

STATE OF NEW YORK

9780

IN ASSEMBLY

February 7, 2018

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

AN ACT to amend the state law and the state technology law, in relation to enacting the "personal information protection act"

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

1 Section 1. Short title. This act shall be known and may be cited as
2 the "personal information protection act".

3 § 2. The state law is amended by adding a new article 3-A to read as
4 follows:

ARTICLE 3-A

PERSONAL INFORMATION BILL OF RIGHTS

Section 45. Legislative findings and determinations.

46. Personal information bill of rights.

47. Publication and posting of the personal information bill of rights.

11 § 45. Legislative findings and determinations. The legislature finds
12 and determines that the unauthorized access to, and the theft and misap-
13 propriation of, personal information can cause serious and significant
14 harm. The legislature further finds and determines that in an attempt
15 to provide some level of protection against the unauthorized access to,
16 and the theft and misappropriation, of such personal information, all
17 persons or entities who collect and maintain such personal information
18 should be required to follow certain minimum safeguards, protocols,
19 standards and best practices. The legislature additionally finds and
20 determines that the minimum safeguards, protocols, standards and best
21 practices established by this article seek to promote the protection of
22 personal information contained in both paper and electronic records, and
23 that the objectives of this article are to promote the security and
24 confidentiality of personal information in a manner fully consistent
25 with customarily accepted safeguards, standards, protocols and best
26 practices; protect against unauthorized access, threats or hazards to
27 the security or integrity of such information as best as can be antic-
28 ipated; and protect against unauthorized access to, or the unauthorized

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

LBD14238-03-8

1 use of, such information that may result in serious, significant or
2 substantial harm or inconvenience. The legislature additionally finds
3 and determines that to promote improved protection of personal informa-
4 tion the state technology law should be amended to establish safeguards,
5 standards, protocols and best practices for the protection of personal
6 information by public and private entities, and this chapter should be
7 amended to establish a personal information bill of rights, with such
8 being published and posted by the office of general services.

9 § 46. Personal information bill of rights. The state of New York
10 hereby establishes a personal information bill of rights, to declare the
11 right of all New Yorkers to have their personal information, such as,
12 but not limited to, personal identifying information, protected as
13 follows:

14 1. That all persons or entities that receive and maintain custody of
15 personal information shall have a legal duty to protect such information
16 from unauthorized access and/or unauthorized use.

17 2. That all persons or entities that receive and maintain custody of
18 personal information, in order to protect the personal information over
19 which they maintain custody, shall establish a comprehensive security
20 program, with safeguards, standards, protocols and best practices.

21 3. That the office of information technology services, in order to
22 facilitate the establishment of quality comprehensive security programs,
23 shall design, produce and publish model comprehensive security programs,
24 with safeguards, standards, protocols and best practices, to provide for
25 the protection of personal information held by persons and entities,
26 with such model programs tailored to the size and scope of all such
27 persons or entities.

28 4. That the office of information technology services shall further
29 approve the comprehensive security program of all agencies of state
30 government, and all regulatory agencies of state government shall
31 approve the comprehensive security program of each of their respective
32 regulated entities.

33 5. That the office of information technology services shall addi-
34 tionally incorporate computer system security requirements within its
35 model comprehensive security programs, and shall require such safe-
36 guards, standards, protocols and best practices to be included within
37 all approved security programs.

38 6. That all persons and entities that receive and maintain custody of
39 personal information shall have a legal duty to notify the division of
40 state police within ten days of their discovery of any breach of securi-
41 ty of the personal information under their custody, and all persons and
42 entities that are required to have their comprehensive security program
43 approved, shall have a legal duty to also notify the approving entity
44 within five days of their discovery of any breach of security of the
45 personal information under their custody.

46 7. That in the event a security breach of personal information is
47 discovered that will adversely impact a personal information subject,
48 the person or entity that maintained custody of such personal informa-
49 tion shall further be required to notify all such personal information
50 subjects of the fact that there has been a breach of security involving
51 their personal information.

52 8. That in the event a security breach of personal information is
53 discovered that will adversely impact a personal information subject,
54 and the person or entity that maintained custody of such personal infor-
55 mation did not establish or maintain a comprehensive security program,
56 or did not substantially follow the safeguards, standards, protocols

1 and/or best practices contained within such program, then the personal
2 information subject shall be entitled to bring an action against, and
3 maintain a recovery from, the person or entity that maintained custody
4 of such personal information, together with costs, disbursements and
5 attorney fees.

6 9. That in the event a security breach of personal information is
7 discovered that will adversely impact a personal information subject,
8 and the person or entity that maintained custody of such personal infor-
9 mation did establish and substantially maintain a comprehensive security
10 program, and did substantially follow the safeguards, standards, proto-
11 cols and best practices contained within such program, then the person
12 or entity that maintained custody of such personal information shall be
13 entitled to a defense against any action brought by a personal informa-
14 tion subject.

