SEYFARTH SHAW

MANAGEMENT ALERT

May 28, 2003

Failure to Report Unauthorized Access of Customer or Employee Information Could Lead to Liability Under New California Identity Theft Law — *California's Law Could Become Model For National Law*

Identity theft is now the fastest growing crime in the United States. As a consequence, measures to address it are the subject of parts of the Homeland Security Act and several bills recently introduced in Congress. California, however, has already enacted a soon-to-be effective statute that is intended to combat the crime by requiring businesses to notify individuals that their confidential information has been compromised. The statute is predicated on the theory that, when armed with notice that information sufficient to steal their identity has been compromised, individuals can take steps to avoid the consequences of full-fledged identity theft. Regardless of the merit of that premise, all agencies, persons or companies that store confidential information of California residents will have a new statutory hurdle to face this summer, and other states are considering similar measures.

California's new statute — California Senate Bill 1386 (SB 1386) — is effective July 1, 2003. It requires companies that store computerized personal information (such as Social Security or account numbers) to provide immediate notice if the security of that information is compromised, for example, if a hacker or employee improperly obtains information. This reporting requirement applies even if no information is taken, and authorizes civil lawsuits for damages and injunctive relief should a breach go unreported.

If you think this could not happen to you — think again! Recently, an employee of a Fortune 100 consumer product company slipped into the company's computer system without authorization and downloaded salary information and Social Security numbers of about 450 co-workers. The company acted responsibly and sent an e-mail advising employees to check bank accounts and credit card balances for anything unusual. The new California law may require more stringent notice.

Like most privacy protection laws, this statute is likely to have effects that are more widespread than originally intended. Because compliance with the law will be extremely difficult without advance planning, it is critical for businesses located or doing business in California to understand the law and its impact as soon as possible to avoid potentially expensive issues down the road.

What kinds of companies does SB 1386 affect?

The law applies to "[a]ny agency" and "[a]ny person or business that conducts business in California." As a result, regardless of the form of your business, or its location, the law applies if you own or license computerized data regarding residents of California. In other words, it does not matter whether a business maintains an office in California. So long as the business owns or licenses a database that includes information regarding at least one California resident, such as customer and employee information, the law applies.

What kind of information does SB 1386 affect?

SB 1386 applies to "personal information," namely the first name (or initial) and last name of an individual coupled with any one or more of the following "data elements":

- Social Security number; OR
- Drivers license number or California identification card number; OR
- Account number or credit or debit card number, if it is coupled with any security code, access code or password that would allow access to the account.

Presumably, if there were no access code or password required to obtain access to an account, then all that would be required to invoke SB 1386 would be data that includes both a customer name and account number. Thus, while identity theft is most often associated with the loss of a Social Security number or credit card, it is possible that SB 1386 would reach those companies that maintain databases of customer or employee names and account numbers for non-financial reasons. The law does provide one method of avoiding its impact: It only applies if either the name or the "data element" is unencrypted. As a result, if all personal information is maintained in a fully encrypted database, it may avoid the reach of SB 1386.

What is a security breach?

A breach under SB 1386 is defined quite broadly. It means any "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal

SEYFARTH ATTORNEYS SHAW

information." This could mean unauthorized access by an employee, vendor or third party. Moreover, it applies to any situation in which personal data was taken, or was "reasonably believed to have been" taken. Thus, a company is required to comply with the notice requirements of SB 1386 even if no information was actually obtained.

What must be done in the event of a security breach?

The notice requirement forms the crux of SB 1386. A breach must be disclosed to every affected person in "the most expedient time possible" after a breach is discovered, and "without unreasonable delay." Disclosure of the breach must be made either by written notice or electronic notice in compliance with the federal electronic signature law (15 U.S.C. Section 7001). In the event that more than 500,000 individuals would need to be notified, or the notification will cost more than $250,000, or the company does not have sufficient contact information to send written notice, the company may fulfill the notification requirement by a) sending an e-mail notice to each affected person, b) posting a "conspicuous" notice on its website, and c) notifying "major statewide media."

The law provides one exception to providing immediate notice: If providing notice would interfere with law enforcement activities, then the notice may be delayed until after the law enforcement authorities determine such notice will not harm their investigation.

What is the penalty for non-compliance?

SB 1386 provides that any person "injured" by a violation of the law may file a civil action to recover damages and seek injunctive relief. When coupled with California's fairly liberal consumer protection laws and the ease by which a class action may be certified, this provision of the law is likely to lead to the filing of class action lawsuits whenever a security breach is discovered. The risk of such expensive litigation can only be mitigated through careful advance planning.

What can be done in advance?

There are several ways in which persons or companies doing business in California could limit the effect of SB 1386. First, if it is technologically possible and economically feasible, it may make sense to store all personal information in encrypted format. Second, companies should take steps to evaluate and increase the security of their computer systems in order to prevent unauthorized access. Third, companies should develop a contingency plan for investigating and providing the required notice, perhaps as an adjunct to their normal communication with their customers. As part of this, companies should develop contacts with local and national law enforcement as well as consider the public relations aspects of making such a notification. Fourth, if appropriate, companies should take the necessary steps to have customers (and employees) agree in advance to receiving notice via e-mail.

Of course, all steps taken by companies must be reviewed in light of their current business objectives and the costs of increasing security and preparedness. Nonetheless, given the broad and vague language of SB 1386, and the express provisions for civil damages and injunctions, it would behoove all companies doing business in California to take a studied and thorough review of systems and procedures prior to July 1, 2003. This is already a requirement for businesses in the financial services and health care industry, and is likely to become an across-the-board industry standard and a national legal requirement.

Seyfarth Shaw is pleased to announce that Patrick Zeller, Former Director of the State of Illinois Computer Crime Institute has joined our Privacy/Security/ Cybercrime Team.

If you have questions regarding SB 1386 or best practices in the data privacy and security areas, please contact Ken Wilton at 310-201-5271 or Bart Lazar at 312-269-8986. This newsletter is a periodical publication of Seyfath Shaw and should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The contents are intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have.

ATLANTA
One Peachtree Pointe
1545 Peachtree Street , N.E., Suite 700
Atlanta, Georgia 30309-2401
404-885-1500
404-892-7056 fax

BOSTON
Two Seaport Lane, Suite 300
Boston, Massachusetts 02210
617-946-4800
617-946-4801 fax

CHICAGO
55 East Monroe Street, Suite 4200
Chicago, Illinois 60603-5803
312-346-8000
312-269-8869 fax

HOUSTON
700 Louisiana Street, Suite 3850
Houston, Texas 77002-2731
713-225-2300
713-225-2340 fax

LOS ANGELES
One Century Plaza
2029 Century Park East, Suite 3300
Los Angeles, California 90067-3063
310-277-7200
310-201-5219 fax

NEW YORK
1270 Avenue of the Americas, Suite 2500
New York, New York 10020-1801
212-218-5500
212-218-5526 fax

SACRAMENTO
400 Capitol Mall, Suite 2350
Sacramento, California 95814-4428
916-448-0159
916-558-4839 fax

SAN FRANCISCO
101 California Street, Suite 2900
San Francisco, California 94111-5858
415-397-2823
415-397-8549 fax

WASHINGTON, D.C.
815 Connecticut Avenue, N.W, Suite 500
Washington, D.C. 20006-4004
202-463-2400
202-828-5393 fax

BRUSSELS
Boulevard du Souverain 280
1160 Brussels, Belgium
011-32-2-647-60-25