SIDLEY AUSTIN BROWN & WOOD LLP
AND AFFILIATED PARTNERSHIPS

OCTOBER 2003

PRIVACY AND DATA PROTECTION ALERT

Privacy, Data Protection and Information Security Practice Group

Sidley Austin Brown & Wood LLP offers clients an inter-disciplinary, international group of lawyers focusing on the complex issues of privacy, data protection, information security, consumer protection and cybercrimes. Members of the Privacy Group are based primarily in Washington, New York, London, Chicago, Brussels, and Los Angeles. The Group includes intellectual property lawyers, litigators, financial institution practitioners, health care lawyers, EU specialists, IT licensing and marketing counsel, and regulatory and white collar lawyers.

If you would like more information on the Privacy, Data Protection and Information Security Practice Group, please contact:

Alan Charles Raul
(202) 736-8477
araul@sidley.com

Peter Toren
(212) 839-7357
ptoren@sidley.com

Ron Ben-Yehuda
(213) 896-6668
rbenyehuda@sidley.com

To receive future copies of the Privacy and Data Protection Alert via email, please send your name, company or firm name and email address to lhersh@sidley.com

Information Security: California's Office of Privacy Protection Issues

Recommendations on Notification of Security Breaches Involving Personal Information

The recent release of new guidelines on responding to computer security breaches offer important guidance for all companies with valuable electronic information. On October 10, 2003, the Office of Privacy Protection within the State of California's Department of Consumer Affairs issued its "Recommended Practices on Notification of Security Breach Involving Personal Information." *See* California Dept. of Consumer Affairs, Office of Privacy Protection, "Recommended Practices on Notification of Security Breach Involving Personal Information," *available* here. The Office of Privacy Protection is tasked with recommending policies and practices that protect California consumers' privacy.

A new California law on notice of security breaches, commonly referred to as SB 1386, took effect on July 1, 2003. The law requires that businesses expeditiously disclose to affected California residents security breaches concerning certain types of computerized, unencrypted personal information, in order to provide early warning where that information has been obtained by an unauthorized party. *See* Cal. Civ. Code § 1798.29. The newly issued Recommended Practices are non-binding guidelines that go beyond the scope of SB 1386, and are intended to aid businesses and other organizations in supplementing and enhancing their information security programs. *See* Recommended Practices, at 8. The Recommended Practices aim to reduce the risk of identity theft through misuse of personal information entrusted to organizations, regardless of whether that information is in electronic or paper form. *See id.* at 5.

Companies both within and outside of California should be aware of these Recommended Practices, as they are directed at any organization in possession of California residents' personal information, without regard to where the organization is located. Moreover, the guidelines set forth in California's Recommended Practices could well become a *de facto* standard of care nationwide.

Regardless of jurisdictional coverage, these guidelines may be helpful in developing and implementing successful cyber-security protocols for any company. In developing such internal procedures, companies may also find it useful to refer to prior FTC settlement agreements specifying privacy and information security elements that it holds out as "best practices." *See*, *e.g.*, "Guess Settles FTC Security Charges; Third FTC Case Targets False Claims about Information Security," (June 18, 2003 corrected) Click here. Likewise, various specific sectors of the economy are governed by particular norms. *See*, *e.g.*, FTC Financial Information Safeguards Rule: "*Standards for Insuring the Security, Confidentiality, Integrity, and Protection of Customer Records and Information*," 16 C.F.R. Part 314 (2002). In order to assist clients in navigating this maze, we have assembled several articles regarding these requirements at www.sidley.com/cyberlaw including, for example, "Privacy Due Diligence: Eli Lilly FTC Consent Order Is A Good Road Map for Corporate Data Protection,"[1] and an examination of "Liability for Computer Glitches and Online Security Lapses."[2]

Definitions of Key Terms

The Recommended Practices provide definitions for certain key terms.

"Notice-triggering information" specifies the threshold for protected information and is defined as an *unencrypted*, computerized first name or initial and a last name, plus any one of various identification numbers, such as a social security number, driver's license number, credit card or other financial account number, in conjunction with a code that would allow access to that financial account.

"Higher-risk personal information" is defined broadly to include notice-triggering information as well as health, financial or other personal information that would violate an individual's privacy if disclosed.

A "data owner" is an individual or organization with primary responsibility for controlling a record system's purpose or function.

A "data custodian" is an individual or organization to whom the data owner has delegated responsibility for maintenance and technological management of a record system. *See id.* at 8.

The Recommended Practices are divided into three major parts: (1) Protection and Prevention; (2) Preparation for Notification, and; (3) Notification. The recommendations contained in each part are summarized below.

Part One - Protection and Prevention

Identifying and classifying personal information. As a means of protection and prevention, organizations are advised to collect the least amount of personal information necessary to fulfill the organization's purpose, and to retain that information for the minimum possible amount of time. Organizations should also inventory all records storage systems to identify those that contain personal information. All personal information should then be classified according to its sensitivity, and any notice-triggering data should be identified.

