

NYS Information Security Breach and Notification Act

Impact on Local Governments
Since 2006, all cities, counties, towns, villages and other local agencies have been required to have information security breach and notification measures in place. They must either develop a notification policy that is consistent with the state law or adopt a local law that is consistent with state law.

What is it?

The Information Security Breach and Notification Act is legislation designed to protect confidential information that could be used in fraud or identity theft and to stimulate a higher level of computer security in organizations in New York State. It requires organizations in New York to notify state agencies and affected residents upon discovery of a security breach when confidential data is reasonably believed to have been acquired without authorization.

What is "confidential data"?

Confidential data, as relates to this law, consists of any personally identifying data (such as a name, personal mark, or other identifier), in conjunction with one or more of the following:

- A social security number
- A driver's license (or non-driver identification card) number
- A credit/debit card number or other interest-bearing account number

In order for the law to apply, either the name or the confidential data element must have been acquired in unencrypted form or in an encrypted form where the encryption key has

been compromised.

What is a security breach?

The unauthorized acquisition (or acquisition without valid authorization) of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the local government.

How do we know if confidential data was acquired?

A local government may consider the following factors, among others:

- indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
- indications that the information has been downloaded or copied; or

- indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Some of these determinations can only be made by technology experts.

Who must be notified?

- New York State residents whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization.
- New York State Office of Cyber Security
- New York State Attorney General's Office
- New York State Department of State Division of Consumer Pro-

Continued on Page 13



*Partnering with Local Leaders to
Accomplish their Goals for Over 45 Years*

**Municipal Engineering • Transportation Surveying
Infrastructure • Water Treatment • Wastewater • Sewer • Parks & Trails
Planning • Economic Development • Zoning • Grant Writing & Administration
Public Outreach • Architecture • Interiors
Offices in Albany and Utica, New York
(518) 458-7112 • www.labergegroup.com**

tection

- In the event that more than 5,000 New York residents are to be notified at one time, the 3 major consumer reporting agencies must also be notified as to the timing, content and distribution of the notices and approximate number of affected people.

When must they be notified?

As soon as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, if any. Time is allowed to determine the scope of the breach and restore the reasonable integrity of the data system. The notifications may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation.

What form is the notification to take?

Either:

- (a) written notice;
- (b) electronic notice, provided that the person to whom notice is required has expressly and voluntarily consented to receiving said notice in electronic form and a log of each such notification is kept;
- (c) telephone notification, provided that a log of each such notification is kept; or
- (d) substitute notice, if a local government demonstrates to the state attorney general that the cost of providing notice would exceed \$250,000, or that the affected people to be notified exceeds 500,000, or the local government does not have sufficient contact information. Substitute notice shall consist of all of the following:
 - (1) e-mail notice, if an e-mail address for the subjects is on file;
 - (2) conspicuous posting of the

notice on the local government's Website page, if one exists; and

- (3) notification to major statewide media.

What must be included in the notice?

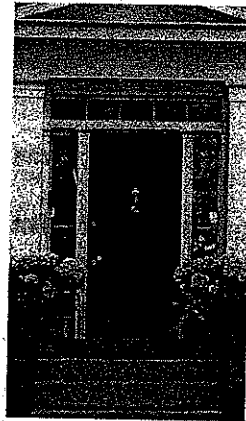
It must include contact information for the local government making the notification and a description of the type of information compromised, in-

cluding specification of what personal information and private information were, or are reasonably believed to have been, acquired.

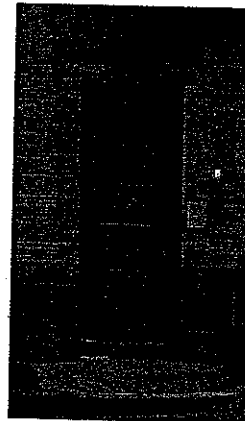
Model Resolution and Local Law

What follows is a model resolution and local law.

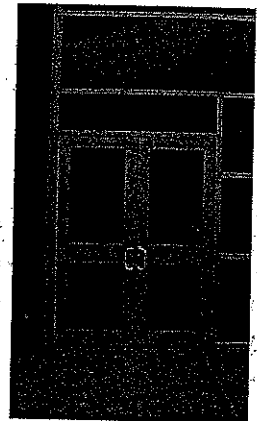
When it comes to
the legal aspects of
community reinvestment,
we know exactly
which doors to open.



Historic Tax Credits



New Markets Tax Credits



Downtown Revitalization

A proud sponsor of and exhibitor at the 2012 Training School and Annual Meeting of the Association of Towns of the State of New York.

CHW

Cannon Heyman & Weiss, LLP

Law Practice Concentrating in Affordable Housing and Community Development Law

WWW.CHWATTYS.COM

© 2011 Cannon Heyman & Weiss, LLP Attorney Advertising.