15 10. That to further protect the security of personal information, the
16 office of information technology services shall further establish and
17 maintain an information sharing and analysis program, to increase the
18 volume, timeliness, and quality of cyber threat information shared with
19 state public and private sector entities so that these entities may
20 better protect and defend themselves against cyber threats and to
21 promote the development of effective defenses and strategies to combat,
22 and protect against, cyber threats and attacks, and thereby better
23 protect personal information stored and/or maintained in electronic
24 format.

25 § 47. Publication and posting of the personal information bill of
26 rights. The office of general services shall publish and prominently
27 post in all state offices, a copy of the personal information bill of
28 rights established in this article. It shall further print and produce a
29 pamphlet on such personal information bill of rights for distribution
30 across the state. The office of general services may sell advertising to
31 be included on such pamphlet to reduce the cost of the production and
32 distribution of the same.

33 § 3. The state technology law is amended by adding a new article 4 to
34 read as follows:

35 ARTICLE IV

36 SAFEGUARDS, STANDARDS, PROTOCOLS AND BEST PRACTICES

37 FOR THE PROTECTION OF PERSONAL INFORMATION

38 Section 401. Definition of terms.

39 402. Duty to protect personal information.

40 403. Comprehensive security program safeguards, standards,
41 protocols and best practices.

42 404. Development of security program safeguards, standards,
43 protocols and best practices.

44 405. Approval of comprehensive security programs.

45 406. Computer system security requirements.

46 407. Breach of security.

47 408. Causes of action.

48 409. Liability protection.

49 410. Information sharing and analysis program.

50 § 401. Definitions of terms. The following definitions are applicable
51 to this article, except where different meanings are expressly speci-
52 fied:

53 1. "Personal information subject" means any natural person who has his
54 or her personal information collected or maintained by a personal infor-
55 mation recipient.

2. "Personal information recipient" means any natural person, corporation, partnership, limited liability company, unincorporated association, government, or other entity, that, in the course of their personal, business, commercial, corporate, association or governmental operations, collects, receives, stores, maintains, processes, or otherwise has access to, personal information.

3. "Personal information collector" means any personal information recipient, that does not maintain or store such personal information, or maintain access to such personal information, for more than five minutes, and was provided with the personal information by the personal information subject.

4. "Personal information holder" means any personal information recipient, that maintains or stores such personal information, or maintains access to such personal information, for more than five minutes, and was provided with the personal information by the personal information subject.

5. "Third party personal information holder" means any personal information recipient, that agrees to collect, receive, store, maintain, process, or otherwise have access to, personal information, and was provided with such personal information from a personal information collector, a personal information holder, or another third party personal information holder.

6. "Personal information" (a) means any information, including paper-based information or electronic information, that contains a New York state resident's first name and last name, or a New York state resident's first initial and last name, in combination with any one or more of the following other informational elements that relate to such resident:

(1) A governmentally issued identification number, including:

(i) social security number;

(ii) driver's license number;

(iii) state issued identification card number;

(iv) military identification card number;

(v) student identification number; or

(vi) a United States passport number;

(2) Personal financial information, including:

(i) financial account information, including:

(A) bank account information;

(B) investment account information;

(C) retirement account information;

(D) deferred compensation account information;

(E) mortgage account information;

(F) car loan account information;

(G) credit line account information;

(H) personal loan account information; or

(I) any other monetary fund or loan account information; including:

(I) the number of such financial account;

(II) any record of such financial account;

(III) a transaction history of such account;

(IV) a balance of such account; and/or

(V) any security code, access code, personal identification number or password, that would permit access to, or use of, such financial account;

(ii) credit or debit card information, including:

(A) the number of such credit card or debit card;

(B) the expiration date of such credit or debit card;

1 (C) the card verification value code number of such credit or debit
2 card;

3 (D) any record of such credit or debit card account;

4 (E) any transaction history of such credit or debit card;

5 (F) any balance of such credit or debit card; and/or

6 (G) any required security code, access code, personal identification
7 number or password, that would permit access to, or use of, such credit
8 or debit card; or

9 (iii) credit status information, including:

10 (A) credit score;

11 (B) credit history; or

12 (C) any information describing credit transactions of the personal
13 information subject;

14 (3) Physical characteristic information, including:

15 (i) the height of the personal information subject;

16 (ii) the weight of the personal information subject;

17 (iii) the hair color of the personal information subject;

18 (iv) the eye color of the personal information subject; and/or

19 (v) any other distinguishing characteristics of the personal informa-
20 tion subject;

21 (4) Biometric information, including:

22 (i) fingerprints of the personal information subject;

23 (ii) voice-prints of the personal information subject;

24 (iii) eye scans of the personal information subject;

25 (iv) blood samples of the personal information subject;

26 (v) deoxyribonucleic acid (DNA) based samples of the personal informa-
27 tion subject;

28 (vi) skin samples of the personal information subject;

29 (vii) hair samples of the personal information subject; and/or

30 (viii) any other biometric information which is intended or collected
31 for the purpose of identification of the personal information subject;
32 or

33 (5) Medical information, including but not limited to, any information
34 collected or maintained about a personal information subject pursuant to
35 examination, testing or treatment for physical or mental illness or
36 wellness, or any other information collected or maintained on a personal
37 information subject by a health care provider or health care insurer;

38 (b) shall not include:

39 (1) personal information that is lawfully obtained from publicly
40 available information, or from federal, state or local government
41 records lawfully made available to the general public; or

42 (2) paper-based information that has been intentionally discarded or
43 abandoned by the personal information subject.

