

The Metropolitan Corporate Counsel®

www.metrocorpcounsel.com

Volume 11, No. 8

© 2003 The Metropolitan Corporate Counsel, Inc.

August 2003

Disclosure Of Security Breaches Required By New California Privacy Legislation

**Cheryl A. Falvey
Elaine M. Laflamme
and Michael A. Oakes**

**AKIN GUMP STRAUSS HAUER
& FELD LLP**

Companies that maintain electronic personal information regarding California residents have a new privacy compliance obligation effective July 1, 2003. In response to hackers breaking into the state of California's payroll database containing personal and financial information on the state's 265,000 employees, voters in that state passed a bill requiring companies doing business in California, as well as state agencies, to disclose publicly any computer security breaches that involve the personal information of a California resident. The new legislation protects consumers against identity theft and credit card fraud by requiring companies and state agencies to act quickly to disclose any breach in the security of a data system when the information that has been hacked is personal and not encrypted. However, many predict that the disclosure obligation will result in massive class action suits for companies victimized by security breaches.

The Security Threat And Disclosure Dispute

Concerns over hacking range from

Cheryl A. Falvey is a Partner in the litigation and technology practice groups, Elaine M. Laflamme is a Partner in the intellectual property and technology practice groups and Michael A. Oakes is an Associate in the litigation practice group of Akin Gump.



Cheryl A. Falvey



Elaine M. Laflamme



Michael A. Oakes

protecting bank account information to ensuring the security of credit card purchases, from protecting executive travel itineraries to maintaining the confidentiality of prescription drug histories as well as a host of other personal information held in public and private databases. Moreover, consumer fears of identity theft and security breaches cost Web-based businesses substantial lost business opportunities. The Gartner Group estimates that 86 percent of American adults admit that security and privacy concerns stop them from doing business on the Internet,¹ and that concerns over privacy, security and fraud have prevented consumers from utilizing the Internet for online bill payment.²

Experts suggest that network intrusions have quadrupled in the past few years.³ Despite the criminal sanctions and other serious consequences that result from vandalizing Web sites, hacking persists with a cult-like following. In February, eight million credit card numbers were accessed by hackers attacking DPI, a payment processing company that handles transactions for VISA, MasterCard, Discover and American Express.

Recently, hackers worked for hours in a loosely coordinated effort in a "contest" to vandalize Internet sites and tally points in competition as a result.⁴ Aggressive law enforcement efforts directed toward hackers have made little impact in the number of network intrusions.

To date, companies have wrestled with the decision about whether to disclose a security breach and its potential ramifications to consumers whose private data may have been compromised by the breach. Advocates of disclosure argue that immediate notification of any security breach minimizes the risk of harm from the attack. Disclosure further aids in the investigation of an attack with the goal of thwarting future attacks by the same perpetrator. Others express concern that disclosure raises a red flag for potential hackers by identifying system vulnerabilities before they can be resolved. Disclosure also may result in class action litigation,⁵ which exposes companies to the expense of civil litigation despite the fact that there may not have been actual harm to consumers resulting from the security breach.

Please e-mail the authors at cfalvey@akingump.com, elaflamme@akingump.com and moakes@akingump.com with questions about this article.

California Favors Disclosure Of Security Breaches

In California, the voters favored disclosure presumably, at least in part, because identity theft is one of the fastest-growing crimes in California. The new California law, section 1798.2 of the Civil Code (the Act), also known as SB 1386, requires public disclosure of security breaches regardless of where the company is located or where the security breach occurs. Starting in July, this first-of-its-kind law requires disclosure of any security breach to each affected resident in California whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.

The Act defines "personal information" as an individual's first name or initial and last name in combination with one or more of the following "data elements," where either the name or the data element(s) is not encrypted:

- social security number
- driver's license number or California ID number
- account number, debit or credit number in combination with any required security code, access code or password that would permit access to a person's financial account.

The Act excludes encrypted data from its definition of personal information, yet does not include a definition of what encryption means or what type of encryption is sufficient in the event of a security breach. Certain methods of encryption offer limited protection against a security breach. The Federal Trade Commission has published a fact sheet that provides insights on how to ensure that information is properly encrypted, which can be found on the FTC Web site at <http://www.ftc.gov>.

Any unauthorized acquisition of computerized data constitutes a security breach under the Act so long as it compromises "the security confidentiality" or integrity of the information. This includes more than attacks on networks by hackers. For example, disclosure may be required in the event that computer hard drives or disks are stolen which contain personal information. Several recent highly publicized thefts of computer hard drives resulted in the disclosure of thousands of names and social security numbers. Under the new law, if any of those individuals whose personal information was stolen had been California residents,

disclosure would have been required.

