**DATA BREACH NOTIFICATION POLICY FOR NY:**

The NYS Information Security Breach and Notification Act is comprised of section 208 of the State Technology Law and **section 899-aa** of the General Business Law:

"State entities and persons or businesses conducting business who own or license computerized data which includes private information must disclose any breach of the data to New York residents whose private information was exposed."

Under section 899-aa of the General Business Law, a person or business conducting business must also notify (in addition to the affected NYS residents) 3 NYS offices: the NYS Attorney General; the NYS Division of State Police; and the Department of State's Division of Consumer Protection.

*SECTION 899-A DETAILS*:

1. Definition of the below terms given in quotes were explained:
    a. “Personal Information”
    b. “Private Information”, which includes - Personal information + “SSN, Driving License, Bank account related information, and Biometrics”
    c. “Breach of the system’s security”, whose factors include-
        i. indications that the information is in the physical possession and control of an unauthorized person
        ii. indications that the information has been downloaded or copied
        iii. indications that the information was used by an unauthorized person
    d. "Consumer reporting agency"

2. Any person or business which owns/licenses private data shall disclose any security breach ASAP following its discovery/notification, to any New York state resident whose private information was/believed to have been compromised, while also being consistent with the law enforcement's needs (as provided in subdivision four of this section) or anyway necessary to determine the scope of breach and restore integrity
    a. Notice to affected persons is not required if the exposure of private information was inadvertently done by authorized people , and if the person/business reasonably determines that such exposure will not result in misuse, or harm the affected persons both financially and emotionally. Such a determination must be documented in writing and maintained for at least five years. If the incident affects over 500 residents of New York, the person or business shall provide the written determination to the state attorney general within ten days after it

b. If notice of the breach is made to affected persons, nothing in this section shall require any additional notice to those affected persons, but notice still shall be provided to the state attorney general, the department of state and the division of state police pursuant to paragraph (a) in subdivision 8 and to consumer reporting agencies pursuant to paragraph (b) in subdivision 8

3. Any person/business which maintains private information which such person or business does not own shall notify the owner/licensee of the information of any breach of the security of the system immediately following discovery, if the private information was/believed to be accessed or acquired by an unauthorized person.

4. The notification may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification shall be made only after such law enforcement agency determines that such notification does not compromise such investigation.

5. Notices to affected persons shall be delivered via:
    a. written notice
    b. electronic notice, provided that the affected person had voluntarily consented to receiving said notice in electronic form and a log is kept by the person/business who notified it, and in no way can it be an involuntary consent
    c. telephone notification provided that a log is kept by the person/business who notified it
    d. substitute notice, if a person/business demonstrates to the state attorney general that the cost of providing notice would exceed $250, or that the affected class of persons to be notified exceeds $500,000, or if there is no sufficient contact information; then a Substitute notice shall consist of:
        i. e-mail notice, except if the breached data includes information which would permit access to the online account, in which case the person/business shall instead provide the notice whenever the consumer connects to their online account by which they customarily access their account
        ii. conspicuous posting of the notice on such business's active website page
        iii. notification to major statewide media

6.
    a. Whenever the attorney general believes from evidence that there is a violation of this article, they may bring an action in a court to restrain the continuation of such violation. In such action, preliminary relief may be granted under article 63 of the civil practice law and rules. In such action the court may award damages for

actual costs or losses incurred by a person if notification was not provided to such person, including consequential financial losses. Whenever the court shall determine in such action that a person/business violated this article, the court may impose a civil penalty of the greater of $5000 - $20000 per instance of failed notification, up to max $250,000

b. The remedies provided by this section shall be in addition to any other lawful remedy available
c. No action may be brought unless it commenced within 3 years after - either from when the attorney general became aware of the violation, or the date of notice sent pursuant to paragraph (a) of subdivision 8. No action shall be brought after six years from discovery of the breach unless the company took steps to hide the breach.

