

The New York State Information Security Breach and Notification Act

Please note: The information provided in this document does not constitute, and is no substitute for, legal or other professional advice. Seek consultation from legal or other professional advisors for individualized guidance regarding the application of the law to your particular situation or regarding other compliance-related concerns.

Q1. What is the New York State Information Security Breach and Notification Act?

A. The Act requires that State entities and persons or businesses conducting business in New York who own or license computerized data which includes private information must disclose any breach of the data to any NY residents (State entities must also notify non-residents) whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

When notification is necessary, then the State entity or person or business conducting business in NY must also notify three (3) NYS offices: The NYS Attorney General (AG), the NYS Office of Cyber Security & Critical Infrastructure Coordination (CSCIC) and the Consumer Protection Board (CPB).

Q2. How do I obtain a copy of the New York State Security Breach Reporting Form?

A. Go to the website of the New York State Office of Security & Critical Infrastructure Coordination www.cscic.state.ny.us/security/securitybreach/ReportForm01_09.pdf

Q3. What is the definition of “Private Information”?

A. “Private Information” is defined as “personal information consisting of any 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 number; or
- 3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

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

Q4. What is “Personal Information”?

A. Personal Information means “any information concerning a natural person which, because of name, number, personal mark, or other identifier can be used to identify such natural person.”

Q5. What is “Breach of the security system”?

A. “Breach of the security system” means an “unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business. Good faith acquisition of personal information by an employee or agent of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

Q6. How quickly must the notice be given?

A. The disclosure must be made in “the most expedient time possible without unreasonable delay”, consistent with the legitimate needs of law enforcement. The notification may be delayed if a law enforcement agency determines that such notification may impede a criminal investigation. The notification should be made after the law enforcement agency determines that such notification will not compromise the investigation.

Q7. When must consumer reporting agencies be notified?

A. In the event that more than 5,000 New York residents must be notified at one time, the person or business must also notify consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected persons.

The contact information for the three nationwide consumer reporting agencies are provided in the NYS AG summary, (see Q. 12).

Q8. How do I determine if information has been acquired by an unauthorized person?

A. Some examples given by the statute are:

- 1) indications that 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 individual person, such as fraudulent accounts opened or instances of identity theft reported.

Q9. What are the required methods to notify affected persons?

A. The notice must be directly provided to the affected persons by one of the following methods:

- a) written notice;
- b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving such notice in electronic form and a log of each such

notification is kept by the person or business who notifies affected persons in such form. Furthermore, a person or business may not require a person to consent to accepting such notice in electronic form as a condition of establishing any business relationship or engaging in any transaction.

c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons.

Q10. What if it is too expensive to provide notification by the above methods?

A. The NYS Attorney General may approve a method of Substitute Notice if the cost of providing notice would exceed \$250,000, or the affected class of subject persons to be notified exceeds 5,000, or such business does not have sufficient contact information. Substitute notice may consist of the following:

- 1) e-mail notice when the business has an e-mail address for the subject persons;
- 2) conspicuous posting of the notice on the business's web site page;
- 3) notification to major statewide media.

Q11. What are the possible risks of violating the law?

A. The NYS AG may bring an action in court to seek an injunction. The court may award damages for actual costs or losses incurred by a person entitled to notice, if notification was not provided to such person, including consequential financial losses. If the court determines that a person or business violated the law knowingly or recklessly, the court may impose a civil penalty of the greater of \$5,000 or up to \$10 per instance of failed notification, provided that the latter amount will not exceed \$150,000.

Q12. Where can I get additional information regarding the Information Security Breach and Notification Act?

A. Go to:

New York State Attorney General's Office Security Breach Information
Consumer Fraud & Protection Bureau
120 Broadway, 3rd Floor
New York, NY 10271
http://www.oag.state.ny.us/bureaus/consumer_frauds/tips/debt_collectors.html

New York State Consumer Protection Board (CPB)
5 Empire State Plaza, Suite 2101
New York, NY 12223
www.consumer.state.ny.us/
(the website contains numerous guidelines identity theft prevention and mitigation)

Statutes – General Business Law section 899-aa applicable to all persons and businesses that conduct business in N.Y.S.

New York State Technology Law section 208 - applicable to state entities.