The Metropolitan
Corporate Counsel®

www.metrocorpcounsel.com

Volume 14, No. 2 February 2006

New Jersey Enacts Identity Theft Prevention Act

David Leit
and Matthew Savare

LOWENSTEIN SANDLER PC

Overview

On September 22, 2005, New Jersey's Acting Governor signed the Identity Theft Prevention Act (the "Act"), into law. The Act includes a number of safeguards intended to prevent identity theft and to mitigate damages in the event of such theft. The Act also includes a strong "security freeze" law. With this legislation, New Jersey joins the growing list of states that have enacted security freeze and security breach notification laws.[1]

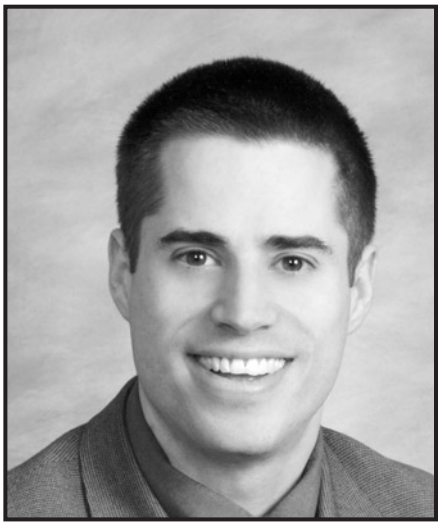
The Act (1) requires businesses to notify New Jersey consumers if their personal information has been compromised, (2) requires businesses and public entities to thoroughly destroy customer records that are no longer to be retained, (3) limits the use and display of social security numbers, and (4) allows consumers to place a security freeze on their consumer reports.

New Jersey's Identity Theft Prevention Act became effective on January 1, 2006.

Security Breach Notification

The first wave of data security and privacy legislation focused on particular industries, most notably financial institutions (regulated by the privacy and security provisions of the Gramm- Leach-Bliley Act) and health care providers (regulated by the privacy and security provisions of the Health Insurance Portability and Accountability Act). In addition, the Federal Trade Commission has been more active in enforcing privacy and security promises made by companies in other industries. Thus, companies in many industries have been taking steps to upgrade their electronic and physical safeguards to protect the personal information of their customers. In addition, we are now seeing a "second wave" of data security and privacy legislation that extends beyond particular industries and instead imposes security and privacy standards that are generally applicable across industries. New Jersey's Identity Theft Prevention Act is an example of this type of legislation.

David Leit



Matthew Savare

One of the key features of the Act, undoubtedly passed in response to numerous well-publicized data breaches that have occurred over the last several years, is a broad provision requiring businesses to notify consumers of breaches of security. The Act provides, in relevant part:

> Any business that *conducts business in New Jersey*, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach *to any customer who is a resident of New Jersey* whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person.

There are several significant features of this law. First, the law applies to "any business that conducts business in New Jersey." In other words, businesses that do not operate or have a physical presence in New Jersey may nevertheless be subject to the law if they sell products or services to New Jersey residents. Second, businesses are obligated under the Act to disclose breaches only to affected customers who are New Jersey residents.[2] Third, the Act does not require disclosure of a security breach if the business or public entity establishes that "misuse of the information is not reasonably possible." Such a determination must be in writing and retained for five years.

Fourth, in the event of a security breach, businesses must report the incident to the New Jersey Division of State Police in the Department of Law and Public Safety *before* notifying their consumers. Businesses must disclose the breach to their consumers only after the applicable law enforcement agency determines that the disclosure will not compromise any civil or criminal investigation they decide to undertake. Fifth, businesses must provide

***David Leit** is a Member of the Tech Group of Lowenstein Sadler PC. **Matthew Savare** is an Associate in the Litigation Department.*

Please email the authors at dleit@lowenstein.com or msavare@lowenstein.com with questions about this article.

the notice either (1) in writing, (2) electronically (in certain circumstances), (3) or by "substitute notice" if they demonstrate that the cost of providing notice would exceed $250,000, or that the affected number of people requiring notification exceeds 500,000, or if they do not have sufficient contact information. "Substitute notice" consists of an e-mail *and* a conspicuous posting on the entity's website *and* notification to major statewide media. Finally, if a business is required to notify more than 1,000 individuals, it must also promptly notify "all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis . . . ."

Given the Act's requirement to notify consumers of a data security breach, businesses should adopt robust electronic and physical safeguards to protect and monitor their consumers' personal information. Businesses also need to have systems and procedures in place that dictate how they will effectively and legally respond to a security breach. In addition, businesses should ensure that contracts providing outside vendors with access to their customers' data include provisions that the vendor (1) will safeguard the personal information in a manner that is at least as secure as the company, and (2) will notify the company immediately if any of its customers' data has been disclosed to an unauthorized third party.

Destruction Of Customers' Records

Most large companies have internal document retention and destruction policies that dictate how long they retain customer records and how they dispose of records that are no longer used. Although the Act does not attempt to dictate businesses' document retention policies, it does dictate how companies must dispose of records containing "personal information" they no longer will retain. Specifically, the Act requires businesses and public entities to:

> destroy, or arrange for the destruction of, a customer's records within its custody or control containing personal information, which is no longer to be retained by the business or public entity, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable, undecipherable or nonreconstructable through generally available means.

