetts: Service-Providers' Contractual Duty to Comply with Data Regulations – Exemption Expires March 1, 2012

A. Background

On March 1, 2010, the Massachusetts Office of Consumer Affairs and Business Regulations (OCABR) promulgated regulations that expanded upon and implemented the state's "Security Breach" statutory scheme. These "Standards for the Protection of Personal Information of Residents of the Commonwealth" imposed various strict information-security obligations on any company that owns or licenses the personal information of Massachusetts residents. These obligations include the maintenance of a comprehensive Written Information Security Program ("WISP") describing the safeguards that have been, or will be, put in place for the protection of PII.

B. New as of March 1, 2012: Service Provider Agreements – Exemption Expires

March 1, 2012 marked the deadline for any company that owns or licenses PII regarding a Massachusetts resident to include data security provisions in all of its agreements with service providers to which the company transmits such PII. On March 1, 2012, an important provision, which had exempted previously existing service provider agreements from this requirement, expired. As a result, many longstanding service provider agreements will now need to be revised to comply with the OCABR's 2010 standards.

Companies that are subject to OCABR's Standards for Protection of Personal Information – by virtue of owning or licensing the PII of Massachusetts residents – and that are a party to service provider agreements executed prior to March 2, 2010 will need to revise those agreements to require *the service providers themselves* to comply with the data security obligations of OCABR. Although OCABR establishes somewhat flexible compliance standards based upon the size of the business, the type of PII it accesses, and the resources available to it, OCABR also sets forth certain very specific obligations that apply directly to companies that are subject to these regulations *and,* contractually, to their service providers as follows:

- Companies subject to the OCABR standards, and their service providers, should develop, implement, and maintain a comprehensive WISP describing the administrative, technical, and physical safeguards that have been, or will be, put in place for the protection of PII.

- The WISP should designate one or more employees to maintain the information security program.

- The WISP should identify and assess foreseeable security risks to stored PII.

- The WISP should contain data security policies for employees to follow as well as disciplinary measures and responsive actions that should occur in connection with any violation or breach of the security program.

- The WISP should address and provide for annual review of implemented security measures.

Although the March 1, 2012 expiration of the OCABR exemption will affect only agreements signed prior to March 2, 2010, the expiration of this exemption marks the final stage in the complete implementation of these regulations. Accordingly, companies that own or license PII regarding a Massachusetts resident should take this opportunity to consider, not only whether longstanding service provider agreements need to be revised, but also whether the companies themselves are, in fact, in compliance with the data-security obligations imposed by regulations.

To learn more about the requirements of OCABR's "Standards for the Protection of Personal Information," companies can refer to information on Massachusetts's Consumer Affairs and Business Regulation page.

Conclusion

In the data-breach realm, a legally defensible approach rests heavily on in-the-trenches deployment of appropriate information-technology and data-security tools and processes. Those same data-breach prevention measures can comprise a baseline for compliance with other privacy-related regulatory regimes. For further information or guidance about compliance with California or Massachusetts data-breach laws or with the many other federal and state privacy statutes, please contact: either of the authors of this Alert, Robert Brownstone or David Marty; or one of their colleagues in Fenwick & West's Privacy & Information Security or Electronic Information Management (EIM) Groups.

Robert D. Brownstone is the Technology & eDiscovery Counsel and the Co-Chair of the Electronic Information Management (EIM) Group at Fenwick & West LLP, a 300-attorney Silicon-Valley-headquartered law firm specializing in representing prominent high-technology and life-sciences companies. Mr. Brownstone is a nationwide advisor, presenter and writer on many law-and-technology issues, including privacy and information-security. He is often quoted in the press as an expert on electronic information. Mr. Brownstone can be reached at rbrownstone@fenwick.com or 650.335.7912.

David Marty is an associate in the Litigation and Privacy & Information Security Groups at Fenwick & West LLP. Mr. Marty's practice often focuses on copyright and data privacy issues. He can be reached at dmarty@fenwick.com or 650.335.7282.