DRAFT

Proposed State Data Security Law

9-28-15

SEC. 1. TITLE

This Act is entitled the Data Security Act.

SEC. 2.

The purposes of this Act are to establish the exclusive standards for data security and notification of a breach of data security applicable to licensees subject to the Act, except as otherwise expressly provided in the Act.

SEC. 3. DEFINITIONS.

For purposes of this Act, the following definitions shall apply:

(1) BREACH OF DATA SECURITY

(A) means the unauthorized acquisition of sensitive personal information, owned or maintained by, or on behalf of, a licensee, that compromises the security, confidentiality, or integrity of the information and is likely to cause substantial harm or inconvenience to the individuals to whom the information relates.

(B) does not include:

(i) the unauthorized acquisition of sensitive personal information that is encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable, if the encryption, redaction, or protection process or key is not also acquired;

ii. the good faith acquisition of sensitive personal information by an employee or agent of the licensee for purposes related to the business of the licensee provided the information is not subject to further unauthorized use or disclosure;

iii. the inadvertent disclosure of sensitive personal information to an employee or agent of another licensee who is authorized to access sensitive personal information provided the information is not subject to further unauthorized use or disclosure; or

iv. the unauthorized disclosure of sensitive personal information where the licensee has a good faith belief that the person to whom the unauthorized disclosure was made is not reasonably able to retain the information.

(2) HEALTH INFORMATION means any information or data of an individual who is a resident of this state, except age or gender, created by or derived from a health care provider or the individual, that identifies the individual who is the subject of the information or with respect to which there is a reasonable basis to believe the information could be used to identify the individual, that relates to:

(A) the past, present, or future physical, mental or behavioral health or condition of the individual;

(B) the provision of health care to the individual or

(C) payment for the provision of health care to the individual.

(3) INFORMATION SECURITY PROGRAM means a comprehensive written program that contains administrative, technical, and physical safeguards that a licensee has implemented and maintains to protect the

confidentiality, security, and integrity of personal information when accessing, collecting, disclosing, processing, storing, using, transmitting, disposing of, or otherwise handling such information.

(4) LICENSEE means all licensed insurers, producers and other persons licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to the Insurance Law of this state.

(5) PERSONAL INFORMATION:

(A) means any of the following information of an individual who is a resident of this state, whether in paper or electronic form, that is owned or maintained by, or on behalf of, a licensee:

(i) the individual's first name or initial and last name in combination with:

(I) the individual's non-truncated social security number;

(II) the financial account number, credit card number, or debit card number of the individual, in combination with any security code, password, or other personal identification information required to access the individual's financial account;

(III) the individual's driver's license number, passport number, or other similar number issued by a federal or state government; or

(IV) the individual's user name or email address, in combination with a password or security question and answer that would

permit access to an online or financial account of the individual; or

(ii) any information:

(I) the individual provides to a licensee to obtain an insurance product or service from the licensee;

(II) about the individual resulting from a transaction involving an insurance product or service between a licensee and the individual;

(III) the licensee otherwise obtains about the individual in connection with providing an insurance product or service to the individual; or

(IV) a list, description or other grouping of individuals (and publicly available information pertaining to them), that is derived using the information described in subsection (I) through (III) that is not publicly available; or

(iii) health information of the individual.

(B) does not include:

(i) publicly available information, except as included on a list described in subsection A(ii)(IV) ; or

(ii) any list, description or other grouping of individuals (and publicly available information pertaining to them) that is

derived without using any information described in subsections A(ii)(I)-(III).

(6) PUBLICLY AVAILABLE INFORMATION means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from:

(A) federal, state or local government records;

(B) widely distributed media; or

(C) disclosures to the general public that are required to be made by federal state or local law.

(7) SENSITIVE PERSONAL INFORMATION

(A) means the following information of an individual who is a resident of this state, that is in electronic form and is owned or maintained by, or on behalf of a licensee:

(i) the individual's first name or initial and last name, in combination with:

(I) the individual's non-truncated social security number;

(II) the individual's financial account number, credit card number, or debit card number, in combination with any security code, access code, password, or other personal identification information required to access the individual's financial account;

(III) the individual's driver's license number, passport number, military identification number, or similar identification number issued by a federal or state government;

(IV) A user name or email address, in combination with a password or security

Formatted: Font: (Default) Verdana, 12 pt, Font color: Gray-80%

Formatted: Font: (Default) Verdana, 12 pt, Font color: Gray-80%

Formatted: Normal, No bullets or numbering

question and answer that would permit access to an online or financial account of the individual; or

(V) health information of the individual;

(B) does not include:

(i) any information of the individual described in subsection (5)(A)(ii); or

(ii) publicly available information.

