STATE OF NEW YORK

8614

2025-2026 Regular Sessions

IN ASSEMBLY

May 22, 2025

Introduced by M. of A. CUNNINGHAM -- read once and referred to the Committee on Governmental Operations

AN ACT to amend the state technology law, in relation to prompt notification to affected individuals in the event of a data breach within certain state entities

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. Paragraphs (b) and (c) of subdivision 1 of section 208 of the state technology law, paragraph (b) of subdivision 1 as amended by chapter 491 of the laws of 2005 and paragraph (c) of subdivision 1 as added by chapter 442 of the laws of 2005, are amended and a new paragraph (e) is added to read as follows:

(b) "Breach of the security of the system" shall mean unauthorized acquisition [~~or~~], acquisition without valid authorization, or unauthorized utilization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by a state entity. Good faith acquisition of personal information by an employee or agent of a state entity for the purposes of the agency 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 utilized, or is reasonably believed to have been acquired or utilized, by an unauthorized person [~~or a~~], person without valid authorization or unauthorized entity, such state entity 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

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD13104-03-5

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

(4) indications that a cybersecurity incident, as defined in paragraph (e) of this subdivision, as occurred.

(c) "State entity" shall mean any state board, bureau, division, committee, commission, council, department, public authority, public benefit corporation, office or other governmental entity performing a governmental or proprietary function for the state of New York, except[~~:~~

~~(1)~~] the judiciary; [~~and~~

~~(2)~~] **but shall include** all cities, counties, municipalities, villages, towns, and other local agencies.

(e) "Cybersecurity incident" shall mean an event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.

§ 2. The opening paragraph of subdivision 2 of section 208 of the state technology law, as amended by chapter 117 of the laws of 2019, is amended to read as follows:

Any state entity that owns [~~or~~]**,** licenses**, or maintains** computerized data that includes private information 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 resident of New York state whose private information was, or is reasonably believed to have been, accessed or acquired by a person **or entity** 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 subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the integrity of the data system. The state entity shall consult with the state office of information technology services to determine the scope of the breach and restoration measures. Within ninety days of the notice of the breach, the office of information technology services shall deliver a report on the scope of the breach and recommendations to restore and improve the security of the system to the state entity.

§ 3. Subdivision 3 of section 208 of the state technology law, as amended by chapter 117 of the laws of 2019, is amended to read as follows:

3. Any state entity that maintains computerized data that includes private information which such agency does not own 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, accessed [~~or~~]**,** acquired**, or utilized** by [~~a~~] **any** person **or entity** without valid authorization.

§ 4. This act shall take effect on the ninetieth day after it shall have become a law.