

## **Is Your Client Prepared To Comply With the Data Security Breach Notification Laws?**

By Alan M. Mansfield, Editor ABTL Report  
Rosner & Mansfield LLP

It is now part of routine life that consumers receive a letter from a financial institution advising them that personal data in a third party's possession has been compromised and that they may need to take steps to protect themselves from identity theft. Or read in the news that a laptop or flash key with personal medical information or client data has been lost. Or for a company to learn, as the nationwide retailer T.J. Maxx recently revealed, that its customer data base with over 45 million names, credit card and driver's license information has been accessed from outside sources, and now the company must take immediate steps to remedy the situation.

This is not an isolated or theoretical issue for companies and consumers. According to [www.attrition.org/data\\_loss](http://www.attrition.org/data_loss) and [www.privacyrights.org/ar/ChronDataBreaches](http://www.privacyrights.org/ar/ChronDataBreaches), over 100 million consumer records have been compromised in close to 1,000 separate incidents since 2004. The U.S. Department of Justice reports that over 3.5 million consumers are the subject of identity theft *each year*, while the U.S. Federal Trade Commission places that figure closer to nine million individuals annually. If you have been one of those unfortunate victims, you know that the time and money necessary to remedy such a breach is significant. Studies have reported that the average identity theft victim spends between \$400 and \$880 and between 40 and over 300 hours to rectify problems caused by identity theft.

The corporate costs of remedying such a breach are also expensive. According to a recent study by the Ponemon Institute of Michigan, the average corporate cost of a data breach is \$182 per compromised record, and the average company cost per data breach incident is \$4.8 million – with insurance coverage for such losses available but highly variable. In the T.J. Maxx situation, for example, the company is now a defendant in at least seven federal and state class action lawsuits, the subject of over a dozen state Attorneys General informal investigations, and claims to have hired more than 50 security experts (and who knows how many lawyers) to investigate security breaches that went on for over a year, presumably undetected.

What started all these revelations? What do they mean? And, most significant, what can be done to prevent them? The short answer – data breach security notification laws, first adopted in California in 2003 and now adopted in a majority of states, require companies to make immediate and significant disclosures if data security breaches take place.

### **What Are Data Security Breach Notification Laws?**

Many of us have heard about the privacy components of the Gramm-Leach-Bliley Act, HIPAA or the Sarbanes-Oxley Act. These federal laws protect different types of personal information from unauthorized access or use, as well as requires disclosure of certain corporate privacy policies. Data security breach notification laws address the issue of what happens when privacy protection measures adopted to protect such data have been compromised.

California adopted the first data security breach notification law, codified at Cal. Civ.

Code Section 1798.80 *et seq.*, effective July 1, 2003. 33 other states have since adopted similar laws modeled after, but not the same as, the California law. Presently pending in Congress are several bills that would adopt a variant of the California model on a nationwide basis, including the Notification of Risk To Personal Data Act of 2007, S.239 (introduced January 10, 2007).

In general, these laws require a company notify law enforcement agencies and consumers if the company learns that personal consumer information has been compromised. Since California was the first to adopt these laws, this article highlights the California law.

First, what data are protected? Any personal, non-public information that has not been encrypted and includes a person's first name or initial and last name plus a wide variety of data, including their Social Security Number, driver's license number, or financial account number in combination with any password that would permit access to a financial account, is covered by the statute. Cal. Civ Code Section 1798.82(e). According to the California Office of Privacy Protection, the vast majority of reported breaches involve Social Security Numbers.

Second, who is covered? Any entity that conducts business in California and owns, licenses or otherwise maintains computerized data about a customer or client located in California is subject to these statutory provisions. Civil Code Section 1798.81.5(e), which addresses a different issue about maintaining reasonable security procedures, provides a list of entities that are governed by other laws and thus may be exempt from some statutory requirements. Unlike other states, these California laws also cover government agencies.