**RESOLUTION ADOPTING COMPUTER SYSTEM SECURITY BREACH
NOTIFICATION POLICY**

WHEREAS, New York State Technology Law Section 208 establishes procedures to be followed to notify affected individuals in the event of a breach of a computer security system and requires municipalities to adopt a notification policy or local law consistent with these procedures;

NOW, THEREFORE, BE IT

RESOLVED, that the attached "Town of _____ Computer System Security Breach Notification Policy" is hereby approved and adopted as the Town's official policy; and be it

FURTHER RESOLVED, that the Town Supervisor is hereby authorized and directed to take such actions as may be necessary to implement the Policy; and be it

FURTHER RESOLVED, that this Resolution shall take effect immediately.

**TOWN OF _____
COMPUTER SYSTEM SECURITY BREACH
NOTIFICATION POLICY**

1. **PURPOSE.** This Computer System Security Breach Notification Policy is intended to alert individuals to any potential identity theft as quickly as possible so that they may take appropriate steps to protect themselves from and remedy any impacts of the potential identity theft or security breach. This Policy is consistent with and adopted pursuant to New York Technology Law Section 208.

2. **DEFINITIONS.** The following terms have the following meanings:

(a) "Breach of the security of the system" means unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality or integrity of personal information maintained by the Town. Good faith acquisition of personal information by an employee or agent of the Town for the purposes of the employee or agent is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, the Town may consider the following factors, among others:

(1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or

(2) indications that the information has been downloaded or copied; or

(3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

(b) "Consumer reporting agency" means any person or entity 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. A list of consumer reporting agencies may be obtained upon request to the State Attorney General.

(c) "Department" means any board, division, committee, commission, council, department, public authority, public benefit corporation, office or other governmental entity performing a governmental or proprietary function for the Town.

(d) "Personal Information" means any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify that person.

(e) "Private information" means personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

(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.

"Private information" does not include publicly available information that is lawfully made available to the general public from Town records.

(f) "Town" means the Town of _____, County of _____.

3. **DISCLOSURE OF BREACH TO AFFECTED PERSONS.** Any Town Department that owns or licenses computerized data that includes private information must disclose any breach of the security of the system to any individual whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in paragraph 5 below, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The Town shall consult with the State Office of Cyber Security and Critical Infrastructure Coordination to determine the scope of the breach and restoration measures.
4. **DISCLOSURE OF BREACH TO OWNER OR LICENSEE.** If the Town maintains computerized data that includes private information which the Town does not own, the Town must notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.
5. **PERMITTED DELAY.** Notification pursuant to this Policy may be delayed if a law enforcement agency determines that notification could impede a criminal investigation. The notification must be made after the law enforcement agency determines that notification would not compromise any criminal investigation.
6. **METHOD OF NOTIFICATION.** The required notice must be directly provided to the affected individuals by one of the following methods:
 - (a) written notice;
 - (b) electronic notice, provided that the person to whom notice is required to be provided has expressly consented to receiving notice in electronic form and a log of each electronic notification is kept by the Town; and provided further that no person or business may require a person to consent to accepting notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;

Continued on Page 16

the Town; or

(c) telephone notification, provided that a log of each telephone notification is kept by

(d) substitute notice, if the Town demonstrates to the State Attorney General that the cost of providing notice would exceed \$250,000 or that the number of individuals to be notified exceeds 500,000, or the Town does not have sufficient contact information. Substitute notice must include all of the following:

- (1) e-mail notice, when the Town has an e-mail address for the subject persons;
- (2) conspicuous posting of the notice on the Town's Website page, if the Town maintains one; and
- (3) notification to major state-wide media.

7. INFORMATION REQUIRED. Regardless of the method by which notice is provided, the notice must include contact information for the Town and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, acquired.

8. NOTIFICATION OF AGENCIES. (a) Whenever any New York State residents are to be notified pursuant to this Policy, the Town must 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 the approximate number of affected people. Such notice must be made without delaying notice to affected individuals.

(b) Whenever more than 5,000 New York State residents are to be notified at one time, the Town must also notify consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected people. Such notice must be made without delaying notice to affected individuals. ❖

**GIRVIN
FERLAZZO, PC**
ATTORNEYS AT LAW

PROFESSIONAL
COMMITTED
RESPONSIVE
ACCESSIBLE
INVOLVED
EFFICIENT
INTEGRITY-DRIVEN

Helping clients navigate through the legal twists
and turns they confront in their daily travels

518.462.0300
20 Corporate Woods Blvd.
Albany, New York 12211

More information is
available at GirvinLaw.com
Listen to us on Talk 1300 Radio
or at www.talk1300.com
on Saturdays at 11:00 a.m.