44 7. "Breach of security" means the unauthorized access, viewing, acqui-
45 sition, copying, duplication, removal or any other use of personal
46 information, either in unencrypted form or in encrypted form together
47 with the confidential process or key that is capable of compromising the
48 security, confidentiality, or integrity of personal information. A good
49 faith unauthorized access, viewing or acquisition of personal informa-
50 tion, for the lawful purposes of a personal information collector, shall
51 not be deemed to be a breach of security unless the personal information
52 is thereafter used in an unauthorized manner or is subject to further
53 unauthorized disclosure, as a result of such good faith unauthorized
54 access or acquisition.

1 8. "Record" means any information upon which written, drawn, spoken,
2 visual, or electromagnetic data or images are recorded or preserved,
3 either as paper-based information or electronic information.

4 9. "Paper-based information" means personal information collected or
5 maintained via paper, writing or other drawing medium, or any other
6 physical based, tangible, recording medium.

7 10. "Electronic information" means personal information collected or
8 maintained via computer, telephone, internet, computer network or other
9 electrical, digital, magnetic, wireless, optical, electromagnetic or
10 similar device.

11 11. "Encryption" means the transformation of data into a form in which
12 the meaning of such data cannot be accessed without the use of a confi-
13 dential process or key.

14 12. "Office" means the office of information technology services.

15 § 402. Duty to protect personal information. Every personal informa-
16 tion recipient shall have a legal duty to protect the security and
17 integrity of all personal information in their custody from unauthorized
18 access or unauthorized use.

19 § 403. Comprehensive security program safeguards, standards, protocols
20 and best practices. 1. Comprehensive security programs for personal
21 information recipients. Every personal information recipient shall
22 develop, implement, and maintain a comprehensive personal information
23 security program that is written in one or more readily accessible
24 parts, and contains administrative, technical, and physical safeguards,
25 standards, protocols and best practices detailing the means, methods and
26 practices to be used regarding the personal information recipient's
27 obligations to safeguard, protect and secure the personal information
28 under such comprehensive information security program, appropriate to:

29 (a) the size, scope and type of the personal, business, commercial,
30 corporate, association or governmental operation of the personal infor-
31 mation recipient;

32 (b) the amount of volunteers, employees and/or financial resources
33 available to such personal information recipient;

34 (c) the amount of personal information in the custody of the personal
35 information recipient; and

36 (d) the need for security and confidentiality of the personal informa-
37 tion.

38 2. Safeguards, standards, protocols and best practices for protection
39 of personal information. The safeguards, standards, protocols and best
40 practices contained in the comprehensive personal information security
41 program required by this section shall be consistent with the safe-
42 guards, standards, protocols and best practices for protection of
43 personal information, contained within the model comprehensive security
44 programs published by the office in accordance with section four hundred
45 four of this article, or as set forth in any state or federal regu-
46 lations produced by an executive agency under which the holder of
47 personal information may be regulated.

48 3. Comprehensive personal information security programs may be indi-
49 vidually tailored. The requirement set forth in subdivision two of this
50 section, that the safeguards, standards, protocols and best practices
51 contained in the comprehensive personal information security program
52 shall be consistent with the safeguards, standards, protocols and best
53 practices for protection of personal information contained within the
54 model comprehensive security programs published by the office in accord-
55 ance with section four hundred four of this article, shall not require
56 that the personal information recipient must adopt a model comprehensive

1 personal information security program published by the office in order
2 to develop, implement and maintain a comprehensive personal information
3 security program that is in compliance with this article. Any individ-
4 ually tailored comprehensive personal information security program that
5 provides better or equal safeguards, standards, protocols and best prac-
6 tices for protection of personal information than a model comprehensive
7 personal information security program published by the office in accord-
8 ance with section four hundred four of this article, for a person or
9 entity of equivalent size and scope as the person or entity seeking to
10 develop, implement or maintain an individually tailored comprehensive
11 personal information security program, shall be deemed in compliance
12 with this article.

13 4. Individually tailored comprehensive personal information security
14 programs. Any personal information recipient that wishes to develop,
15 implement and maintain an individually tailored comprehensive personal
16 information security program that is not a model comprehensive personal
17 information security program published by the office, may submit their
18 individually tailored program to the office for a security review to
19 determine, and obtain approval from the office, that such individually
20 tailored program provides better or equal safeguards, standards, proto-
21 cols and best practices for protection of personal information, than a
22 model comprehensive personal information security program published by
23 the office for a person or entity of equivalent size and scope of the
24 person or entity seeking to develop, implement or maintain the individ-
25 ually tailored comprehensive personal information security program. If
26 the office determines that such individually tailored program submitted
27 for security review and approval does not provide such better or equal
28 safeguards, standards, protocols and best practices for protection of
29 personal information, the office shall specify, with detail, their
30 reasons for denial of approval of such plan, together with recommenda-
31 tions on how such plan can be amended to be in compliance with this
32 article and provide such better or equal safeguards, standards, proto-
33 cols and best practices for protection of personal information. If the
34 office does not provide the person or entity that has submitted their
35 individually tailored plan for review and approval, with an approval or
36 such detailed denial of approval of the individually tailored plan,
37 within 90 days of the submission, then such individually tailored plan
38 shall be deemed approved.