Third, what must companies do if they become aware of a breach? Companies must notify any resident of California whose unencrypted personal data were, or are reasonably believed to have been, acquired by an unauthorized person that a security breach has taken place. Pursuant to Section 1798.82(g), this notification can be accomplished by written notice, electronic notice, or, if the cost of providing notice would exceed \$250,000 or involve more than 500,000 persons, a combination of email notice, "conspicuous posting" of the notice on the Web site page and notification to major statewide media. The form of that notice is discussed *infra*.

Fourth, when must companies undertake this notification effort? According to Section 1798.82(a), companies must accomplish this notification "in the most expedient time possible and without unreasonable delay". What does this mean? The California Office of Privacy Protection recommends such notification be accomplished within 10 business days after learning about the breach, depending on the sensitivity of the data. However, if a company believes the unauthorized access may be the result of a crime, this notification obligation may be delayed if a law enforcement agency first determines notification will impede a criminal investigation. Cal. Civ. Code Section 1798.82(c). Thus, a company should immediately (within a day or two) give notice of the relevant facts to appropriate state and/or federal law enforcement agencies so that the agency can first ensure any notification will not compromise their investigation prior to the company implementing a notification program.

Because these data security breach notification laws differ from state to state, a multi-state business needs to immediately consider numerous factual and legal issues if a data breach occurs. Where was the data lost? Where are the clients or customers whose data were compromised located and are there data security breach notification laws in those states? If

possible, where can the data breach be traced to? Answers to these questions are critically important to determine, because simply relying on the law of the state where the business is located may not be the answer.

Multiple laws could apply depending on the residence of the individual whose data were compromised, triggering a potential conflicts analysis. This issue was recently recognized in *Kearney v. Salomon Smith Barney*, 39 Cal. 4<sup>th</sup> 95 (2006), where a conflict between Georgia and California law on a privacy issue was resolved in favor of partially applying California law due to California's significant interest in protecting the privacy of its residents. The Court permitted a class claim for injunctive relief, but not damages, to proceed. The Court applied California law in part based on its conclusion that California "repeatedly has enacted new legislation in related areas in an effort to increase the protection of California consumers' privacy in the face of a perceived escalation in the impingement upon privacy interests caused by various business practices." *Id.* at 125.

While most of these laws may not directly conflict, some states have a safe harbor provision and some do not. Some have different time periods in which officials and consumers should be notified of a breach. Some apply to government agencies and some do not. Some require different information be contained in the notification letter. Thus, a company needs to quickly determine what state laws may apply in order to assess what its specific obligations may be. Because of the sensitivity of the data and the laws that come into play, this is not a question that can be resolved in weeks – this is a question that must be resolved within days after learning about the possible breach. The following links to other state laws are a helpful resource for quickly reviewing these laws' similarities and differences:

[www.consumersunion.org/campaigns/Breach\\_laws\\_May05.pdf](http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf) (compiled by Consumers Union); and [www.ncsl.org/programs/lis/cip/priv/breach.htm](http://www.ncsl.org/programs/lis/cip/priv/breach.htm) (compiled by the National Conference of State Legislatures).

### **What Can Entities And Consumers Do To Protect Themselves?**

Any entity that maintains personal consumer data in computerized format needs to undertake several important proactive measures before any breach event may occur: (1) understand what data they possess, (2) review the security of their data, and (3) adopt a data breach notification policy.

While the first step sounds simple, non-technical management within companies are sometimes surprised to learn what data they actually possess. Thus, an important threshold issue is to ensure that key management knows what information is collected that falls under the applicable security breach notification laws. Many companies, including large corporate retailers, do not have a good idea of what information they have collected from, or about, their customers. A company data audit is a good place to start.

As to the second issue, privacy officers marvel (or shiver) over how much personal data their companies actually retain. Some companies report having set a default mechanism for electronically stored data so that customer data is not deleted for 99 years! Data are maintained on active hard drives that may be downloaded on to laptops or flash keys. If that laptop or flash

key is lost, stolen or misplaced (which has resulted in close to 50% of the data notification events), that may trigger the need to comply with the data security breach notification laws. Companies need to know: 1) what data are maintained, 2) for how long and on what systems, 3) whether such data are segregated and/or encrypted, 4) what data can be downloaded to personal devices, 5) who can access or download such data and 6) how access to such data is monitored.

