LOS ANGELES
Daily Journal

MONDAY,
JULY 10, 2006

SINCE 1888

OFFICIAL NEWSPAPER OF THE LOS ANGELES SUPERIOR COURT AND UNITED STATES SOUTHERN DISTRICT COURT

Focus

Employers Need Master Plan to Protect Privacy of Personal Data

By John Nadolenco & Francisco Ochoa

California statutes require employers to safeguard the personal and private information that they obtain from their employees, including employees' medical information, credit information, and Social Security numbers. Employers store much of this information electronically to increase the manageability of the information.

Recent headlines, however, also highlight the risk companies now face from the involuntary disclosure of such information. For example, it was reported in May of this year that the United States Department of Veterans' Affairs announced that a thief had stolen a laptop with the names, Social Security numbers, and birth dates of up to 26.5 million veterans. Apparently, this information, which reportedly has now been recovered, was maintained electronically on a laptop that was taken from the home of a VA employee. Just a few days earlier, a similar article reported that the American Institute of Certified Public Accountants announced that it had lost a hard drive containing the personal information of approximately 300,000 of its members.

Private employers have faced similar issues. Reports appeared in April of this year indicating that data protection and storage company Iron Mountain admitted losing back-up tapes for two of its customers, including one tape containing the private information of approximately 17,000 employees of the Long Island Rail Road Co. Similar reports indicated that in February 2005, approximately 10,000 employees of McAfee Inc. - a software company - learned that an unencrypted CD containing their personal information was lost by an external auditor who left the CD on an airplane. One Internet site lists approximately 174 information security breaches that have been disclosed since February 2005. See www.privacyrights.org.

As these examples indicate, the strictest data and personnel policies will probably not be able to preclude all breaches of private information. As a result, employers should assess their own policies and procedures and develop an approach to responding to any such breaches. In formulating a planned response, here are some of the factors employers should consider:

Stop the breach: Upon learning that private employee information has been compromised, the first step is to take all reasonable steps to prevent further breaches. Depending on the circumstances, this may require communication with the company's IT department, as well as notifying law enforcement and, in some cases, the company's regulators.

Mandatory disclosure: Next, companies and their attorneys should evaluate whether any notification or disclosure to the affected individuals is required. Several states have adopted mandatory disclosure laws. In California, for example, the Civil Code requires that employers who own or license computerized data that includes unencrypted personal information disclose any breach of their system's security when the breach is discovered or when the employer is notified of the breach. Personal information is defined as an individual's first name or initial and last name combined with an unencrypted Social Security number; driver's license or California identification number; or financial account, credit card or debit card number combined with any access code or password that could allow access to the individual's finances. The disclosure must be made as soon as possible and without unreasonable delay; however, the timing of the disclosure can take into account the needs of law enforcement. The Civil Code requires written or electronic notice or, in certain circumstances, notice by e-mail, Web-site posting or by major statewide media.

Since July 1, 2003 — when California adopted its security-breach-disclosure law - at least 22 states have passed similar laws. See www.vigilantminds.com. While federal law does not currently require disclosure of security breaches, several bills pending in Congress include disclosure requirements. See, e.g., Personal Data Privacy and Protection Act of 2005 (SB 1332).

Voluntary disclosure: Even if disclosure is not required by law, the company and its attorneys should consider whether voluntary disclosure is in the company's best interest, as well as in the interests of the affected employees. Several factors affect this analysis. If the breach may result in identity theft, a company may be able to mitigate any damages to its employees (and, by extension, to itself) by disclosing the breach to the affected individuals so that they can take steps to minimize the impact of the breach. The company also should consider whether it should take any steps to minimize potential loss, such as purchasing identity-theft protections or insurance for affected employees.

A company's failure to disclose a breach also may increase the company's exposure in other ways.

Indeed, in response to growing concern over electronic security breaches and identity theft, a number of employers are taking proactive measures to minimize any potential harm to their employees even before any breach occurs. For example, according to published reports, companies like Rite Aid, Reed Elsevier PLC and Qwest Communications International recently have purchased identity-theft resolution insurance, which they offer as a benefit to aid employees in quickly clearing their name and restoring their credit should they become victims of identity theft. See "Employers Offer Help Fighting ID Theft," The Wall Street Journal, May 24, 2006. While all companies can benefit from taking such early steps to minimize their potential exposure, any company that already has experienced an information security breach should carefully consider obtaining identity-theft insurance and other protections for its employees.

A company's failure to disclose a breach also may increase the company's exposure in other ways. If the matter were ever litigated, the company's refusal to voluntarily disclose the breach and warn affected employees likely would affect the trier-of-fact's analysis and verdict, and may even expose the company to punitive damages. Indeed, ChoicePoint's reported decision in February 2005 to disclose a significant data breach of customer information, reportedly resulting in hundreds of cases of identity theft, may have helped create a public expectation that all companies would do likewise whether the breach pertained to customer or employee information.

Of course, voluntary disclosure may have costs of its own. According to CNET News.com, ChoicePoint spent about $11.4 million in the first and second quarters of 2005 to cover costs related to the breach. Additionally, ChoicePoint reportedly paid $15 million earlier this year to settle claims brought against it by the Federal Trade Commission in connection with the 2005 breach. See www.ftc.gov/opa/2006/01/choicepoint.htm.

While storing employees' personal information electronically has streamlined many aspects of the modern business world, it also has created new risks and opportunities for identity thieves. As a result, it is no longer enough to have a comprehensive information-security system; employers now must be prepared to deal effectively and promptly with an information-security breach so they can comply with applicable laws and minimize the potential damage to them and their employees.

John Nadolenco is a partner at Mayer Brown Rowe & Maw in Los Angeles. Francisco Ochoa is an associate with the firm. E-mail jnadolenco@mayerbrownrowe.com, fochoa@mayerbrownrowe.com.