New York Law Journal

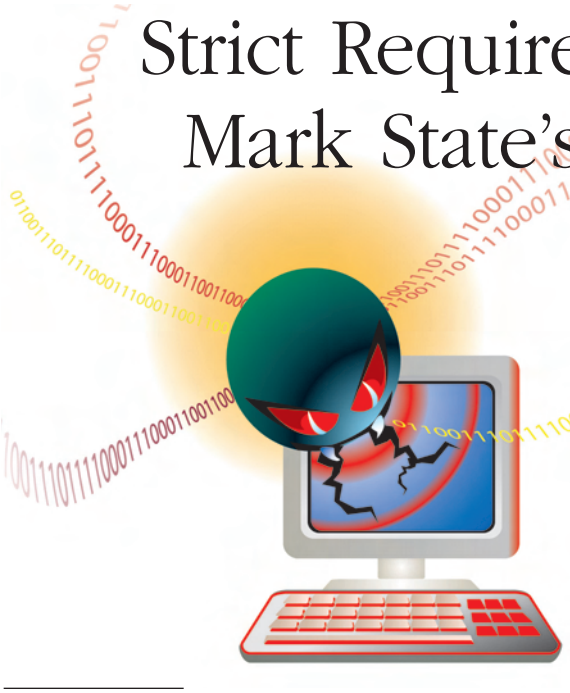
SPECIAL SECTION

Law & Technology

MONDAY, JANUARY 30, 2006

Strict Requirements, Harsh Penalties Mark State's New Data Breach Act

Law Requires Companies Doing Business In New York or With New York Residents To Timely Notify After a Breach Has Occurred



BY YAIR Y. GALIL AND MAURICIO F. PAEZ

Following the trend in other states, New York last summer enacted the Information Security Breach and Notification Act, an important data security and notice statute.

The act, which took effect Dec. 8, imposes certain reporting burdens on state and local agencies and companies doing business with New York residents.

The act obligates companies that own or license computerized data that include "private information" to notify New York residents of any breach to the database storing their data, whenever such residents' private information is acquired, or reasonably believed to have been acquired, by a person without valid authorization.

The statute applies regardless of whether the computerized data are maintained in New York. As long as a company conducts business in New York and owns or licenses computerized data that include private information about a New York resident, it has a legal obligation to notify that resident of a security breach to the resident's private information.

Additionally, the act imposes obligations on a company that maintains personal data owned by another, for example, a data-processing service provider that maintains data for another company. Such a maintainer of data must notify the data's owner (typically, the company that contracted for the maintainer's services) of a breach, regardless of where the data is maintained.

Thus, the statute has broad implications for companies across the United States and abroad if they maintain, own, or license computer data containing personal information about New York residents.

In addition to the notification obligation, companies must report a security breach to the state attorney general, the Consumer Protection Board, and the State Office of Cyber Security and Critical Infrastructure Coordination regarding the timing, content and distribution of the notices and approximate number of affected persons. If the number of affected persons exceeds 5,000 New Yorkers, the companies must also provide the same report to United States consumer reporting agencies.

"Private information," as used in the statute, means any personally identifying data (such as a name, number, personal mark or other identifier) in conjunction with one of the following data elements: a U.S. Social Security number; a driver's license (or non-driver identification card) number; or an account number or credit/debit card number in combination with the access code to such account or card.

To trigger the statute's notice and reporting obligations, either the identifier or the data element must have been acquired in unencrypted form or in encrypted form where the encryption key has also been compromised.

Notice Obligations

A company must notify any New York resident whose private information was, or was reasonably believed to have been, acquired by a person without valid authorization. The notice must include specific information, including contact information for the company making the notification and a description of the categories of information breached.

The law also provides that notice must be expedient and without unreasonable delay. However, a company may delay notice (i) if a law enforcement agency determines that the notification will impede a criminal investigation, or (ii) if notification would compromise the company's ability to determine the scope of the breach and implement remedial measures. Where the data is maintained by third-party providers, the notification of a breach by the third-party provider to the data's owner must occur "immediately" after its discovery.

The required notification to New York residents must be in the form of personal notice to each affected New York resident.

If such personal notices would cost more than $250,000, or if the number of persons to be notified is greater than 500,000, the company is permitted to use an alternative method of notification specified in the statute, which involves the use of public media.

The statute provides a strong incentive for companies to adopt comprehensive security procedures to limit the vulnerability of their computer systems, to establish compartmentalized encryption routines, and to create a plan of action in the event of a security breach.

Companies that fail to implement encryption technologies face the cost of notification and significant reputation risk attendant to the public disclosure of a security breach.

In addition, the state attorney general is authorized to sue a business violating the statute to recover damages for actual costs or losses, including consequential financial losses, incurred by affected New York residents. The statute also authorizes the imposition of civil penalties, which could reach as much as $150,000 in the aggregate, for knowing

Yair Y. Galil *and* **Mauricio F. Paez** *are Jones Day associates.*

or reckless violation of the notification or reporting requirements.

Stricter Statute

The New York Security and Notification Act is emblematic of a trend, in state security breach notification laws, toward stricter requirements and harsher penalties.

