A.S.A.P.™

A LITTLER MENDELSON TIME SENSITIVE NEWSLETTER

IN THIS ISSUE

JUNE 2003

Effective July 1, 2003, Employers Are Required to Notify California Residents Whose Unencrypted Personal Information May Have Been Misappropriated from the Employer's Computer Network or Databases.

THEFT OF COMPUTERIZED PERSONAL INFORMATION WILL TRIGGER NEW NOTICE OBLIGATIONS FOR EMPLOYERS CONDUCTING BUSINESS IN CALIFORNIA

By Nancy L. Ober and Dylan W. Wiseman

Effective July 1, 2003, a data security law intended to combat identity theft will impose new notice obligations and liability exposure on California employers who store personal information about employees or customers in computer databases. Last year hackers accessed the state controller's payroll database containing personal and financial information about thousands of employees, including state legislators. The breach went unreported for several weeks after it was detected. SB 1386 followed.

PROTECTION OF PERSONAL INFORMATION

SB 1386 requires any person or business that conducts business in California, as well as any state agency, to notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. "Personal information" means an individual's name and one or more of the individual's (1) social security number; (2) driver's license or California identification card number, or (3) account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to the individual's financial account.

NOTICE OBLIGATION UPON SECURITY BREACH

The notice obligation is triggered when the owner or licensee of computerized data discovers or is notified of a security breach. A security breach occurs upon unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information. Good faith acquisition of personal information by an employee or agent of the business for the purposes of the business is not a security breach, provided that the employee or agent does not use or make further unauthorized disclosure of such information.

TIMING OF NOTICE

The owner or licensee of the data must give notice of the security breach in "the most expedient time possible," without unreasonable delay. A person or business that maintains the data for the owner or licensee must notify the owner or licensee of the breach immediately following discovery. Notice to individuals may be delayed, however, if a law enforcement agency determines that notice will impede a criminal investigation, or if additional time is needed to determine the scope of the breach and restore the integrity of the system.

FORM OF NOTICE

SB 1386 specifies how notice must be given. The permitted methods include written notice, electronic notice or substitute notice. Substitute notice is only

allowed if the business demonstrates that the cost of providing notice would exceed $250,000, or that the affected class to be notified exceeds 500,000 persons, or that the person or business giving notice does not have sufficient contact information. Substitute notice consists of all of the following: e-mail notice, conspicuous posting on the business's website and notification to major statewide media.

However, SB 1386 permits a business that maintains its own notice procedure as part of its information security policy to give notice in accordance with that policy, provided that the policy provides for notice consistent with the timing requirements of SB 1386.

PENALTIES

Any "customer" who is injured by a violation of SB 1386 may bring a civil action to recover damages and an injunction to stop the violation. It is unclear whether "customers" permitted to file a civil lawsuit include non-customer employees whose personal information is misappropriated.

Because a breach of data security may affect many individuals, any litigation may take the form of a class action. Finally, the rights and remedies under SB 1386 are cumulative to other rights and remedies available under law.

RECOMMENDED ACTIONS TO PREPARE FOR SB 1386

Employers doing business in California should take several steps to prepare for SB 1386. First, determine what "personal information" of employees or customers residing in California is stored in unencrypted form in company databases. Second, review the company's data security systems and policies to determine whether they reasonably protect against unauthorized access. Employers should not overlook internal as well as external security measures: Recent statistics show that over 70% of misappropriated computerized data is taken by current employees. The company's security policies should include actions to be taken in the event of a security breach (discussed below).

Third, review any agreements with vendors or licensees who maintain databases with personal information and ensure that such agreements require the vendor to notify your company immediately of any unauthorized access, and to indemnify your company if it fails to do so. Fourth, train IT employees and others who maintain the security of the system to identify security breaches. Fifth, determine whether your existing data security policies require notice to individuals who may be affected by unauthorized access to their personal information. If so, ensure that such notice provisions are compliant with the notice timing provisions of the new law; if not, consider designating the company's own form of notice, consistent with the timing requirements of SB 1386. Sixth, consider encrypting any information that comes within SB 1386's definition of "personal information" — if the information is encrypted, it is not personal information under SB 1386 and the notice obligations do not apply. (However, SB 1386 does not specify what level of encryption is sufficient to avoid triggering its notice requirements.)

RECOMMENDED STEPS IN THE EVENT OF A SECURITY BREACH

If you, as the employer, discover, or reasonably suspect, that a security breach involving personal information has occurred, it is important to have a plan of action in place to preserve evidence. Personal information stored on databases may include customer lists or other confidential information, and may be an employer trade secret. In addition to civil remedies for misappropriation that may be available to the employer, the theft of computerized information is a crime under Penal Code section 502.

Never allow the company's own IT personnel to conduct a forensic assessment. Allowing the company's own personnel to conduct such work will contaminate the chain of custody of the evidence. As a result, it may be difficult or impossible to pursue a damages or injunctive action for misappropriation of trade secrets, and most law enforcement agencies will not take action upon learning that the company's own IT personnel handled the evidence.

Upon discovering an apparent security breach, the employer should seek legal advice and retain qualified forensic technicians to conduct a technical assessment. If a breach is confirmed, the employer with legal and technical support can then plan a course of action to comply with SB 1386 and, if warranted, seek an injunction to prevent further use or disclosure of personal information.

A PRELUDE TO FEDERAL LEGISLATION?

While SB 1386 only protects California residents, in actual practice it is likely to have national effect. It will be difficult for multistate companies to draw the line at notifying only California residents in the event of a security breach of their networks. In addition, Senator Feinstein has made it known that she intends to introduce similar legislation in Congress.

Nancy L. Ober is a shareholder in Littler Mendelson's San Francisco office and Dylan W. Wiseman is a senior associate in Littler Mendelson's Sacramento office. If you would like further information, please contact your Littler attorney at 1.888.Littler, info@littler.com, Ms. Ober at nlober@littler.com, or Mr. Wiseman at dwiseman@littler.com.

ASAP™ is published by Littler Mendelson in order to review the latest developments in employment law. ASAP™ is designed to provide accurate and informative information and should not be considered legal advice. ©2003 Littler Mendelson. All rights reserved.

THE NATIONAL EMPLOYMENT & LABOR LAW FIRM™

1.888.littler www.littler.com info@littler.com

ASAP™ is published by Littler Mendelson in order to review the latest developments in employment law. ASAP™ is designed to provide accurate and informative information and should not be considered legal advice. ©2000 Littler Mendelson. All rights reserved.