Local Privacy Notification Policies Must Be Enacted

The New York State Information Security Breach and Notification Act took effect on December 7, 2005. This law was enacted to provide individuals with another weapon in the battle against identity theft. Prior to the enactment of this law, neither the government nor a corporation was required to notify a person whose private information might have been acquired by an unauthorized source due to a security breach in the business's or government's computer system. Computer security breaches can result in unauthorized access to a person's personal information, such as social security numbers and credit card pin numbers. In New York State, for example, more than nine thousand individuals' personal information was compromised in a security breach at ChoicePoint, a large personal information aggregating firm. This breach occurred prior to the enactment of the New York State Information Security Breach and Notification Act when ChoicePoint was not required to notify the affected victims. The only notification of the theft of social security numbers was through the national news.

As a result of the enactment of the New York State Information Security Breach and Notification Act, ChoicePoint would now have to personally notify victims of identity theft resulting from a breach in their systems. Another example of this problem occurred at DSW, a shoe outlet whose customer credit card information from the 2004-2005 holiday season was also stolen - exposing thousands of New York consumers and over 1.4 million customers nationwide.

Identity theft and break-ins are only a part of the bigger picture as it relates to a person's ability to regulate the use of their personal information. The privacy and financial security of individuals is increasingly at risk due to the widespread collection of personal information by both the public

and private sectors. Credit card transactions, magazine subscriptions, telephone numbers, real estate records, automobile registrations, consumer surveys, warranty registrations, credit reports, and Internet Web sites are all sources of personal information and form the source material for identity thieves.

The New York State Legislature recognized that a law requiring prompt notification when a person's personal or financial information has be compromised is a good first step in giving people the tools they deserve to protect themselves. The new Information Security Breach and Notification Act will require state agencies and corporations who conduct business in New York State to comply with new notification procedures set forth in the Act. In addition to setting up notification requirements for state agencies and businesses that service New York state residents, the law requires local governments to enact their own notification policy as it applies to town government operations. **The statute requires a local policy to be in place within 120 days of the enactment of the state law, or by April 6, 2006.** A local policy may parallel the State policy – in other words the town policy may be adapted from State Technology Law, §208. Websites to view this law are provided below.

"Private information" under the Act 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.

Notice and reporting obligations are activated when 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. In most cases personal notice to the affected person will be required, but there are exceptions due to cost or volume.

Jones Day Commentaries issued on AUGUST 2005 suggests the following strategies for security and compliance:

Review in house 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 [the town] 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.

To read the New York State Information Security Breach and Notification Act please see:

Chapter 442 of the laws of 2005 - http://public.leginfo.state.ny.us/menugetf.cgi

Chapter 491 of the laws of 2005 - http://public.leginfo.state.ny.us/menugetf.cgi