Proposed Model State Cybersecurity Preparedness Legislation

American Financial Services Association

1. Definitions.
(A) "Personal identifying information" means an individual's first name or first initial and last name in combination with one or more of the following data elements that relate to the individual, when the data elements are not protected through encryption or redaction or otherwise rendered unreadable or unusable:

(1) social security number;
(2) driver's license number;
(3) government-issued identification number;
(4) account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account; or
(5) medical, health insurance or unique biometric data of that individual generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

However, personal identifying information does not mean information that is lawfully obtained from publicly available sources or from federal, state or local government records lawfully made available to the general public.

(B) “Person” means an individual, corporation, business trust, estate, trust, partnership, association or other legal entity that conducts business in this state.

2. Required Procedures and Practices. A person who owns or licenses personal identifying information of a resident of this state seeking a safe harbor under subsection 4 shall implement and maintain security procedures and practices to protect personal identifying information from unauthorized access, acquisition, misuse, destruction, modification or disclosure that substantially comply with the National Institute of Science and Technology cybersecurity framework, other industry security framework or statute or regulation, as described in subsection 4.

3. Authority to Enforce. Nothing in this section is intended to, or does, create a private right of action against any person, based on compliance or noncompliance with this section. Authority to review and enforce compliance with this section is vested exclusively in the (NAME OF STATE AGENCY). Any documents, materials or information prepared for and furnished by a person to that agency pursuant to this section shall be confidential and privileged and shall not be discoverable or admissible in any private civil action. No person who received those documents, material or information while acting under the authority of that agency, shall be permitted or required to testify in any private civil action regarding those documents, materials or information. That agency may share that information with any other state or federal agency, provided that it is permitted or required by law to do so and the recipient enters into an agreement with that state agency and the person to maintain the same confidentiality and privileged status of that information.

4. Appropriate Procedures and Practices. (A) A person will be deemed to have appropriate security procedures and practices to protect personal identifying information from unauthorized access, acquisition, destruction, modification or disclosure and shall have a safe harbor, if:

(1) the person is in substantial compliance with any of the following:

(a) National Institute of Standards and Technology Special Publication 800-171;

(b) National Institute of Standard and Technology Special Publications 800-53 and 800-53a;

(c) The Federal Risk and Authorization Management Program;

(d) Center for Internet Security Critical Security Controls;

(e) International Organization for Standardization/International Electrotechnical Commission 27000 family - Information Security Management Systems; or

(f) the standards applicable to the person of the Federal Financial Institutions Examination Council Cybersecurity Assessment Tool, as amended, for the inherent risk level of the person determined using that Tool; or

(2) The person is regulated by the state or federal government and is in substantial compliance with the entirety of any of the following to the extent applicable to that person:

(a) The security requirements of the "Health Insurance Portability and Accountability Act of 1996," as set forth in 45 CFR Part 164 Subpart C, as amended;

(b) the security requirements of Title V of the "Gramm-Leach-Bliley Act of 1999," Public Law 106-102, as amended; or

(c) The "Federal Information Security Modernization Act of 2014," Public Law 113-283, as amended.

(B) Compliance with this section shall constitute a safe harbor to any cause of action that alleges that the failure to implement adequate information security controls resulted in unauthorized access, acquisition, destruction, modification or disclosure of computerized data that compromises the security or confidentiality of personal identifying information owned or licensed by a person and that causes, is reasonably believed to have caused, or is reasonably believed will cause, a material risk of identity theft or other harm to the person or property of a resident of this state.

(C) Following any update to any industry security framework or statute or regulation described above, a person shall have a period of one year from the stated effective date as prescribed in the framework or statute or regulation to comply with the update. If the person complies with the update within one year of the stated effective date found in the framework or statute or regulation as updated, the person shall still be deemed to be in continuous compliance with this section.

5. Severability. If any provision of this section or the application thereof to a person is for any reason held to be invalid, the remainder of the provisions under this section and the application of such provisions to other persons shall not be thereby affected.

6. Notices. This section does not affect any obligation of a person under applicable state or federal law to provide notice of unauthorized access or acquisition of computerized data.

***[NOTE**: Amendments may be need to conform to existing state law and state legislation drafting rules and practices, such as conforming the definition of "Personal identifying information" in subsection 1 to the definition of personal information in any existing state data security breach notification law.]*