39 5. Failure to submit an individually tailored program for approval.
40 The failure of a person or entity to submit an individually tailored
41 comprehensive personal information security program to the office for a
42 security review and approval, as provided by subdivision four of this
43 section, shall not require a court in accordance with section four
44 hundred eight or four hundred nine of this article, to deem such indi-
45 vidually tailored plan as not in compliance with this article. Such
46 failure, shall however, require the court to determine whether such
47 individually tailored plan in question was actually designed to provide
48 better or equal safeguards, standards, protocols and best practices for
49 protection of personal information than a model comprehensive personal
50 information security program published by the office for a person or
51 entity of equivalent size and scope as the defendant, before such court
52 will grant such defendant the liability protections contained within
53 section four hundred nine of this article.

54 § 404. Development of security program safeguards, standards, proto-
55 cols and best practices. 1. The office shall publish model comprehen-
56 sive security programs containing recommended standards, safeguards,

protocols and best practices for personal information recipients. Such model plans shall be tailored in consideration of the following factors of the personal information recipient:

(a) the size, scope and type of the personal, business, commercial, corporate, association or governmental operation of the personal information recipient;

(b) the amount of volunteers, employees and/or financial resources available to such personal information recipient;

(c) the amount of personal information in the custody of the personal information recipient; and

(d) the need for security and confidentiality of the personal information.

2. Requirements for model comprehensive security programs. Every model comprehensive information security program shall include, but shall not be limited to:

(a) Designating one or more persons, or in the case of a business with one or more employees, to maintain the comprehensive information security program;

(b) Clearly identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic information, paper-based information or other records containing personal information, in the custody of the personal information recipient, and evaluating and improving, where necessary, the effectiveness of the current safeguards, standards, protocols and best practices contained within the comprehensive personal information security program for limiting such risks, including but not limited to:

(1) ongoing personal, volunteer, and/or employee training;

(2) personal, volunteer, and/or employee compliance with policies and procedures;

(3) the means for detecting and preventing security system risks; and/or

(4) the means for detecting and preventing security system failures;

(c) Developing safeguards, standards, protocols, best practices and security policies for persons, volunteers and/or employees relating to the storage, access and transportation of records containing personal information on the premises and in the systems and record storage of the personal information recipient;

(d) Developing safeguards, standards, protocols, best practices and security policies for persons, volunteers and/or employees relating to the storage, access and transportation of records containing personal information outside the premises, systems or record storage of the personal information recipient;

(e) Imposing disciplinary measures for violations of the comprehensive information security program rules;

(f) Preventing disassociated persons or volunteers, and/or former or terminated employees from accessing records containing personal information;

(g) Oversight of third party personal information recipients, by:

(1) taking reasonable steps to select and retain third party personal information recipients that are capable of maintaining appropriate security measures, safeguards, standards, protocols and best practices to protect such personal information, consistent with this article and any other applicable federal or state statutes or regulations; and

(2) requiring such third party information recipients by contract to implement and maintain such appropriate security measures for personal information;

1 (h) Reasonable restrictions upon physical access to any electronic
2 information, paper-based information or other records containing
3 personal information, and storage of such information and/or records and
4 data in locked, secure, and/or protected facilities, storage areas or
5 containers;

6 (i) Regular monitoring to ensure that the comprehensive information
7 security program is operating in a manner reasonably calculated to
8 prevent unauthorized access to, or unauthorized use of, personal infor-
9 mation; and upgrading information safeguards, standards, protocols and
10 best practices as necessary to limit and minimize such risks;

11 (j) Reviewing the scope of the safeguards, standards, protocols, best
12 practices and security measures, not less than quarterly, or whenever
13 there is a material change in the personal, business, commercial, corpo-
14 rate, association or governmental operation practices of the personal
15 information recipient that may reasonably effect the security or integ-
16 egrity of records containing personal information;

17 (k) Documenting responsive actions to be taken in connection with any
18 incident involving a breach of security, and mandatory post-incident
19 review of events and actions taken, if any, to make changes in the
20 personal, business, commercial, corporate, association or governmental
21 operation practices of the personal information recipient, relating to
22 protection of personal information; and

23 (l) Detailing all physical security, safeguards, standards, protocols,
24 and best practices, as well as all encryption methods that will be used
25 by the personal information recipient to safeguard the personal infor-
26 mation.