(8) SUBSTANTIAL HARM OR INCONVENIENCE- means

(A) identity theft; or

(B) fraud.

(9) THIRD PARTY SERVICE PROVIDER means a person that maintains, processes or otherwise is permitted access to sensitive personal information in connection with providing services to a licensee.

(a) SECURITY PROCEDURES REQUIRED- -

(1) IN GENERAL- Each licensee shall develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards for the protection of personal information.

(2) OBJECTIVES- A licensee's information security program shall be designed to –

(A) ensure the security and confidentiality of personal information;

(B) protect against any anticipated threats or hazards to the security or integrity of such information; and

(C) protect against unauthorized acquisition of such information that could result in substantial harm or inconvenience to any individual to whom the information relates.

Formatted: Indent: Left: 2.18"

(3) APPROPRIATENESS – A licensee's information security program under subsection (1) shall be appropriate to—

(A) the size and complexity of the licensee;

(B) the nature and scope of the activities of the licensee;

(C) the sensitivity of the personal information to be protected;

(D) the probability and criticality of potential risk to personal information; and

(E) the resources available to the licensee.

(4) ELEMENTS- To develop, implement, maintain, and enforce its information security program, a licensee shall—

(A) designate an employee or employees to coordinate the information security program;

(B) identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of personal information and assess the sufficiency of any safeguards in place to control these risks, including consideration of risks in each relevant area of the licensee's operations, including—

(i) employee training and management;

(ii) information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and

(iii) detecting, preventing, and responding to attacks, intrusions, or other systems failures;

(D) oversee third-party service providers by—

(i) taking reasonable steps to select and retain third-party service providers that are capable of

maintaining appropriate safeguards for the personal information at issue;

(ii) requiring third-party service providers by contract to implement and maintain such safeguards; and

(iii) reasonably overseeing or obtaining an assessment of the third-party service provider's compliance with contractual obligations, where appropriate in light of the licensee's risk assessment; and

(E) evaluate and adjust the information security program in light of the results of the risk assessments and testing and monitoring required by subparagraphs (B), (C), and (D) and any material changes to the licensee's operations or business arrangements, or any other circumstances that the licensee knows or has reason to know may have a material impact on its information security program.

(5) SECURITY CONTROLS- Each licensee shall—

(A) consider whether the following security measures are appropriate for the licensee, and if so, adopt those measures the licensee concludes are appropriate --

(i) access controls on information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing personal information to unauthorized individuals who may seek to obtain this information through fraudulent means;

(ii) access restrictions at physical locations containing personal information, such as buildings, computer facilities, and records storage facilities, to permit access only to authorized individuals;

(iii) encryption of sensitive personal information, while in transit across public networks or in storage on lap top computers, tablets, or other portable devices;

(iv) procedures designed to ensure that information system modifications are consistent with the licensee's information security program;

(v) monitoring systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;

(vi) response programs that specify actions to be taken when the licensee suspects or detects that unauthorized individuals have gained access to information systems; and

(vii) measures to protect against destruction, loss, or damage of personal information due to potential environmental hazards, such as fire and water damage or technological failures;

(B) develop, implement, and maintain appropriate measures to properly dispose of personal information; and

(C) train staff to implement the licensee's information security program.

(6) ADMINISTRATIVE REQUIREMENTS-

(A) BOARD OVERSIGHT- If a licensee has a board of directors, the board or a senior officer designated by the Board, shall oversee the licensee's written information security program;

(B) REPORT TO THE BOARD- If a licensee has a board of directors, its senior management shall report to its board or an appropriate committee of the board at least annually, including describing—

(i) the overall status of the information security program and the licensee's compliance with this Act; and

(ii) material matters related to the development, implementation, and maintenance of the licensee's program, addressing issues such as risk assessment, risk management and control decisions,

service provider arrangements, results of testing, security breaches or violations and management's responses, and recommendations for changes in the information security program.

