AUGUST 2005

TECHNOLOGY

NEW YORK ENACTS DATA SECURITY AND NOTIFICATION LAW

Following the trend in other states, on August 10, 2005, New York enacted the Information Security Breach and Notification Act (the "NY Security and Notification Act"), an important data security and notice statute. The NY Security and Notification Act will take effect on December 8, 2005, and will impose certain reporting burdens on state and local agencies and companies doing business with New York residents. Generally, the NY Security and Notification Act requires businesses and state agencies, upon discovery or notification of a security breach in their computer systems, to notify any New York resident whose personal information has been acquired, or is reasonably believed to have been acquired, without authorization. This *Technology Commentary* provides a brief overview of the NY Security and Notification Act.

SECURITY BREACH STATUTE

The NY Security and Notification 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' personal 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 the resident of a security breach to the resident's private information. Additionally, if a

company maintains computerized data owned by another (*e.g.*, data-processing service providers), that company must notify the data's owner 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 these companies 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 York residents, the companies must also provide the same report to consumer reporting agencies.

"Private information" 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 Social Security number
- a driver's license (or non-driver identification card) number
- an account number or credit/debit card number in combination with the access code to that 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 UPON A BREACH OF SECURITY

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 if a law enforcement agency determines that the notification will impede a criminal investigation, or if notification would compromise the company's ability to determine the scope of the breach and take 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, based on public media disclosure.

CONSEQUENCES OF NONCOMPLIANCE

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 New York 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 New York residents entitled to notification. The statute also authorizes the imposition of civil penalties, which could reach as much as $150,000 in the aggregate, for knowing or reckless violation of the notification or reporting requirements.

STRATEGIES FOR SECURITY AND COMPLIANCE

Affected companies should review their data security policies, privacy practices, and information technology and security systems for compliance. This should include:

- Inventorying existing computer systems and electronic files to determine what personal information companies collect and maintain.

- Identifying how personal information is collected and stored.
- Reviewing the contact and addressing information available for persons who may potentially need to be notified of a breach, and determining the best means of notification.
- Reviewing public and nonpublic representations concerning security, privacy, and notification procedures.
- Reviewing existing procedures for maintaining personal information in an encrypted format, and safekeeping relevant encryption keys.

Companies who handle private information about New York residents will need to consider implementing a number of preventive measures to mitigate liability risks. Such measures may include:

- Establishing compartmentalized procedures for encrypted data to limit the risk of encryption keys being acquired.
- Limiting employee access to computer data to a "need to know" basis using passwords or other techniques.
- Training employees on the importance of information protection and immediate reporting of breaches.
- Developing internal assessment procedures and contingency plans for investigating the scope and source of a security breach, possibly with the assistance of outside investigators.
- Implementing industry standard encryption solutions.
- Developing a contingency public relations plan to minimize the reputational damage from a public notification of a security breach, including arrangements with credit reporting agencies.
- Implementing new technologies designed to provide detail about network conduct and data-flow patterns to understand potential security gaps.
- Reviewing and revising third-party contracts involving the transfer of computerized personal information to ensure compliance with notification and reporting obligations.

CONCLUSION

The recent enactment of the NY Security and Notification Act is part of a flurry of recent state-level legislative initiatives, spurred in part by several high-profile security breaches earlier this year. Similar laws have already been passed in several other states, including Arkansas, California, Connecticut, Florida, Georgia, Illinois, Indiana, Maine, Minnesota, Montana, Nevada, North Dakota, Tennessee, Texas, and Washington. Other states are currently 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.

RELATED JONES DAY TECHNOLOGY COMMENTARIES

- What You Should Know About Security Breaches: Notification Requirements, Insider Trading Implications, and Reporting Obligations—August 2005
- California First State to Require Online Privacy Policies—January 2004
- California Raises the Bar on Data Security and Privacy—September 2003
- Privacy Issues in Cross-Border Transactions—June 2003

LAWYER CONTACTS

For further information, please contact your principal Firm representative or the lawyers listed below. We invite you to visit our web site for additional information on privacy topics. General e-mail messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Mauricio Paez
1.212.326.7889
mpaez@jonesday.com

Yair Galil
1.212.326.3855
ygalil@jonesday.com