STATE OF NEW YORK

465

2019-2020 Regular Sessions

IN ASSEMBLY

(Prefiled)

January 9, 2019

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:

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

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

§ 45. Legislative findings and determinations. The legislature finds and determines that the unauthorized access to, and the theft and misappropriation of, personal information can cause serious and significant harm. The legislature further finds and determines that in an attempt to provide some level of protection against the unauthorized access to, and the theft and misappropriation, of such personal information, all persons or entities who collect and maintain such personal information should be required to follow certain minimum safeguards, protocols, standards and best practices. The legislature additionally finds and determines that the minimum safeguards, protocols, standards and best practices established by this article seek to promote the protection of personal information contained in both paper and electronic records, and that the objectives of this article are to promote the security and confidentiality of personal information in a manner fully consistent

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

LBD03808-01-9

with customarily accepted safeguards, standards, protocols and best practices; protect against unauthorized access, threats or hazards to the security or integrity of such information as best as can be anticipated; and protect against unauthorized access to, or the unauthorized use of, such information that may result in serious, significant or substantial harm or inconvenience. The legislature additionally finds and determines that to promote improved protection of personal information the state technology law should be amended to establish safeguards, standards, protocols and best practices for the protection of personal information by public and private entities, and this chapter should be amended to establish a personal information bill of rights, with such being published and posted by the office of general services.

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

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

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

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

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

5. That the office of information technology services shall additionally incorporate computer system security requirements within its model comprehensive security programs, and shall require such safeguards, standards, protocols and best practices to be included within all approved security programs.

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

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

8. That in the event a security breach of personal information is discovered that will adversely impact a personal information subject, and the person or entity that maintained custody of such personal information did not establish or maintain a comprehensive security program, or did not substantially follow the safeguards, standards, protocols and/or best practices contained within such program, then the personal information subject shall be entitled to bring an action against, and maintain a recovery from, the person or entity that maintained custody of such personal information, together with costs, disbursements and attorney fees.

9. That in the event a security breach of personal information is discovered that will adversely impact a personal information subject, and the person or entity that maintained custody of such personal information did establish and substantially maintain a comprehensive security program, and did substantially follow the safeguards, standards, protocols and best practices contained within such program, then the person or entity that maintained custody of such personal information shall be entitled to a defense against any action brought by a personal information subject.

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

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

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

ARTICLE IV

SAFEGUARDS, STANDARDS, PROTOCOLS AND BEST PRACTICES FOR THE PROTECTION OF PERSONAL INFORMATION

§ 401. Definitions of terms. The following definitions are applicable to this article, except where different meanings are expressly specified:

1. "Personal information subject" means any natural person who has his or her personal information collected or maintained by a personal information 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;

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

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

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

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

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

(iii) credit status information, including:

(A) credit score;

(B) credit history; or

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

(3) Physical characteristic information, including:

(i) the height of the personal information subject;

(ii) the weight of the personal information subject;

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

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

(v) any other distinguishing characteristics of the personal information subject;

(4) Biometric information, including:

(i) fingerprints of the personal information subject;

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

(iii) eye scans of the personal information subject;

(iv) blood samples of the personal information subject;

(v) deoxyribonucleic acid (DNA) based samples of the personal information subject;

(vi) skin samples of the personal information subject;

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

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

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

(b) shall not include:

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

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

7. "Breach of security" means the unauthorized access, viewing, acquisition, copying, duplication, removal or any other use of personal information, either in unencrypted form or in encrypted form together with the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information. A good faith unauthorized access, viewing or acquisition of personal information, for the lawful purposes of a personal information collector, shall

not be deemed to be a breach of security unless the personal information is thereafter used in an unauthorized manner or is subject to further unauthorized disclosure, as a result of such good faith unauthorized access or acquisition.

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

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

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

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

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

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

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

(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. Safeguards, standards, protocols and best practices for protection of personal information. The safeguards, standards, protocols and best practices contained in the comprehensive personal information security program required by this section shall be consistent with the safeguards, standards, protocols and best practices for protection of personal information, contained within the model comprehensive security programs published by the office in accordance with section four hundred four of this article, or as set forth in any state or federal regulations produced by an executive agency under which the holder of personal information may be regulated.

3. Comprehensive personal information security programs may be individually tailored. The requirement set forth in subdivision two of this section, that the safeguards, standards, protocols and best practices contained in the comprehensive personal information security program shall be consistent with the safeguards, standards, protocols and best

practices for protection of personal information contained within the model comprehensive security programs published by the office in accordance with section four hundred four of this article, shall not require that the personal information recipient must adopt a model comprehensive personal information security program published by the office in order to develop, implement and maintain a comprehensive personal information security program that is in compliance with this article. Any individually tailored comprehensive personal information security program that provides better or equal safeguards, standards, protocols and best practices for protection of personal information than a model comprehensive personal information security program published by the office in accordance with section four hundred four of this article, for a person or entity of equivalent size and scope as the person or entity seeking to develop, implement or maintain an individually tailored comprehensive personal information security program, shall be deemed in compliance with this article.