Recognizing that victims of identity theft must act quickly to minimize damage, the law requires that notice be made "in the most expedient time possible" and "without unreasonable delay." The need for speed is tempered by the requirements of law enforcement. The California law requires that any disclosure of the security breach be "consistent with the legitimate needs of law enforcement" and with the time necessary to restore "reasonable integrity" to the affected data system. This encourages companies to report security breaches to law enforcement while they decide whether and when to notify consumers.

Failure to provide prompt notice may expose a company to a suit for damages. The Act provides that consumers who have been injured by a violation of the law may bring a civil action for damages. Claims under the Act also may be accompanied by claims of unfair business practices under state law or misrepresentation claims premised on violations of company privacy policies ensuring protection of consumer data. Class action litigation will inevitably result from security breaches where unencrypted personal information is accessed.

An Emerging Standard Of Care For Data Protection

The Act creates an interesting conundrum for multistate enterprises. In the unfortunate event of a security breach, should a company discretely notify only its California customers? Other questions under the law are sure to arise as companies grapple with law enforcement demands and the meaning of "reasonable belief" that personal information has been acquired without authorization. Any delay in disclosure may be used against companies in later litigation for damages, yet disclosure may not always be warranted immediately.

While the disclosure obligations in the Act impose new duties, companies that post privacy policies or are subject to privacy laws have been required to employ security measures to prevent, detect and monitor intrusions for some time now. The FTC has aggressively targeted companies who fail to properly encrypt personal information when they have promised consumers that they have done so.⁶ A close reading of FTC complaints reveals a standard of care requiring storage of consumer information in an "unreadable, encrypted format at all

times" and the implementation of procedures that ensure compliance not only with company privacy policies but also "reasonably foreseeable vulnerabilities in their Web site and computer networks."⁷ FTC settlements in recent cases where posted privacy policies were breached further reveal the need to update written security policies, periodically monitor for risks and train employees on how to identify and manage security breaches.⁸ Likewise, settlements in privacy and security cases pursued by state attorneys general suggest the need for immediate action to suspend activities impacted by a security breach, investigate the cause of such an incident and take whatever remedial action may be warranted.

Privacy compliance has moved beyond the need for awareness, audit and oversight of the handling of confidential information. The California statute's disclosure requirement for the first time subjects companies which are attacked to additional public scrutiny regarding not only the details of the breach, but quite possibly their efforts to avoid such an intrusion from the start. The rewards may include greater security awareness, increased public awareness of the deceptive tactics used by hackers and greater law enforcement to prevent future attacks. Despite these possible advantages, the price of disclosure may be significant class action litigation burdens for companies — which, like consumers, may simply be victims of criminal activities.

¹ Information Security, *September 2001, Trusecure Corporation*.

² Economic Perspectives, *December 2001, Federal Reserve Bank of Chicago*.

³ Robert A. Clyde, *Guarding Against Network Security Attacks, Journal of Counterterrorism and Homeland Security International*, Winter 2003.

⁴ Ted Bridis, *Hackers Limit Disruption to Small Internet Sites, Washington Post (Monday, July 7, 2003)*.

⁵ See, e.g., *Lawsuit Accuses Tri-West Health Care of Negligence, Arizona Republic, January 30, 2003 (class action filed in Arizona after computer files and data files containing personal information were stolen)*.

⁶ See *Press Release, Federal Trade Commission, Guess Settles FTC Security Charges; Third FTC Case Targets False Claims About Information Security (June 18, 2003)*, available at <http://www.ftc.gov/opa/2003/06/guess.htm>; see also, *Press Release, Federal Trade Commission, FTC Targets Security to Combat Identity Theft (Apr. 3, 2003)*, available at <http://www.ftc.gov/opa/2003/04/idthestimony.htm>; *Press Release, Federal Trade Commission, Microsoft Settles FTC Charges Alleging False Security and Privacy Promises (Aug. 8, 2002)*, available at <http://www.ftc.gov/opa/2002/08/microsoft.htm>; *Press Release, Federal Trade Commission, Eli Lilly Settles FTC Charges Concerning Security Breach (Jan. 18, 2002)*, available at <http://www.ftc.gov/opa/2002/01/ellililly.htm>.

⁷ *Id.* Indeed, failure to deploy anti-worm patches to protect networks against attack has been found to be unreasonable in certain circumstances. See *BNA, Computer Technology Law Report, Volume 4, No. 12 (June 20, 2003)*.

⁸ *Id.*