BPU# _____

CL 252
SR 260
TR xxx
DR F
CR 19

House Copy OLS Copy Public Copy

For Official House Use

BILL NO. _____

Date of Intro. _____

Ref. _____

NOTE TO SPONSOR	Notify OLS if you require changes in this document. A revised copy for introduction will be prepared on the legislative computer system. Handwritten changes will not appear in the printed bill.

AN ACT concerning comprehensive information security programs and supplementing P.L.1960, c.39 (C.56:8-1 et seq.).

Requires certain persons and business entities to maintain comprehensive information security program.

PRIME Sponsor _____ /

CO-Sponsor	District	CO-Sponsor	District

Same as _____ 14/15 Same as _____ 16/17

Suggested allocation: ss.1-4: C.56:8-208 et seq. to 2017/91

DRAFT

AN ACT concerning comprehensive information security programs and supplementing P.L.1960, c.39 (C.56:8-1 et seq.).

BE IT ENACTED *by the Senate and General Assembly of the State of New Jersey:*

1. As used in this act:

"Breach of security" means the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the State. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of the person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

"Electronic" means relating to technology or having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

"Encrypted" means the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

"Owns or licenses" means receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

"Person" means a natural person, corporation, association, partnership or other legal entity, other than an agency, department, board, commission, bureau, division or authority of the State or any political subdivision thereof.

"Personal information" means a New Jersey resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to a resident: (1) Social Security number; (2) driver's license number or state-issued identification card number; or (3) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

"Record" means any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

"Service provider" means any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this act.

D R A F T

2. a. Every person that owns or licenses personal information about a resident of the State shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to:

(1) the size, scope and type of business of the person obligated to safeguard the personal information under the comprehensive information security program;

(2) the amount of resources available to such person;

(3) the amount of stored data; and

(4) the need for security and confidentiality of both consumer and employee information.

The safeguards contained in the program shall be consistent with the safeguards for protection of personal information and information of a similar character set forth in any State or federal regulations by which the person who owns or licenses the information may be regulated.

b. Every comprehensive information security program shall include, but shall not be limited to:

(1) designating one or more employees to maintain the comprehensive information security program;

(2) identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting the risks, including but not limited to:

(a) ongoing employee training, including ongoing training for temporary and contract employees;

(b) employee compliance with policies and procedures; and

(c) means for detecting and preventing security system failures;

(3) developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises;

(4) imposing disciplinary measures for violations of the comprehensive information security program rules;

(5) preventing terminated employees from accessing records containing personal information;

(6) oversee service providers, by:

(a) taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal information consistent with this act and any applicable federal regulations; and

(b) requiring third-party service providers by contract to implement and maintain appropriate security measures for personal information;

D R A F T

(7) reasonable restrictions upon physical access to records containing personal information, and storage of records and data in locked facilities, storage areas or containers;

(8) 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 as necessary to limit risks;

(9) reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information; and

(10) documenting responsive actions 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 business practices relating to protection of personal information.

3. Every person that owns or licenses personal information about a resident of this State and electronically stores or transmits the information shall include in its comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:

a. secure user authentication protocols including:

(1) control of user IDs and other 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 passwords are kept in a location or format that does not compromise the security of the data they protect;

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

(5) blocking 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 that information to perform their job duties; and

(2) assign unique identifications and 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, and encryption of all data containing personal information to be transmitted wirelessly;

DRAFT

d. reasonable monitoring of systems for unauthorized use of or access to personal information;

e. encryption of all personal information stored on laptops or other portable devices;

f. with respect to files containing personal information on a system that is connected to the Internet, reasonably up-to-date firewall protection and operating system security patches, which are reasonably designed to maintain the integrity of the personal information;

g. reasonably up-to-date versions of system security agent software which shall include malware protection and reasonably up-to-date patches and virus definitions, or a version of that software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis; and

h. education and training of employees on the proper use of the computer security system and the importance of personal information security.

4. It shall be an unlawful practice and a violation of P.L.1960, c.39 (C.56:8-1 et seq.) to willfully, knowingly or recklessly violate the provisions of this act.

5. This act shall take effect on the 120th day next following enactment.

D R A F T

STATEMENT

This bill requires any person, corporation, association, partnership or other legal entity that owns or licenses personal information about a resident of this State to develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are necessary to protect the personal information.

The bill provides that it would be an unlawful practice under the consumer fraud act, P.L.1960, c.39 (C.56:8-1 et seq.), to willfully, knowingly or recklessly violate the provisions of the bill. An unlawful practice is punishable by a monetary penalty of not more than $10,000 for a first offense and not more than $20,000 for any subsequent offense. Additionally, a violation can result in cease and desist orders issued by the Attorney General, the assessment of punitive damages, and the awarding of treble damages and costs to the injured.

Requires certain persons and business entities to maintain comprehensive information security program.

DRAFT