4. Individually tailored comprehensive personal information security programs. Any personal information recipient that wishes to develop, implement and maintain an individually tailored comprehensive personal information security program that is not a model comprehensive personal information security program published by the office, may submit their individually tailored program to the office for a security review to determine, and obtain approval from the office, that such individually tailored program provides better or equal safeguards, standards, protocols and best practices for protection of personal information, than a model comprehensive personal information security program published by the office for a person or entity of equivalent size and scope of the person or entity seeking to develop, implement or maintain the individually tailored comprehensive personal information security program. If the office determines that such individually tailored program submitted for security review and approval does not provide such better or equal safeguards, standards, protocols and best practices for protection of personal information, the office shall specify, with detail, their reasons for denial of approval of such plan, together with recommendations on how such plan can be amended to be in compliance with this article and provide such better or equal safeguards, standards, protocols and best practices for protection of personal information. If the office does not provide the person or entity that has submitted their individually tailored plan for review and approval, with an approval or such detailed denial of approval of the individually tailored plan, within ninety days of the submission, then such individually tailored plan shall be deemed approved.

5. Failure to submit an individually tailored program for approval. The failure of a person or entity to submit an individually tailored comprehensive personal information security program to the office for a security review and approval, as provided by subdivision four of this section, shall not require a court in accordance with section four hundred eight or four hundred nine of this article, to deem such individually tailored plan as not in compliance with this article. Such failure, shall however, require the court to determine whether such individually tailored plan in question was actually designed to provide better or equal safeguards, standards, protocols and best practices for protection of personal information than a model comprehensive personal information security program published by the office for a person or entity of equivalent size and scope as the defendant, before such court

will grant such defendant the liability protections contained within section four hundred nine of this article.

§ 404. Development of security program safeguards, standards, protocols and best practices. 1. The office shall publish model comprehensive 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;

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

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

(j) Reviewing the scope of the safeguards, standards, protocols, best practices and security measures, not less than quarterly, or whenever there is a material change in the personal, business, commercial, corporate, association or governmental operation practices of the personal information recipient that may reasonably effect the security or integrity of records containing personal information;

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

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

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

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

2. Minimum standards for computer system security program. Every personal information holder with more than fifty employees, or with more than one hundred volunteers, and/or with more than one million dollars in annual revenue, shall additionally, establish a computer system security program, that, at a minimum, and to the extent technically feasible, has the following elements:

(a) Secure user authentication protocols including:

(1) control of user IDs, user names, passwords and other unique identifiers;

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

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

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

(5) a requirement to block access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

(b) Secure access control measures that:

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

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

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

(d) Encryption of all data containing personal information to be transmitted wirelessly, or an alternative system of data protection and security that has been accepted by computer industry standards as equivalent or superior;

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

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

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

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

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

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

3. Review of computer system security programs. Every personal information holder or third party personal information holder who electronically stores or transmits personal information shall further review and update its written, approved, comprehensive personal information security program not less than annually, to include all feasible recently developed technological safeguards, standards, protocols and best prac-

tices that could enhance the protection of the collection, storage and maintenance of such personal information.

§ 407. Breach of security. 1. Notification to the division of state police. In addition to any other requirements contained within any other provision of law, not later than ten days after discovering a security breach involving personal information, any personal information recipient 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 provisions of subparagraph four of paragraph (c) of subdivision two of this section.

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

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

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

(c) Actions involving damages. Any action brought in accordance with this section, seeking damages for a breach of security involving a security breach of personal information from a personal information recipient, shall be brought as follows:

(1) personal information holders or third party personal information holders with annual revenues of ten million dollars or more. Any personal information holder, or third party personal information holder, that has annual revenues of ten million dollars or more, that fails to maintain the safeguards, standards, protocols or best practices for the protection of personal information as established in its comprehensive information security program, or that fails to establish a comprehensive personal information security program as required by this article, and that experiences a breach of security involving such personal information, shall be liable in a civil action brought in accordance with this section, for damages, if the personal information subject involved in the breach of security sustains any damages as a result of such breach. Such liability shall extend to damages in the amount of three times the amount of such damages sustained by the personal information subject, or an amount of up to ten thousand dollars, whichever is less, together with costs, disbursements and attorneys fees of the action. Where the court finds that the personal information holder or a third party personal information holder, intentionally failed to establish a comprehensive personal information security program, or intentionally failed to seek and obtain approval for a comprehensive personal information security program, where required, or intentionally failed to maintain the safeguards, standards, protocols or best practices for the protection of personal information as established in its comprehensive personal information security program, then the court may also award

punitive damages to the plaintiff of an action brought under this subdivision.

