



Labor & Employment Law News

April 2007

New Privacy Protection Legislation Impacts Employers

New York has enacted the Information Security Breach and Notification Act, which can be found in §208 of the State Technology Law and §899-aa of the General Business Law. The new law is intended to protect the privacy of New York consumers, including employees, by providing them with the right to know when a security breach has resulted in the exposure of personal or private information.

Who does the law cover?

The law applies to every employer in New York that owns, licenses or maintains computerized data containing private information, including state entities, individuals and businesses.

What is “private information”?

“Private information” includes any unencrypted personal information used to identify a natural person, in combination with any one of the following: (1) social security number; driver’s license number or non-driver identification card number; (2) or account number, credit or debit card number in combination with required security code, access code or password.

What does the law require?

The law requires any business which believes an unauthorized employee or third party has breached the security of a computer system to notify all New York residents whose private information “was, or is reasonably believed to have been, acquired by a person without valid authorization.”

Are there additional requirements?

Whenever the law requires notice to New York residents, it also requires that the Attorney General, Consumer Protection Board and State Office of Cyber Security and Critical Infrastructure Coordination be notified of the timing, content and distribution of notices and the approximate number of affected persons. If more than 5,000 New York residents are to be notified at one time, all consumer credit reporting agencies must be added to the list of entities which must be notified of the timing, content and distribution of notices. Upon request, the state will provide a list of all credit reporting agencies required to be notified.

When must affected parties be notified?

The law requires that notice to employees or customers is to be made in the most expedient time possible, consistent with any measures the business deems necessary to determine the scope of the breach and to restore the integrity of the computer system. Notice may be delayed if a law enforcement agency determines that it will impede a criminal investigation.

Is there information that is not protected under the law?

The law does not apply to information which is lawfully made available to the general public from federal, state or local government records.

When has a security system been “breached”?

A security system has been breached when there has been unauthorized acquisition of computerized data which “compromises the security, confidentiality, or integrity of personal information” maintained by the employer.

How should an employer determine if protected information has been acquired?

Employers may consider the following factors to determine whether protected information has been acquired or is reasonably believed to have been acquired: (1) indications that the information is in the possession and control of unauthorized persons, such as where a computer is lost or stolen; and (2) indications that the information has been downloaded or copied or circumstances such as new fraudulent accounts, indicating that the information was used by an unauthorized person.

Are there any exceptions to the law?

The good faith acquisition of personal information by an employee or agent of a business entity for use by the business is not a breach, provided the information is not later disclosed without authorization.

How must notice be provided?

The law requires notice by any one of the following methods: (1) written notice; (2) electronic notice, provided the person receiving notice has consented to electronic notice and a log of such notification is kept; (3) notice by telephone, provided a log of the notification is kept; or (4) substitute notice, where it is demonstrated that the cost of providing notice to affected persons would exceed \$250,000. Substitute notice consists of e-mail,

conspicuous posting on the business’s web site or notification to statewide media.

What should the notice say?

Regardless of the method of notification, the notice must include the contact information for the business or entity and a description of both the categories of information believed to have been acquired and the elements of information within those categories which are believed to have been acquired.

What are the penalties for failure to provide notice?

Failure to provide prompt notice may result in injunctive relief and liability for actual losses suffered by an individual not receiving notice. If a court determines that a violation was knowing or reckless, it may impose a civil penalty of up to \$150,000.

Practical Pointers:

- Make sure all employees, especially those with access to computers and private information, are aware of the duty to report any unauthorized access to the computer system.
- Implement policies and procedures for reporting and investigating suspected breaches of any computer systems as well as procedures for providing the notice required by the law.
- Make sure your computer security is reviewed and updated on a consistent basis, including issuing new passwords to employees, not allowing employees to change or select passwords and training employees on security issues.

HANCOCK & ESTABROOK, LLP
COUNSELORS AT LAW

Labor & Employment Law Practice Group Attorneys:

*Michael J. Sciotti, John T. McCann, Lindsey H. Hazelton, John F. Corcoran, Wendy A. Marsh
Edward J. Smith, III, Laurel E. Baum, Maureen E. Maney, Tyler G. Brass & Melinda B. Bowe*

“Labor & Employment Law News” is published periodically and is the sole property of Hancock & Estabrook, LLP, with all rights reserved. The articles contained herein are for informational purposes only and are not intended as legal advice.