

Citizen Information Security Breach Notification Policy
Approved 12/18/2023

A. This policy is consistent with the State Technology Law § 208 as added by Chapters 442 and 491 of the Laws of 2005. This policy requires notification to affected New York residents and nonresidents.

New York State values the protection of private information of individuals. The Village of Brockport ("Village") is required to notify an individual when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and this policy.

Definitions. When used in this section, the following words and phrases shall have the following meanings:

BREACH OF THE SECURITY OF THE SYSTEM — Unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the Village. Good-faith acquisition of personal information by an employee or agent of the Village for the purposes of the Village 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 Village 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.

CONSUMER REPORTING AGENCY — 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. The City may request a list of consumer reporting agencies from the State Attorney General when required to make a notification under Subsection C of this section.

PRIVATE INFORMATION — 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 nondriver 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 federal, state, or local government records.

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

(1)

(2) 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.

(3)

C. Where the City owns or licenses computerized data that includes private information, the City shall

disclose any breach of the security of the system following discovery or notification of the breach in

the security of the system to any person whose private information was, or is reasonably believed to

have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs

of law enforcement, as provided in Subsection E of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

City of Rochester, NY

Downloaded from <https://ecode360.com/RO0104> on 2023-09-29

:1

D. Where the City maintains computerized data that includes private information which the City does

not own, the City shall 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.

B. The Village, after consulting with the State's Office of Cyber Security and Critical Infrastructure Coordination (CSCIC), is to determine the scope of the breach and restoration measures, must notify an individual when it has been determined that there has been, or is reasonably believed to have been a compromise of the individual's private information through unauthorized disclosure.

C. A compromise of private information means the unauthorized acquisition of unencrypted computerized data with private information.

D. If encrypted data is compromised along with the corresponding encryption key, the data is considered unencrypted and thus falls under the notification requirements.

E. Notification may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. In such case, notification will be delayed only as long as needed to determine that notification no longer compromises any investigation.

F. The Village will notify the affected individual directly 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 notice in electronic form and a log of each notification is kept by the Village when notifying affected persons; or
- (3) Telephone notification, provided that a log of each notification is kept by the Village when notifying affected persons; or
- (4) Substitute notice, if the Village demonstrates to the State Attorney General that the cost of providing notice would exceed \$250,000, that the affected class of persons to be notified exceeds 500,000, or that the Village does not have sufficient contact information. The following constitute sufficient substitute notice:
 - (a) E-mail notice when the Village has an e-mail address for the subject persons;
 - (b) Conspicuous posting of the notice on the Village's web site page; and
 - (c) Notification to major statewide media.

G. The Village must notify CSCIC as to the timing, content and distribution of the notices and approximate number of affected persons.

H. The Village must notify the Attorney General and the Consumer Protection Board, whenever notification to a New York resident is necessary, as to the timing, content and distribution of the notices and approximate number of affected persons.

I. Regardless of the method by which notice is provided, the notice must include contact information for the Village when making the notification 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, so acquired.

J. This policy also applies to information maintained on behalf of the Village by a third party.

K. When more than 5,000 New York residents must be notified at one time, then the Village must notify the consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected individuals. This notice, however, will be made without delaying notice to the individuals.