7. All kinds of notices shall include contact information of the person/business making the notification, the telephone numbers and websites of the relevant state and federal agencies, and a description of the compromised information, including specification of which of the elements of personal and private informations were part of it

8.
   a. In the event that any New York residents are to be notified, the person/business shall notify the state attorney general, the department of state and the division of state police as to the timing, content and distribution of the notices and approximate number of affected persons, and shall also provide a copy of the template of the notice sent to affected persons, without delaying the original notices of affected residents.
   b. In the event that more than 5000 New York residents are to be notified at one time, the person/business shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons, without delaying the original notices of affected residents.

9. Any covered entity required to provide notification of any kind of information breach (to secretary of health and human services pursuant to the Health Insurance Portability and Accountability Act of 1996, or the Health Information Technology for Economic and Clinical Health Act, as amended from time to time) shall provide such notification to the state attorney general within five business days of notifying the secretary.

10. The provisions of this section shall be exclusive and shall preempt any provisions of local law, ordinance or code, and no locality shall impose requirements that are inconsistent with or more restrictive than those set forth in this section.

**DATA BREACH NOTIFICATION POLICY FOR MAS:**

1. According to **Chapter 93-H Section 3**, the Data Breach Notification Law requires businesses and others that own or license personal information of residents of Massachusetts to notify the Office of Consumer Affairs and Business Regulation and the Office of Attorney General when they know or have reason to know of a breach of security
2. They must also provide notice if they know or have reason to know that the personal information of a Massachusetts resident was acquired or used by an unauthorized person, or used for an unauthorized purpose
3. In addition to providing notice to government agencies, you must also notify the consumers whose information is at risk

CHAPTER 93-H DETAILS:

1. A person/agency that maintains or stores any kind of data which they do not own/license shall provide notice to the owner/licensor ASAP when they (1) knows/has reason to know of a breach (2) knows/has reason to know that the personal information of such owner/licensor was acquired, or used by an unauthorized person or for an unauthorized purpose. In addition to that, such person/agency shall cooperate with the owner/licensor on - informing about the breach, the date, the nature thereof, and any steps the person/agency has taken relating to the incident, except that they don't need to disclose confidential business information or trade secrets, or provide notice to an affected resident or unauthorized acquisition or use.

2. Section 3A states that if a person knows or has experienced an incident such as breach of security which includes social security number, the person shall contract with a third party to offer each person whose social security number was disclosed, to offer credit monitoring services at no cost to that said resident at a period of not less than 18 months If the person that experienced the security breach is a consumer reporting agency, then the credit monitoring services are tend to be contracted for a period of not less than 42 months.

3. Any delay in issuing the notice will thereby result in delay of criminal investigation and Section 4 specifies that the person or agency shall cooperate with the law enforcement in the investigation of any security breach or unauthorized use, which shall include the sharing of information related to the incident.

4. According to Section 5, a person or an agency is not relieved to comply with the necessary requirements of the applicability of the other state and federal laws regarding

the protection and the privacy of the personal information. However, if the person or the agency maintains necessary procedures in order to respond to the breach of security which is pursuant to the federal laws and regulations, then they are deemed to be compliant to this chapter. When a breach occurs, the person or the agency is required to notify the Massachusetts residents who are affected accordingly with the necessary procedures. Furthermore, it is the responsibility of the person or the agency to escalate the breach notification to the attorney general, director of the office of consumer affairs and the business regulation of the breach at the earliest possible.

5. The notice which is produced to the attorney general and the director of the office of the consumer affairs and business regulation should consist of the steps or plans taken by the person or the agency related to the breach. These steps and plans should be compliant to the federal laws, rules and regulations and if not, then they are subject to the provisions of this chapter.

**REFERENCES:**


- https://its.ny.gov/breach-notification
- https://www.nysenate.gov/legislation/laws/GBS/899-AA
- https://www.mass.gov/info-details/requirements-for-data-breach-notifications
- https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93H/Section3
- https://www.jonesday.com/en/insights/2010/02/massachusetts-law-raises-the-bar-for-data-security
- https://law.justia.com/codes/massachusetts/2019/part-i/title-xv/chapter-93h/section-5/