Using safeguards. Organizations should use both physical and technological security safeguards where feasible to protect personal information. Organizations should restrict employee access to

[1] http://www.sidley.com/cyberlaw/features/lilly.asp

[2] http://www.sidley.com/cyberlaw/features/liability.asp. This piece was also published in the BNA Electronic Commerce Law Report, Volume 6 Number 31, Wednesday, August 8, 2001, Page 849.

personal information, allowing access to only that information necessary for employees to fulfill their jobs. Any employee access to higher-risk information should be monitored, and access privileges of former employees should be terminated.

Employee training. Employers should provide ongoing training and communications to ensure employees' awareness of privacy policies and procedures. They should also monitor employee compliance, and impose penalties for violations.

Third-party information handlers. Organizations should enter into contracts obligating third parties, such as service providers and business partners, to comply with privacy and security policies. Third-party compliance should also be monitored.

Intrusion detection measures. Intrusion detection technology and complementary procedures should be used to ensure that security breaches are swiftly detected.

Data encryption. Data encryption and access control protections should be employed for higher-risk personal information.

Records disposal. Organizations should dispose of personal information in a secure manner, such as by shredding records and overwriting data stored on hard drives.

Security plan review. Security plans should be reviewed at least annually or any time there is a material change in business practices that may affect the security of personal information. *See id.* at 8-9.

Part Two - Preparation for Notification

Each organization's information security program should have an incident response plan to be implemented in the event of a security breach. This will help to ensure that affected individuals receive timely notice of breaches.

Internal response. Organizations should have written procedures for internal notification of security breaches. One individual should be charged with coordinating these procedures, and employees should receive regular training on their roles in the response plan.

Containment measures. Organizations should devise measures for controlling, containing and remedying the impact of any security breach.

Notification of data owner. The data owner must be immediately notified of any breach.

Third-party compliance. Third parties such as service providers and business partners must be contractually required to comply with incident response procedures.

Notification of law enforcement authorities. Where security incidents may involve illegal activity, law enforcement authorities should be notified.

Procedures for notification of affected individuals. Organizations should have written procedures for notifying those individuals whose notice-triggering personal information has been or is reasonably believed to have been accessed by an unauthorized person.

Documentation. Organizations should maintain documentation of their actions taken in response to a security incident.

Incident response plan review. Incident response plans should be reviewed at least annually or any time there is a material change in business practices that may affect the security of personal information. *See id.* at 10.

Part Three - Notification

Expeditious notification. Affected individuals should be notified as soon as possible after the organization

becomes aware that unauthorized access to notice-triggering information has occurred. The Recommended Practices advise notification within ten business days. If law enforcement instructs that notification of affected individuals within ten days would impede an investigation, organizations should ask to be informed as soon as affected individuals may be notified.

Individuals to notify. Notification must be given to California residents whose notice-triggering information was acquired by an unauthorized person. The Recommended Practices suggest that organizations also provide notice of breaches involving information that is higher-risk but not notice-triggering, in order to allow affected individuals to protect themselves. If specific individuals cannot be identified, notification should be provided to all groups likely to have been affected.

Avoiding over-inclusiveness. Organizations should take care to send notification only to those individuals who were actually affected by the security breach.

Coordination with credit reporting agencies. Organizations should coordinate with credit reporting agencies, who can provide helpful information to affected individuals.

Form, contents and manner of notice. Notices to affected individuals should include a description of the incident, the nature of the personal information involved, information on the steps the organization has taken to protect against further unauthorized acquisition, details concerning assistance available to affected individuals, such as a toll-free internal number, information on protecting oneself from identity theft, and contact information for the three credit reporting agencies, as well as the California Office of Privacy Protection and the FTC.

Notices should be written in clear, simple language, and should be sent as a stand-alone document to avoid confusion. Individual notice is preferred where feasible. Notification can be sent by first class mail, by e-mail where prior consent to e-mail notification has been given, or, if the number of affected individuals exceeds 500,000 or the cost of providing individual notice exceeds $250,000, notice may be given by e-mail, in addition to being posted on the organization's website and provided to major statewide media. *See id.* at 11-13.

Finally, the commentary accompanying the Recommended Practices cautions that these guidelines are not exhaustive; organizations should continually review their practices to ensure compliance with applicable privacy laws and standards, particularly as technology evolves. *See id.* at 8.

The information law practice of Sidley Austin Brown & Wood LLP is experienced in addressing all aspects of privacy, data protection and information security. For further information about developments in this area, please contact:

Alan Charles Raul (202)736-8477 araul@sidley.com
Peter Toren (212)839-7357 ptoren@sidley.com
Ron Ben-Yehuda (213)896-6668 rbenyehuda@sidley.com