The NYS SHIELD Act: What Local Governments Need to Know

The threat of cybercrimes has been a significant focus of the State and local governments for decades. In 2005, long before the recent spate of data breaches and ransomware attacks, the New York State Legislature enacted the New York State Information Security Breach and Notification Act, designed to protect State residents from unauthorized access to their private information stored in electronic format.

The Act requires individuals, businesses, and local governments to adopt a notification policy which mandates that they disclose to any New York resident any breach of security, unauthorized access, or unauthorized release of personal computerized data whose information has been accessed or is reasonably believed to have been accessed.

Since 2005, cyber security threats have increased exponentially as society has greatly expanded its use of technology. In an age where people virtually live off their phones, local governments have kept pace with the ever increasing utilization of and reliance on electronics, offering services to their constituents such as online portals that allow individuals to pay their taxes and parking tickets. Moreover, it is rare to find a municipal service or infrastructure that is not currently reliant on technology which is connected to the internet. This connectivity offers substantial benefits but also exposes local governments to substantial cyber security threats that come along with that connectivity.

In December 2019, internet security firm Kaspersky reported that 174 municipalities suffered ransomware attacks in 2019, a 60 percent year-over-year increase in such attacks. Ransomware attacks substantially impacted New Orleans, Pensacola, and Baltimore, garnering national headlines and highlighting the critical nature of municipal systems. The
importance of local government systems became evident in Baltimore as information necessary to complete real-estate transactions was inaccessible, which in turn temporarily crippled the Baltimore housing market. In addition to those prominent cases, hundreds of other municipalities have fallen prey to ransomware attacks, costing the municipalities millions of dollars to remove the malware and rebuild their computer systems.

As data breaches and ransomware attacks continue, seemingly unabated, on July 25, 2019, Governor Cuomo signed into law the Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act"), which amended New York’s data breach notification law. This article will provide an overview of the SHIELD Act’s requirements as they pertain to local governments.

**Data Breach Notification**

Pursuant to State Technology Law § 208, every local government must either develop a notification policy or adopt a local law which is consistent with Section 208. New York’s local governments should have complied with this requirement back in 2006.² The SHIELD Act expands the definition of private information which is covered by Section 208. Private information is now defined as:

i. Personal information in combination with the following data elements:
   1. Social security number;
   2. Driver’s license number or non-driver identification card number;
   3. Account number, credit or debit card number, in combination with any required security code, access code, password or other information which would permit access to an individual’s financial account;
   4. Account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual’s financial account without additional identifying information, security code, access code, or password; or
   5. Biometric information, meaning data generated by electronic measurements of an individual’s unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual’s identity; when either (a) the data element or (b) the personal information plus the data element is either (i) not encrypted or (ii) is encrypted with an encryption key that has also been acquired; or

ii. A user name or email address in combination with a password or security question and answer that would permit access to an online account.

Private information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

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.

The SHIELD Act clarified that affected persons are not required to be notified if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the person, business, or local government reasonably determines such exposure will not likely result in misuse of such information or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials. Note, however, that such determination must be documented in writing and maintained for at least five years. If the incident affects over 500 New York residents, the written determination must be provided to the NYS Attorney General within 10 days of the determination.

**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 which 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;
3. Telephone notification provided that a log of each such notification is kept by the state entity who notifies affected persons; or
4. If either the cost of providing notice would exceed $250,000 or the number of individuals affected by the data breach exceed 500,000 or there is insufficient contact information for the individuals impacted by the breach, then by (1) email or on the consumer’s online account, (2) conspicuous posting of the notice on the local government’s website, and (3) notification to major statewide media.
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 NYS Attorney General, the Department of State, and the State Police as to the timing, content and distribution of the notices and approximate number of affected persons.4

The SHIELD Act added an alternative method of complying with the notification requirement. Specifically, if a local government notifies affected individuals pursuant to the breach notification under (a) Title V of the federal Gramm–Leach–Bliley Act (15 U.S.C. 6801 to 6809), (b) the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act, Title 23 NYCRR Part 500, or any other federal or New York State data statutes, rules or regulations, then the local government is not required to notify the affected individuals again. Note, however, that the local government must still notify the New York State Attorney General, the Department of State and the Office of Information Technology Services.

For more information on the Information Security Breach and Notification Act, please contact NYCOM General Counsel Wade Beltramo at (518) 463-1185 or by email at wade@nycom.org.

Endnotes
2. State Technology Law § 208(8).
3. 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 website page, if its maintains one; and (c) notification to major statewide media.
4. 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).