(2) personal information holders or third party personal information holders with annual revenues of between one million dollars and ten million dollars. Any personal information holder, or third party personal information holder, that has annual revenues of between one million dollars and ten million dollars, and that fails to maintain the safeguards, standards, protocols or best practices for the protection of personal information as established in its comprehensive personal information security program, or that fails to establish a comprehensive personal information security program as required by this article, and that experiences a breach of security involving such personal information, shall be liable in a civil action brought in accordance with this section, for damages, if the personal information subject involved in the breach of security sustains any damages as a result of such breach. Such liability shall extend to damages in the amount of three times the amount of such damages sustained by the personal information subject, or an amount of up to five thousand dollars, whichever is less, together with costs, disbursements and attorneys fees of the action. Where the court finds that the personal information holder or a third party personal information holder, intentionally failed to establish a comprehensive personal information security program, or intentionally failed to seek and obtain approval for a comprehensive personal information security program, where required, or intentionally failed to maintain the safeguards, standards, protocols or best practices for the protection of personal information as established in its comprehensive personal information security program, then the court may also award punitive damages to the plaintiff of an action brought under this subdivision.

(3) personal information holders or third party personal information holders with annual revenues of less than one million dollars. Any personal information holder, or third party personal information holder, that has annual revenues of less than one million dollars, and that fails to maintain the safeguards, standards, protocols or best practices for the protection of personal information as established in its comprehensive personal information security program, or that fails to establish a comprehensive personal information security program as required by this article, and that experiences a breach of security involving such personal information, shall be liable in a civil action brought in accordance with this section, for damages, if the personal information subject involved in the breach of security sustains any damages as a result of such breach. Such liability shall extend to damages in the amount of three times the amount of such damages sustained by the personal information subject, or an amount of up to one thousand dollars, whichever is less, together with costs, disbursements and attorneys fees of the action. Where the court finds that the personal information holder or a third party personal information holder, intentionally failed to establish a comprehensive personal information security program, or intentionally failed to seek and obtain approval for a comprehensive personal information security program, where required, or intentionally failed to maintain the safeguards, standards, protocols or best practices for the protection of personal information as established in its comprehensive personal information security program, then the court may also award punitive damages to the plaintiff of an action brought under this subdivision.

(4) personal information collectors. Any personal information collector that fails to maintain the safeguards, standards, protocols or best practices for the protection of personal information as established in its comprehensive personal information security program, or that fails to establish a comprehensive personal information security program as required by this article, and that experiences a breach of security involving such personal information, shall be liable in a civil action for damages brought in accordance with this section, in the amount of such damages so sustained. Where the court finds that the personal information collector intentionally failed to establish a comprehensive personal information security program, or intentionally failed to seek and obtain approval for a comprehensive personal information security program, where required, or intentionally failed to maintain the safeguards, standards, protocols or best practices for the protection of personal information as established in its comprehensive personal information security program, then the court may also award punitive damages to the plaintiff of an action brought under this subdivision.

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

§ 409. Liability protection. 1. It shall be a complete defense to any civil action brought in accordance with section four hundred eight of this article, for the personal information recipient that is the defendant in such action, that such personal information recipient established and maintained a comprehensive personal information security program, as required by this article, and substantially followed and complied with all provisions of such comprehensive personal information security program, and substantially maintained, if required, all computer system security requirements, in accordance with section four hundred six of this article, and substantially maintained, if required, the proper approval for such comprehensive personal information security program, in accordance with section four hundred five of this article, at the time of the breach of such security.

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

§ 410. Information sharing and analysis program. 1. The office shall establish and maintain a voluntary New York state cyber security information sharing and analysis program.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6. The development of the cyber security framework shall:

(a) Include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks;

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

(c) Provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure and public and private computer systems, networks and operations, to identify, assess, and manage cyber risk;

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

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

(f) Enable technical innovation and account for organizational differences, to provide guidance that is technology neutral and that enables critical infrastructure sectors and public and private computer systems, networks and operations, to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, processes, safeguards, protocols and best practices to be developed to address cyber risks;

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

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

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

7. The regulations promulgated pursuant to subdivision three of this section shall additionally establish a voluntary critical infrastructure cyber security program to support the adoption of the cyber security framework by owners and operators of critical infrastructure and any other interested entities, where under this program implementation guidance or supplemental materials would be developed to address sector-specific risks and operating environments.

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

§ 4. This act shall take effect on the one hundred eightieth day after it shall have become a law; provided, however, that the office of information technology services is authorized and directed to (i) publish its model comprehensive security programs containing recommended standards, safeguards, protocols and best practices for holders of personal infor-

mation in accordance with section 404 of the state technology law, as added by section three of this act, and (ii) establish the information sharing and analysis program and promulgate regulations regarding the same, in accordance with section 410 of the state technology law, as added by section three of this act, on or before the one hundred fifti-eth day after this act shall have become a law.