27 § 405. Approval of comprehensive security programs. On or before the
28 first day of April, every personal information holder and every third
29 party personal information holder, that is a state government agency, or
30 a contractor paid by state government, shall annually submit its compre-
31 hensive personal information security program, for approval to the
32 office.

33 § 406. Computer system security requirements. 1. Computer system
34 security program. Every personal information holder or third party
35 personal information holder who electronically stores or transmits
36 personal information shall include in its written, comprehensive infor-
37 mation security program the establishment and maintenance of a computer
38 security system program covering all of its computers, electronic
39 systems and/or networks, including any wireless system.

40 2. Minimum standards for computer system security program. Every
41 personal information holder with more than fifty employees, or with more
42 than one hundred volunteers, and/or with more than one million dollars
43 in annual revenue, shall additionally, establish a computer system secu-
44 rity program, that, at a minimum, and to the extent technically feasi-
45 ble, has the following elements:

46 (a) Secure user authentication protocols including:

47 (1) control of user IDs, user names, passwords and other unique iden-
48 tifiers;

49 (2) a reasonably secure method of assigning and selecting passwords,
50 or use of unique identifier technologies, such as biometrics or token
51 devices;

52 (3) control of data security passwords to ensure that such passwords
53 are kept in a location and/or format that does not compromise the secu-
54 rity of the data they protect;

55 (4) a program of restricting access to active users and active user
56 accounts only; and

1 (5) a requirement to block access to user identification after multi-
2 ple unsuccessful attempts to gain access or the limitation placed on
3 access for the particular system;

4 (b) Secure access control measures that:

5 (1) restrict access to records and files containing personal informa-
6 tion to those who need such information to perform their job duties; and

7 (2) assign unique identifications plus passwords, which are not vendor
8 supplied default passwords, to each person with computer access, that
9 are reasonably designed to maintain the integrity of the security of the
10 access controls;

11 (c) Encryption of all transmitted records and files containing
12 personal information that will travel across public networks, or an
13 alternative system of data protection and security that has been
14 accepted by computer industry standards as equivalent or superior;

15 (d) Encryption of all data containing personal information to be tran-
16 smitted wirelessly, or an alternative system of data protection and
17 security that has been accepted by computer industry standards as equiv-
18 alent or superior;

19 (e) Reasonable monitoring of systems, for unauthorized use of or
20 access to personal information;

21 (f) Encryption of all personal information stored on laptops or other
22 portable devices, or an alternative system of data protection and secu-
23 rity that has been accepted by computer industry standards as equivalent
24 or superior;

25 (g) Protocols for establishing state of the art, air-gapped systems
26 for the storage and maintenance of personal information, or an alterna-
27 tive system of data protection and security that has been accepted by
28 computer industry standards as equivalent or superior;

29 (h) For files containing personal information on a system that is
30 connected to the internet, reasonably up-to-date firewall protection and
31 operating system security patches, reasonably designed to maintain the
32 integrity of the personal information, or an alternative system of data
33 protection and security that has been accepted by computer industry
34 standards as equivalent or superior;

35 (i) Reasonably up-to-date versions of system security agent software
36 which include malware protection and reasonably up-to-date patches and
37 virus definitions, or a version of such software that can still be
38 supported with up-to-date patches and virus definitions, set to receive
39 the most current security updates on a regular basis, or an alternative
40 system of data protection and security that has been accepted by comput-
41 er industry standards as equivalent or superior; and

42 (j) Education and training of persons, volunteers and/or employees on
43 the proper use of the computer security system and the importance of
44 personal information security.

45 3. Review of computer system security programs. Every personal infor-
46 mation holder or third party personal information holder who electron-
47 ically stores or transmits personal information shall further review and
48 update its written, approved, comprehensive personal information securi-
49 ty program not less than annually, to include all feasible recently
50 developed technological safeguards, standards, protocols and best prac-
51 tices that could enhance the protection of the collection, storage and
52 maintenance of such personal information.

53 § 407. Breach of security. 1. Notification to the division of state
54 police. In addition to any other requirements contained within any other
55 provision of law, not later than ten days after discovering a security
56 breach involving personal information, any personal information recipi-

ent that has experienced a breach of security involving personal information, shall make a comprehensive report to the division of state police, in the form and manner required by such division, notifying the division of state police of such security breach.

2. Notification of comprehensive personal information security program approval entity. If such personal information recipient or third party personal information recipient is required in accordance with section four hundred five of this article to obtain approval of its comprehensive personal information security program, then such personal information recipient or third party personal information recipient shall also make a comprehensive report to the entity from which the personal information recipient or third party information recipient is required to obtain approval for its comprehensive personal information security program, in the form and manner required by such approval entity, notifying such approval entity of the security breach.

3. Notification of the chief information officer. Not more than five days after receiving the notification required pursuant to subdivision one or two of this section, the division of state police, and/or the entity required to approve the comprehensive personal information security program pursuant to section four hundred five of this article, shall provide the comprehensive report provided to such division and/or approval entity to the chief information officer of the office. Upon such notification, the chief information officer shall add the pertinent information concerning such breach to the information sharing and analysis program established in accordance with section four hundred ten of this article.