As part of their best practices, New Jersey businesses are well-advised to incorporate this statutory language into their document retention and destruction policies, and follow the guidance provided by the Act. Companies that do not currently have document retention and destruction policies should consider drafting such policies in order to help them comply with the new law.

Restrictions On Use And Display Of Social Security Numbers

The Act restricts the use and display of social security numbers. The Act mandates that no person or public or private entity shall:

(1) publicly post or display an individual's social security number, or any four consecutive digits of the SSN;

(2) print an individual's social security number on any materials that are mailed to the individual, unless required to do so by law;

(3) print an individual's social security number on any card required for the person to access products and services provided by the entity;

(4) intentionally communicate or disclose an individual's social security number to the general public;

(5) require an individual to transmit his or her social security number over the Internet, unless the social security number is encrypted or the connection is secure;

(6) require an individual to use his or her social security number to access an Internet website, unless a password or some other unique personal identification number or authentication device is also required to access the site.

The Act states that entities are still permitted to use social security numbers for internal verification and administrative purposes, as required by state or federal law, and in "applications and forms sent my mail."[3]

Security Freeze

Subject to certain narrow exceptions, the Act permits consumers to place a security freeze on their consumer reports simply by making a request to a consumer reporting agency by certified or overnight mail or through a secure e-mail. The consumer reporting agency must place a security freeze on the consumer report within five business days after receiving this written request. Consumers cannot be charged for this security freeze.

Once the security freeze is in effect, the consumer reporting agency is prohibited from "releasing the report or any information from it without the express authorization of the consumer . . . ." In addition, consumer reporting agencies cannot change any of the following official information in a consumer report while it is frozen without sending a written confirmation of the change to the consumer within 30 days of the change: name, date of birth, social security number, and address.

A security freeze remains in effect until the consumer requests that the freeze be removed. However, the Act does allow consumers to temporarily lift the freeze for a particular party or for a specific period of time. After receiving a proper request to temporarily lift the freeze, the consumer reporting agency has three (3) business days to comply. However, the Act expressly states that consumer reporting agencies must develop procedures to receive and process such requests through the phone, fax, Internet, or other electronic media, with the goal of processing the temporary lift within 15 minutes of the request. Consumer reporting agencies can charge consumers a "reasonable fee, not to exceed $5" for temporarily lifting the freeze.

Conclusion

New Jersey's Identity Theft Prevention Act imposes several obligations on businesses operating in New Jersey to take affirmative steps to help prevent identity theft. Based on the requirements of the Act, businesses operating in New Jersey should review, revise, and strengthen their policies and procedures governing the personal information of their employees, customers, and third party vendors. As noted above, companies should implement robust physical and electronic safeguards that protect personal data and create strict internal procedures that dictate how they will respond to any security breaches. Similarly, companies must insist that their outside vendors safeguard personal information in a manner that is at least as secure as the company's own methods. Companies should also create, monitor, and enforce a strict document destruction policy. Of course, the most effective way for companies to mitigate their exposure under the Act is to limit the amount of personal information they collect and restrict access to such data to a limited number of employees who have been trained on how to properly protect personal information.

---

[1] *In addition to New Jersey, the following states have passed security freeze laws: California, Colorado, Connecticut, Illinois, Louisiana, Maine, Nevada, North Carolina, Texas, Vermont, and Washington. Numerous other states are considering adopting such measures. Legislation mandating disclosure of security breaches was introduced in at least 35 states in 2005. As of January 4, 2006, at least 23 states, including New Jersey, Arkansas, California, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Maine, Minnesota, Montana, Nevada, New York, North Carolina, North Dakota, Ohio, Pennsylvania, Rhode Island, Tennessee, Texas, and Washington have enacted some type of security breach notification law. Numerous other states are considering adopting such* measures.

[2] *However, given the myriad other state laws and the attendant harm caused by withholding prompt disclosure, businesses may consider notifying customers of a data breach even if they are not New Jersey residents. In a well-publicized security breach in 2004, ChoicePoint, Inc., a major consumer data company, originally decided to disclose the existence of the breach to California residents, because, at the time, California was the only state that had a law requiring such disclosure for its own residents. Shortly after the incident became public, ChoicePoint decided to disclose the security breach to all affected consumers, regardless of whether or not they were California residents.*

[3] *The permissibility of including social security numbers in "applications and forms sent by mail" conflicts with number two outlined above, which prohibits printing an individual's social security number on "any materials that are mailed to the individual." However, because the exception allowing social security numbers to be used in certain mailings begins with "Notwithstanding this section," it does appear that social security numbers may be used in forms sent by mail, so long as they comply with the requirements of the exception, which delineate certain types of documents containing social security numbers which may be sent by mail, and which specify that social security numbers should never appear so that they are visible without first opening the envelope, box, or other shipping material. Postcards, or any other mailer that does not require an envelope, box or other shipping material should never contain social security numbers.*