For the Record

by Wade Beltramo
NYCOM Counsel

Local Government Obligations Under the State's New Information Security Breach and Notification Act

News headlines from 2005 were filled with instance after instance of sensitive private financial information being lost or stolen:

- In March 2005, outsiders gained unauthorized access to LexisNexis files that contained personal data on as many as 310,000 people;[1]
- ChoicePoint, a company which maintains and sells background information on virtually every adult American, had as many as 145,000 individuals' private information stolen;[2]
- One bank lost information on 90,000 of its account holders;[3]
- Marriott Vacation Club lost computer tapes containing credit card account information, Social Security numbers and addresses of approximately 206,000 time-share owners, customers and company employees;[4]
- Chicago-based LaSalle Bank Corp. lost a computer tape containing the names, addresses and Social Security numbers of two million residential mortgage customers;[5]
- A former Blockbuster Video store employee, using the store's on-line database, stole 65 customers' credit card numbers, Social Security numbers, and other private information, to buy more than $117,000 in trips, electronics, and even a new Mercedes-Benz;[6] and
- The personal information of 70,000 Ford Motor Company employees were stolen."[7]

In response to this rash of thefts and losses, the New York Legislature enacted the New York State Information Security Breach and Notification Act (the "Act") to protect State residents from unauthorized access to their private information stored in electronic format.

Notification Policy

Every local government must individually adopt its own notification policy within 120 days of the State law's effective date.[8] Because the law became effective on December 7, 2005, cities and villages have until April 6, 2006 to adopt a notification policy.

Because the notification policy adopted by local governments must be consistent with the notification provisions of the statute, it is recommended that local governments base their notification policies on the Cyber Security Citizens' Notification Policy that has been drafted by the State's Office of Cyber Security & Critical Infrastructure Coordination (CSCIC). A copy of this model policy can be downloaded from CSCIC's web site at: www.cscic.state.ny.us/lib/policies/.

Information Covered by the Act

The Act is designed to help protect New York State residents form unauthorized access to their private information stored in electronic format. Under the law, private information means personal information (any information concerning a natural person which, because of name, number, symbol, mark or other identifier, can be used to identify that natural person)[9] in combination with a:

1. Social security number;
2. Driver's license number or non-driver identification card number; or
3. Account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account when the personal information or the data element is either (a) not encrypted or (b) encrypted with an encryption key that has also been acquired.[10]

Under the Act, private information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.[11]

The policy adopted by local governments must provide that the local government disclose, without unreasonable delay, any breach of security, unauthorized access, or unauthorized release of personal computerized data to any New York resident whose information has been accessed or is reasonably believed to have been accessed. While the law requires that notice be given only to New York residents, it is recommended that notice also be provided to non-New York residents.

Method of Notifying Individuals

In the event of a security breach and the unauthorized access of private information, local governments must notify affected individuals by one of the following methods:

1. Written notice;
2. Electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the state entity who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction; or
3. Telephone notification provided that a log of each such notification is kept by the state entity who notifies affected persons.[12]

Regardless of the method used to provide notice, it must include the entity's contact information and a description of the categories of information and the specific personal information and private information that is reasonably believed to have been acquired by a person without valid authorization.

If any New York resident must be notified, the entity must also notify the State Attorney General, the Consumer Protection Board, and the State Office of Cyber Security and Critical Infrastructure Coordination as to the timing, content and distribution of the notices and approximate number of effected persons.[13]

For more information on the Information Security Breach and Notification Act, or to obtain a copy of the model policy, please contact NYCOM Counsel Wade Beltramo at 518-463-1185 or by e-mail at wade@nycom.org.

Endnotes

1. http://msnbc.msn.com/id/7475594
2. http://www.msnbc.msn.com/id/6979897
3. http://money.cnn.com/2006/01/12/news/companies/identity/
4. http://yro.slashdot.org/article.pl?sid=06/01/02/0219231&from=rss
5. http://www.banktech.com/showArticle.jhtml?articleID=175803074
6. http://www.freerepublic.com/focus/f-news/1391494/posts
7. http://www.newsinferno.com/storypages/12-24-2005~001.html
8. State Technology Law § 208(8).
9. State Technology Law § 202(5).
10. State Technology Law § 208(1)(a).
11. Id.
12. State Technology Law § 208(5). The law also provides for entities to use substitute notice, if the entity demonstrates to the state attorney general that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or if the entity does not have sufficient contact information. Substitute notice consist of all of (a) e-mail notice when the entity has an e-mail address for the subject persons; (b) conspicuous posting of the notice on the entity's web site page, if its maintains one; and (c) notification to major statewide media.
13. State Technology Law § 208(7). If more 5,000 New York residents must be notified at one time, the entity must also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents. "Consumer reporting agency" means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. See State Technology Law § 208(1)(d).