4. Notification of personal information subjects. In addition to any other requirements pursuant to any other provision of law, upon the receipt of the comprehensive report required by subdivision three of this section, the chief information officer of the office may require, in a specified timeframe, and in a specified form and manner, that the personal information recipient, or third party personal information recipient, which sustained the breach of security of the personal information, notify all personal information subjects impacted by the security breach, of the fact that there has been a breach of security involving their personal information. If the chief information officer reasonably believes that the personal information subject will be adversely impacted in any manner by the discovered breach of security, then the chief information officer shall require that the personal information recipient, or third party personal information recipient, notify all such personal information subjects, of the fact that there has been a breach of security involving their personal information.

§ 408. Causes of action. 1. Limitation on civil actions. Any personal information subject may bring a civil action, against a personal information holder in the supreme court of any county in which the personal information recipient resides or conducts business operations, for damages or equitable relief, arising from a breach of security, and in accordance with the provisions of this section. A civil action for damages or equitable relief, shall not, however, be brought by a personal information subject, in any other state court of competent jurisdiction, other than in accordance with the provisions of this section, if such civil action arises out of a breach of security by a personal information holder. No action shall be brought under this section against a personal information collector or a third party personal information collector unless brought in accordance with the

1 provisions of subparagraph four of paragraph (c) of subdivision two of
2 this section.

3 2. Civil actions that may be brought by a personal information subject
4 against a personal information recipient.

5 (a) Timeliness of actions. A civil action may be brought in accordance
6 with this section if such civil action is brought within six years of
7 the date of the reporting of the breach of security as required by
8 section four hundred seven of this article, or in the event no such
9 report was ever made, within any time after the date of the discovery of
10 the breach of security by the personal information subject.

11 (b) Equitable action. Any action brought in accordance with this
12 section, may seek either damages or equitable relief. If a personal
13 information subject seeks equitable relief for a breach of security
14 involving a security breach of personal information from a personal
15 information recipient, and the court determines that such equitable
16 relief is just and proper and should be awarded, then in addition to
17 such equitable relief, the court may also award the personal information
18 subject costs, disbursements and attorneys fees of the action. No action
19 brought under this section for equitable relief shall prohibit a
20 personal information subject from also bringing any additional cause of
21 action for damages, when such additional cause of action is allowed
22 under this article.

23 (c) Actions involving damages. Any action brought in accordance with
24 this section, seeking damages for a breach of security involving a secu-
25 rity breach of personal information from a personal information recipi-
26 ent, shall be brought as follows:

27 (1) personal information holders or third party personal information
28 holders with annual revenues of ten million dollars or more. Any
29 personal information holder, or third party personal information holder,
30 that has annual revenues of ten million dollars or more, that fails to
31 maintain the safeguards, standards, protocols or best practices for the
32 protection of personal information as established in its comprehensive
33 information security program, or that fails to establish a comprehensive
34 personal information security program as required by this article, and
35 that experiences a breach of security involving such personal informa-
36 tion, shall be liable in a civil action brought in accordance with this
37 section, for damages, if the personal information subject involved in
38 the breach of security sustains any damages as a result of such breach.
39 Such liability shall extend to damages in the amount of three times the
40 amount of such damages sustained by the personal information subject, or
41 an amount of up to ten thousand dollars, whichever is less, together
42 with costs, disbursements and attorneys fees of the action. Where the
43 court finds that the personal information holder or a third party
44 personal information holder, intentionally failed to establish a compre-
45 hensive personal information security program, or intentionally failed
46 to seek and obtain approval for a comprehensive personal information
47 security program, where required, or intentionally failed to maintain
48 the safeguards, standards, protocols or best practices for the
49 protection of personal information as established in its comprehensive
50 personal information security program, then the court may also award
51 punitive damages to the plaintiff of an action brought under this subdivi-
52 vision.

53 (2) personal information holders or third party personal information
54 holders with annual revenues of between one million dollars and ten
55 million dollars. Any personal information holder, or third party
56 personal information holder, that has annual revenues of between one

1 million dollars and ten million dollars, and that fails to maintain the
2 safeguards, standards, protocols or best practices for the protection of
3 personal information as established in its comprehensive personal infor-
4 mation security program, or that fails to establish a comprehensive
5 personal information security program as required by this article, and
6 that experiences a breach of security involving such personal informa-
7 tion, shall be liable in a civil action brought in accordance with this
8 section, for damages, if the personal information subject involved in
9 the breach of security sustains any damages as a result of such breach.
10 Such liability shall extend to damages in the amount of three times the
11 amount of such damages sustained by the personal information subject, or
12 an amount of up to five thousand dollars, whichever is less, together
13 with costs, disbursements and attorneys fees of the action. Where the
14 court finds that the personal information holder or a third party
15 personal information holder, intentionally failed to establish a compre-
16 hensive personal information security program, or intentionally failed
17 to seek and obtain approval for a comprehensive personal information
18 security program, where required, or intentionally failed to maintain
19 the safeguards, standards, protocols or best practices for the
20 protection of personal information as established in its comprehensive
21 personal information security program, then the court may also award
22 punitive damages to the plaintiff of an action brought under this subdi-
23 vision.