(b) INVESTIGATION REQUIRED- - If a licensee believes that a breach of data security has or may have occurred in relation to sensitive personal information that is owned or maintained by the licensee, the licensee shall conduct an investigation to—

(1) assess the nature and scope of the incident;

(2) identify any sensitive personal information that may have been involved in the incident;

(3) determine if the sensitive personal information has been acquired without authorization and is reasonably likely to cause substantial harm or inconvenience to the individuals to whom the information relates; and

(4) take reasonable measures to restore the security and confidentiality of the systems compromised in the breach.

(c) NOTICE REQUIRED-

(1) IN GENERAL- If a licensee that owns sensitive personal information determines under subsection (b), or is informed pursuant to paragraph (2) of this subsection (c) or subsection (d), that the unauthorized acquisition of sensitive personal information involved in a breach of data security is reasonably likely to cause substantial harm or inconvenience to the individuals to whom the information relates, the licensee, or other party described in subsection (d), shall--

(A) notify, without unreasonable delay, but not later than sixty days after discovery of the breach of data security:

(i) all individuals to whom the sensitive personal information relates, as required in subsections (1)(B) and (1)(C) of this subsection (c);

(ii) the Department of Insurance if the breach involves sensitive personal information relating to 500 or more individuals ;

(iii) the state Attorney General, if the breach involves sensitive personal information relating to 500 or more individuals; and

(iv) each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, if the breach involves sensitive personal information relating to 1,000 or more individuals.

(B) provide notice to individuals to whom the sensitive personal information relates, by—

(i) written notification by first-class mail sent to the postal address of the individual in the records of the licensee;

(ii) telephonic notification to the number of the individual in the records of the licensee;

(iii) e-mail notification to the individual (or via other electronic means) in the records of the licensee ; or

(iv) substitute notification in print and to broadcast media where the individual whose sensitive personal information was acquired resides, if providing written, telephonic, or e-mail notification is not feasible due to--

(I) lack of sufficient contact information for the individuals that must be notified;

(II) excessive cost to the licensee; or

(III) exigent circumstances; and

(C) provide notice to individuals to whom the sensitive personal information relates, that includes—

(i) a description of the type of sensitive personal information involved in the breach of data security;

(ii) a summary of rights of victims of identity theft prepared under section 609(d) of the Fair Credit Reporting Act (15 U.S.C. 1681g(d)).

(iii) contact information for the three nationwide consumer reporting agencies;

(iv) contact information for the licensee or its designated call center; and

(v) an offer from the licensee that owns the sensitive personal information to the consumer to provide appropriate identity theft protection services free of cost to the individual for a period of not less than twelve months.

(2) LICENSEES THAT MAINTAIN SENSITIVE PERSONAL INFORMATION – A licensee that maintains sensitive personal information it does not own shall notify the licensee that owns the information immediately upon discovery of a breach of data security.

(3) DELAY PERMITTED WHEN REQUESTED BY LAW ENFORCEMENT- A licensee may delay any notification described under paragraph (1) if such delay is requested by a law enforcement agency.

(d) SPECIAL NOTIFICATION REQUIREMENTS-

(1) THIRD PARTY SERVICE PROVIDERS - In the event of a breach of data security in a system maintained by a third-party service provider, that has been contracted to maintain, store, or process data containing sensitive personal information on behalf of a licensee, such third-party service provider shall notify the licensee of the breach of data security immediately following discovery.

(2) AGREEMENT TO PROVIDE NOTICE – Nothing in this section shall prevent or abrogate an agreement between a licensee and another licensee, a third-party service provider or an other third party to provide the notice required under subsection (c)(1)(A).

(e) IDENTITY THEFT PROTECTION- - A licensee that owns sensitive personal information that is required to provide notice to an individual under subsection (c)(1)(A)(i) shall offer to the individual appropriate identity theft protection services free of cost to the individual for a period of not less than twelve months. The licensee shall provide all information necessary for the individual to enroll in such a service or services.

(f) COMPLIANCE - A licensee shall be deemed to be in compliance with subsections (a), (b), and (c), if the licensee is a covered entity for purposes of the regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d-2 note), to the extent that the licensee is in compliance with such regulations.

SEC. 5. ADMINISTRATIVE ENFORCEMENT.

Notwithstanding any other provision of law, section 4 shall be enforced exclusively under [insert reference to state unfair trade practices act or other applicable state law].

SEC. 6. SEVERABILITY

If any section or portion of a section of this statute or its applicability to any person or circumstance is held invalid by a court, the remainder of this statute or the applicability of the provision to other persons or circumstances shall not be affected.