For some guidance on these data security protection issues, ISO 17799 entitled “Information Technology – Security Techniques – Code of Practice For Information Security Management” provides a nationally recognized data security reference standard. In addition, the FTC just recently issued a brochure entitled “Protecting Personal Information: A Guide for Business”, located at [www.ftc.gov/bcp/edu/pubs](http://www.ftc.gov/bcp/edu/pubs), which contains five key principles for companies to follow in developing a plan for securing personal information.

One of the best sources of information on how to comply with the data security breach notification laws (at least in California, and as a model for elsewhere) is available through the California Office of Privacy Protection. This Office has prepared and recently revised a brochure available at [www.privacy.ca.gov/recommendations/secbreach.pdf](http://www.privacy.ca.gov/recommendations/secbreach.pdf) entitled “Recommended Practices on Notice of Security Breach Involving Personal Information”. This brochure provides businesses and consumers with: 1) a summary of the California data security breach notification law, 2) preventative practices to adopt, 3) sample letters to send to consumers, and 4) what government agencies to contact. The latter are extremely important to consider, since many states (including California, see Cal. Civ. Code Section 1798.82(g)) have adopted a safe harbor provision for companies that have adopted their own security and notification procedures as part of a pre-data breach program that makes following those notification procedures *per se* compliance with that state’s notification law.

If your company or client has not adopted these protections and a data breach occurs, the best advice you can give is to gather information quickly. Who lost the data or how was the data compromised? Was the data lost, stolen or hacked? Can you trace definitively what data were lost or accessed? Where are the customers or clients whose data were compromised located? What state or federal government agencies may need to be immediately notified? Once you gather the answers to these questions, you can better assess and advise what laws may apply, what form the notification can take and how to ensure compliance.

In California there is no case law yet on what constitutes compliance with these statutes, so this is an area for future case law development. This will include cutting edge issues such as 1) whether failure to adopt such policies or follow the statutory requirements constitutes negligence *per se* or an unlawful business practice if required by statute, 2) conversely, if the safe harbor can be invoked does that create immunity from suit, 3) what type of liability can flow if a data breach occurs, and 4) what to do in the event a conflict of laws exist. These are important issues to consider and analyze in advising your clients.

If you receive one of these letters and it indicates your Social Security Number has been compromised, an important first step is to contact the three major credit reporting agencies (Experian, TransUnion and Equifax) to place a fraud alert on your credit report. You are entitled by law to one free annual credit report, so it is also a good idea to request a report to make sure

no incidents have immediately arisen. You can request such a report through [www.annualcreditreport.com](http://www.annualcreditreport.com). Sometimes banks will cancel and re-issue credit or debit cards if financial account information is disclosed, so consumers should also contact any relevant financial institutions. Finally, the California Office of Privacy Protection, the public interest group the Privacy Rights Clearinghouse, and the FTC all have available free information on their website listing steps consumers can take to protect themselves in the case of identity theft or compromised data due to a data security breach.

### **Conclusion**

In the 21<sup>st</sup> Century even data that are not made available on the Internet can be compromised. In fact, most breaches are decidedly “low tech”, the result of losing or misplacing a lap top computer or CD-ROM. How corporate entities protect and treat personal consumer data – and that goes for retailers, government agencies, and even law firms – is a critical component of their corporate data security practices. Ideally entities will proactively manage, encrypt and/or delete unnecessary or outdated personal data they gather and retain. However, companies must have both an understanding and a plan about what to do if personal data in its possession are compromised. Having such policies in place not only makes good legal sense and can limit potential liability, but also is critical to avoid spending potentially millions of dollars and untold customer good will in the unfortunate event data are compromised.

©Alan M. Mansfield 2007. All Rights Reserved.