24 (3) personal information holders or third party personal information
25 holders with annual revenues of less than one million dollars. Any
26 personal information holder, or third party personal information holder,
27 that has annual revenues of less than one million dollars, and that
28 fails to maintain the safeguards, standards, protocols or best practices
29 for the protection of personal information as established in its compre-
30 hensive personal information security program, or that fails to estab-
31 lish a comprehensive personal information security program as required
32 by this article, and that experiences a breach of security involving
33 such personal information, shall be liable in a civil action brought in
34 accordance with this section, for damages, if the personal information
35 subject involved in the breach of security sustains any damages as a
36 result of such breach. Such liability shall extend to damages in the
37 amount of three times the amount of such damages sustained by the
38 personal information subject, or an amount of up to one thousand
39 dollars, whichever is less, together with costs, disbursements and
40 attorneys fees of the action. Where the court finds that the personal
41 information holder or a third party personal information holder, inten-
42 tionally failed to establish a comprehensive personal information secu-
43 rity program, or intentionally failed to seek and obtain approval for a
44 comprehensive personal information security program, where required, or
45 intentionally failed to maintain the safeguards, standards, protocols or
46 best practices for the protection of personal information as established
47 in its comprehensive personal information security program, then the
48 court may also award punitive damages to the plaintiff of an action
49 brought under this subdivision.

50 (4) personal information collectors. Any personal information collec-
51 tor that fails to maintain the safeguards, standards, protocols or best
52 practices for the protection of personal information as established in
53 its comprehensive personal information security program, or that fails
54 to establish a comprehensive personal information security program as
55 required by this article, and that experiences a breach of security
56 involving such personal information, shall be liable in a civil action

1 for damages brought in accordance with this section, in the amount of
2 such damages so sustained. Where the court finds that the personal
3 information collector intentionally failed to establish a comprehensive
4 personal information security program, or intentionally failed to seek
5 and obtain approval for a comprehensive personal information security
6 program, where required, or intentionally failed to maintain the safe-
7 guards, standards, protocols or best practices for the protection of
8 personal information as established in its comprehensive personal infor-
9 mation security program, then the court may also award punitive damages
10 to the plaintiff of an action brought under this subdivision.

11 (5) no action brought under this section for damages shall prohibit a
12 personal information subject from also bringing any additional cause of
13 action for equitable relief, when such additional cause of action is
14 also allowed under this article.

15 § 409. Liability protection. 1. It shall be a complete defense to any
16 civil action brought in accordance with section four hundred eight of
17 this article, for the personal information recipient that is the defend-
18 ant in such action, that such personal information recipient established
19 and maintained a comprehensive personal information security program, as
20 required by this article, and substantially followed and complied with
21 all provisions of such comprehensive personal information security
22 program, and substantially maintained, if required, all computer system
23 security requirements, in accordance with section four hundred six of
24 this article, and substantially maintained, if required, the proper
25 approval for such comprehensive personal information security program,
26 in accordance with section four hundred five of this article, at the
27 time of the breach of such security.

28 2. Any civil action brought by a personal information subject, in any
29 court of competent jurisdiction, involving damages arising from a breach
30 of security that is not brought in accordance with the provisions of
31 section four hundred eight of this article, shall be dismissed without
32 prejudice, against such personal information recipient or third party
33 personal information recipient, but that such personal information
34 subject may bring a new, subsequent action, if timely, in accordance
35 with the provisions of section four hundred eight of this article.

36 § 410. Information sharing and analysis program. 1. The office shall
37 establish and maintain a voluntary New York state cyber security infor-
38 mation sharing and analysis program.

39 2. It shall be the purpose of the New York state cyber security infor-
40 mation sharing and analysis program to increase the volume, timeliness,
41 and quality of cyber threat information shared with state public and
42 private sector entities so that these entities may better protect and
43 defend themselves against cyber threats and to promote the development
44 of effective defenses and strategies to combat, and protect against,
45 cyber threats and attacks.

46 3. To facilitate the purposes of the New York state cyber security
47 information sharing and analysis program, the office shall promulgate
48 regulations, in accordance with the provisions of this section.

49 4. The regulations promulgated pursuant to subdivision three of this
50 section shall:

51 (a) Provide for the timely production of unclassified reports of cyber
52 threats to the state and its public and private sector entities, includ-
53 ing, but not limited to, all participants in the information sharing and
54 analysis program, with express details on threats that identify a
55 specific targeted entity or specific threat type or activity;

1 (b) Address the need to protect intelligence and law enforcement
2 sources, methods, operations, and investigations;

3 (c) Establish a process that rapidly disseminates the reports produced
4 pursuant to paragraph (a) of this subdivision, to any targeted entity,
5 any program participant, and such other and further public and private
6 entities as the office shall deem necessary to advance the purposes of
7 this subdivision;