The California Security Breach Information Act, which became effective in 2003, served as the template for much of the recent legislative activity at the state level, including the New York act. However, the New York act is notably stricter along several dimensions. For instance, it provides for legal action by the state attorney general, with statutory damages, whereas the California act does neither; it sets forth specific requirements for the content of the notification to customers, where the California act is silent on this issue, requiring merely that notice be delivered; it requires notification to the state attorney general, the Consumer Protection Board, and New York's cyber-security authorities, where the California act requires no notice beyond that to the affected California residents; and, unlike the California act, it makes no exception for companies that maintain and implement their own notification procedures pursuant to an information security policy.

Other states have also modified the California template in ways that tighten its requirements. For example, Connecticut expanded the definition of a security breach to mean mere unauthorized access to, as opposed to acquisition of, computerized data. Florida's version mandated a 45-day time period for a notification. Delaware provided for private action with treble damages plus attorney's fees. A number of states have expanded the definition of personal data, e.g. to include medical information.

Companies affected by New York's law can and should take preventative measures to minimize its impact on their business. These measures fall into three main categories: steps to prevent security breaches, steps to ensure compliance with the law, and steps to mitigate the other repercussions of a breach.

Reducing Risk of a Breach

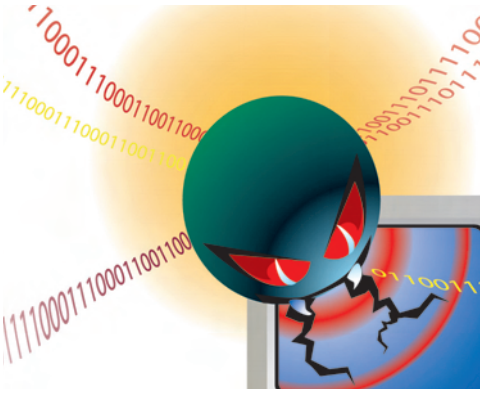
Data security risks may come from a variety of sources, such as hackers, employees and third-party vendors. Different classes of potential intruders will attempt to access confidential data in different ways and therefore each class of potential intruder must be addressed separately.

Intrusion detection systems, firewalls, and encryption may deter hackers but offer little protection against employees with access to confidential consumer data. Furthermore, personal data transferred to or stored by third-party vendors also pose a compliance risk.

Breach notification laws provide no exception for data that is compromised while in the possession of a third party. Protecting sensitive information against these various threats requires assessing and addressing security vulnerabilities in the way in which data is entered, transferred, stored, and accessed.

Some protective measures include:

- Developing and implementing mechanisms such as firewalls, intrusion detection systems, and access controls;
- Deploying tracking technologies to provide information about network flow and data flow patterns to prevent and detect unauthorized conduct on networks;
- Encrypting personal information, and maintaining the encryptions keys separately from the encrypted data;
- Reviewing and, if necessary, bolstering access control, identification and authentication procedures and systems;



Companies need to review their data collection systems and procedures from a legal perspective to ensure they are able to comply effectively and efficiently with the New York act, should a breach occur despite these security measures.

- Creating a data classification system for employees and using access controls to limit employee access to computer data to a "need to know" basis;
- Educating employees on human risk factors involved in accessing and transporting data, such as failing to log off a database or storing data on devices and on media that are not secure; and
- Reviewing and possibly renegotiating third-party contracts involving the transfer of personal data to ensure effective data security and compliance with notification obligations.

Ensuring Compliance

In addition to securing their data as outlined above, companies need to review their data collection systems and procedures from a legal perspective to ensure that they are able to comply effectively and efficiently with the New York act, should a breach occur despite these security measures.

Some typical compliance-oriented audit and other measures would include:

- Inventorying existing computer systems and electronic files to determine what personal data are collected and maintained, and how they are stored;
- Identifying how personal information is gathered, including what notices are given to, and consents obtained from, the individuals whose personal information is collected;
- Reviewing the contact name and address information available for persons who may potentially need to be notified of a breach, and determining the best means of notification;
- Developing internal assessment procedures and contingency plans for investigating the scope and source of a security breach, possibly with the assistance of outside investigators;
- Establishing an internal reporting mechanism to ensure that relevant decision-makers within the company are promptly notified of a security breach;
- Reviewing public and nonpublic representations concerning security, privacy and notification procedures; and
- Reviewing and possibly renegotiating third-party contracts involving the transfer of personal data to ensure compliance with notification obligations.

Mitigating Other Repercussions

Compliance with the notification requirements triggered by a security breach does not represent the end of the incident's repercussions for a company; in some ways, it is just the beginning.

As the breach is publicized, a company may face a negative impact on its relations with customers, suppliers and capital providers. In some cases, the company may also need to confront class action shareholder litigation.

There are, however, ways to mitigate these types of damage, including:

- Developing a contingency public relations plan to address the reputational damage from a public notification of a security breach, including arrangements with credit reporting agencies;
- Maintaining a relationship with relevant public authorities and private data security service providers, whose credibility may be called upon to affirm the company's public statements regarding the limits of the breach and the efficacy of the company's countermeasures; and
- Preparing pro forma financial projections for the consequences of a security breach under different likely scenarios, so as to be able to provide swift answers to the capital markets.

Conclusion

The New York Security and Notification Act is part of a flurry of state-level legislative initiatives, spurred in part by several high-profile security breaches early in 2005.

Similar laws have already been passed in several other states, including Arkansas, California, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Maine, Minnesota, Montana, Nevada, New Jersey, North Carolina, North Dakota, Rhode Island, Tennessee, Texas, and Washington. And other states are considering equivalent bills.

As these initiatives bear legislative fruit, companies will find it ever more difficult to avoid dealing with security breach notification obligations arising out of state law.