PROSKAUER ROSE®

Client Alert

A report for clients and friends of the firm

January 2003

New California Law Requires All Companies That Do Business In State To Provide Notice Of Computer Security Breaches

Nationwide Applicability and Vague Language Presents Challenges for Business

A new consumer notification law recently was enacted and signed into law in California that may present legal and logistical challenges for companies all across the country that use computers to store customer information.[1]

On July 3, 2003, companies that do business in California and that maintain computerized customer records — *no matter where they are located* — must notify customers of computer security breaches. Given the increasing and unpredictable frequency with which computer intrusions now occur, this law may require major new ways of doing and monitoring business use of computers. And since the term "breach" is not defined in the law, employee access to restricted information may trigger the notification requirement. The impact on interstate commerce of this new consumer protection law may be significant, and that might prompt a Constitutional challenge to the statute.

The California law specifies that notice must be provided if there is a computer security breach and if the computerized records contain names, together with unencrypted data including Social Security numbers, driver's license numbers, state identification card numbers, account numbers, or credit card or debit account numbers with passwords. The law further requires that, in the event of a security breach, the disclosure of such breach must take place in the "most expedient time possible and without unreasonable delay." However, the notice may be delayed if law enforcement officials deem it necessary.

The required notice may be written or electronic (e-mail), and if the cost of such a notice would be more than $250,000, or if more than 500,000 people must be notified, a company may use media outlets as a substitute for a formal notice.

Violations of the new law may result in an injunction and/or civil damages. A private right of action is given to injured customers. An injunction against doing business with California customers could have dire consequences for untold numbers of businesses.

The law presents many unanswered questions:

- What evidence of a breach is necessary to trigger notification?
- What information must be contained in the notice?
- How quickly must a company act to notify customers?
- Does law enforcement involvement mean no notice is required?
- And, significantly, is the law Constitutional? There is a serious issue under the Commerce Clause over the authority of California over data maintained on a server in New York, for example.

---

[1] Section 1798.82 of the California Civil Code reads:

1798.82. (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(Continued on next page)

The issue of what constitutes a breach may be very problematic. The CERT® Coordination Center at Carnegie Mellon reported more than 82,000 computer intrusions in 2002. How may of them would have required the California notice? And "breach" can go beyond an external intrusion. For instance, what if the access by a current employee to computerized customer records is more than authorized by the company (intentionally or by mistake), does that have to be reported? There are many imponderables.

But unless a Court invalidates the law, businesses should consider their current security procedures and whether they are able to detect security breaches. (Even if a suit is filed, that is not likely to occur before the July 1 implementation date and invalidation is by no means a foregone conclusion.) Companies also need to evaluate their ability to notify law enforcement and customers of potential breaches. Also, an issue to consider is whether California customers may be segregated for notification and, even if they can be separated from other customers, whether customers in other states may demand notification even if not legally required.

The many questions raised by this statute likely will result in close consultation with counsel as companies prepare to comply.

NEW YORK LOS ANGELES
WASHINGTON BOCA RATON
NEWARK PARIS

Client Alert

This client alert was prepared by Christopher Wolf, Chair of Proskauer's Computer Security Practice Group. Chris is a member of the New York and Washington, DC Electronic Crimes Task Force, organized under the auspices of the United States Secret Service, and is a founding member of the Cyber-Crisis Network, which brings together computer, investigatory, communications and legal experts to assist companies with computer security problems. Proskauer's Computer Security Practice Groups counsels clients on their obligations in the event of a computer security breach and the steps that may be taken to avoid or limit legal liability from potential computer intrusions.

Christopher Wolf
202.416.6818 — cwolf@proskauer.com

Proskauer is an international law firm with more than 590 attorneys who handle a full spectrum of legal issues worldwide.

(Continued from previous page)

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the person or business has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

SEC. 5. This act shall become operative on July 1, 2003.