8 (d) Provide for protections from liability for entities sharing and
9 receiving information with the New York state cyber security information
10 and analysis program, so long as the entity acted in good faith;

11 (e) Establish a system for tracking the production, dissemination, and
12 disposition of the reports produced in accordance with the provisions of
13 this subdivision;

14 (f) Establish an enhanced cyber security services program, within the
15 state, to provide for procedures, methods and directives, for a volun-
16 tary information sharing program, that will provide cyber threat and
17 technical information collected from both public and private sector
18 entities, to all participants in the information sharing and analysis
19 program and all such private and public sector entities as the office
20 deems prudent, and to also advise all critical infrastructure companies
21 or commercial service providers that offer security services to critical
22 infrastructure on cyber security threats and defense measures;

23 (g) Seek to develop strategies to maximize the utility of cyber threat
24 information sharing between and across the private and public sectors;

25 (h) Promote the use of private and public sector subject matter
26 experts to address cyber security needs in the state, with these subject
27 matter experts providing advice regarding the content, structure, and
28 types of information most useful to critical infrastructure owners and
29 operators in reducing and mitigating cyber risks;

30 (i) Establish a consultative process to coordinate improvements to the
31 cyber security of critical infrastructure, where as part of the consul-
32 tative process, the public and private entities of the state shall
33 engage;

34 (j) Provide that the office shall seek and consider the advice of the
35 division of homeland security and emergency services, the division of
36 state police, the center for internet security, and such other and
37 further private and public sector entities, universities, and cyber
38 security experts as the office may deem prudent; and

39 (k) Establish a baseline framework to reduce cyber risk to critical
40 infrastructure and public and private computer systems, networks and
41 operations.

42 5. The office shall use the information sharing and analysis program
43 developed under this section to lead in the development of a voluntary
44 framework to reduce cyber risks to critical infrastructure and public
45 and private computer systems, networks and operations, to be known as
46 the cyber security framework.

47 6. The development of the cyber security framework shall:

48 (a) Include a set of standards, methodologies, procedures, and proc-
49 esses that align policy, business, and technological approaches to
50 address cyber risks;

51 (b) Incorporate voluntary consensus standards, safeguards, protocols
52 and best practices to the fullest extent possible;

53 (c) Provide a prioritized, flexible, repeatable, performance-based,
54 and cost-effective approach, including information security measures and
55 controls, to help owners and operators of critical infrastructure and

1 public and private computer systems, networks and operations, to identi-
2 fy, assess, and manage cyber risk;

3 (d) Focus on identifying cross-sector security standards and guide-
4 lines applicable to critical infrastructure and public and private
5 computer systems, networks and operations;

6 (e) Identify areas for improvement that should be addressed through
7 future collaboration with particular sectors and standards-developing
8 organizations;

9 (f) Enable technical innovation and account for organizational differ-
10 ences, to provide guidance that is technology neutral and that enables
11 critical infrastructure sectors and public and private computer systems,
12 networks and operations, to benefit from a competitive market for
13 products and services that meet the standards, methodologies, proce-
14 dures, processes, safeguards, protocols and best practices to be devel-
15 oped to address cyber risks;

16 (g) Include guidance for measuring the performance of an entity in
17 implementing the cyber security framework;

18 (h) Include methodologies to identify and mitigate impacts of the
19 cyber security framework and associated information security measures or
20 controls on business confidentiality, and to protect individual privacy
21 and civil liberties; and

22 (i) Engage in the review of threat and vulnerability information and
23 technical expertise.

24 7. The regulations promulgated pursuant to subdivision three of this
25 section shall additionally establish a voluntary critical infrastructure
26 cyber security program to support the adoption of the cyber security
27 framework by owners and operators of critical infrastructure and any
28 other interested entities, where under this program implementation guid-
29 ance or supplemental materials would be developed to address sector-spe-
30 cific risks and operating environments.

31 8. In developing the New York state cyber security information sharing
32 and analysis program in accordance with the provisions of this section,
33 the office, in consultation with the division of homeland security and
34 emergency services and the division of state police, shall produce and
35 submit a report, to the governor, the temporary president of the senate,
36 and the speaker of the assembly, making recommendations on the feasibil-
37 ity, security benefits, and relative merits of incorporating security
38 safeguards, standards, protocols and best practices into acquisition
39 planning and contract administration. Such report shall further address
40 what steps can be taken to harmonize and make consistent existing
41 procurement requirements related to cyber security and the feasibility
42 of including risk-based security standards into procurement and contract
43 administration.

44 § 4. This act shall take effect on the one hundred eightieth day after
45 it shall have become a law; provided, however, that the office of infor-
46 mation technology services is authorized and directed to (i) publish its
47 model comprehensive security programs containing recommended standards,
48 safeguards, protocols and best practices for holders of personal infor-
49 mation in accordance with section 404 of the state technology law, as
50 added by section three of this act, and (ii) establish the information
51 sharing and analysis program and promulgate regulations regarding the
52 same, in accordance with section 410 of the state technology law, as
53 added by section three of this act, on or before the one hundred fifti-
54 eth day after this act shall have become a law.