

PRELIMINARY WORKING AND DISCUSSION DRAFT

Draft: 2/27/2017 (proposed version 23)

A new model: Insurance Data Security Model Law
Cybersecurity (EX) Task Force.

INSURANCE DATA SECURITY MODEL LAW

Table of Contents

Section 1.	Title
Section 2.	Purpose and Intent
Section 3.	Definitions
Section 4.	Information Security Program
Section 5.	Investigation of a Data Breach
Section 6.	Notification of a Data Breach
Section 7.	Consumer Protections Following a Data Breach
Section 8.	Power of Commissioner
Section 9.	Enforcement
Section 10.	Confidentiality
Section 11.	Penalties
Section 12.	Rules and Regulations
Section 13.	Severability
Section 14.	Effective Date

Section 1. Title

This act shall be known and may be cited as the “Insurance Data Security Act.”

Section 2. Purpose and Intent

~~A. Notwithstanding any other provision of law including [insert reference to state’s general data security breach notification law], the purpose and intent of this Act is to establish the exclusive standards in this state for data security and investigation and notification of a Data Breach applicable to Licensees, as defined in Section 3G.~~

~~This Act shall not be construed as superseding, altering, or affecting any statute, regulation, order or interpretation of law in this state, except to the extent that such statute, regulation, order or interpretation is inconsistent with the provisions of this Act and then only to the extent of the inconsistency. A state statute, regulation, order or interpretation is not inconsistent with the provisions of this Act if the protection such statute, regulation, order or interpretation affords any person is greater than the protection provided under this Act.~~

~~B. It is not the intent of this Act to require that a Licensee send notice to Consumers affected by a Data Breach when notice has been or is being sent to Consumers in accordance with a federal statute or regulation applicable to that Licensee that provides at least as much protection as this Act. It is also not the intent of this Act that a Licensee be required to set up a separate Information Security Program under Section 4 if that Licensee has established and maintained an Information Security Program in accordance with a federal statute or regulation applicable to that Licensee that provides at least as much protection as this Act. Therefore, a Licensee subject to Pub.L. 106–102, 113 Stat. 1338, enacted November 12, 1999, or to Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996, that complies with the privacy and data breach notification requirements of such statutes, or rules, regulations, procedures or guidelines established thereunder, and a Licensee that complies with those statutes, rules, regulations, procedures, or guidelines pursuant to state law requirements, is deemed to be in compliance with the requirements of Sections 4, 5D and 6C of this Act. If a Licensee relies upon this provision it shall provide to the Commissioner, upon request, the specific federal statute or regulation upon which it relies and the manner in which it asserts compliance.~~

~~C. This Act may not be construed to create or imply a private cause of action for violation of its provisions nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.~~

Section 3. Definitions

As used in this Act, the following terms shall have these meanings:

~~A.~~ “Commissioner” means the chief insurance regulatory official of the state.

~~A.B.~~ “Consumer” means an individual, including but not limited to applicants, policyholders, insureds, beneficiaries, claimants, certificate holders and others who is a resident of this state and whose Nonpublic Personal Information is in a Licensee’s possession, custody or control.

~~B.C.~~ “Consumer Reporting Agency” has the same meaning as “consumer reporting agency that compiles and maintains files on consumers on a nationwide basis” in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

~~D.~~ “Data Breach” means the ~~unauthorized acquisition, release or use~~ of unencrypted Personally Identifiable Information by an unauthorized person.

The term “Data Breach” does not include the unauthorized acquisition, ~~release or use~~ of Encrypted Personally Identifiable Information if the encryption, process or key is not also acquired, released or used without authorization.

“Acquisition” does not include a Data Breach ~~for~~ with regard to which the Licensee has determined with a very high degree of certainty that the Personally Identifiable Information released to an unauthorized person has not been used and has been returned or destroyed without ~~further~~ release.

The term “Data Breach” does not include “Data Breach Without Use of Personally Identifiable Information.”

~~E.~~ “Data Breach Without Use of Personally Identifiable Information” means a Data Breach ~~for~~ with regard to which the Licensee has determined with a very high degree of certainty that the Personally Identifiable Information acquired by the unauthorized person has not been used and has been returned or destroyed without further release or acquisition.

~~E.F.~~ “Encrypted” means the transformation of data into a form which results in a low probability of assigning meaning without the use of a protective process or key.

~~D.~~ “Harm or inconvenience” means any of the following or the reasonable likelihood thereof:

~~(1)~~ Identity theft;

~~(2)~~ Fraudulent transactions on financial accounts; or

~~(3)~~ Other misuse as defined by [insert state definition of misuse or comparable term, if applicable].

~~Drafting Note: Several states have defined the term “misuse” in state law and can refer to this in Section 3E(3). If a state does not have this term defined, they may consider either deleting that paragraph or defining misuse above using a definition similar to that of other states. For example, see 17-A Me. Rev. Stat. § 905-A, which provides that~~

~~A person is guilty of misuse of identification if, in order to obtain confidential information, property or services, the person intentionally or knowingly:~~

~~A. Presents or uses a credit or debit card that is stolen, forged, canceled or obtained as a result of fraud or deception;~~

~~B. Presents or uses an account, credit or billing number that that person is not authorized to use or that was obtained as a result of fraud or deception; or~~

~~C. Presents or uses a form of legal identification that that person is not authorized to use.~~

~~E.G.~~ “Information Security Program” means the administrative, technical, and physical safeguards that a Licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle Nonpublic Personal Information.

PRELIMINARY WORKING AND DISCUSSION DRAFT

F.H. “Licensee” means any person or entity licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this state but shall not include a risk retention group chartered and licensed in a state other than this state.

I. “Nonpublic Personal Information” means information:

- (1) A Consumer provides to a Licensee to obtain an insurance product or service from the Licensee;
- (2) About a Consumer resulting from a transaction involving an insurance product or service between a Licensee and a Consumer;
- (3) The Licensee otherwise obtains about a Consumer in connection with providing an insurance product or service to that Consumer;
- (4) Account balance information and payment history;
- (5) The fact that an individual is or has been one of the Licensee’s customers or has obtained an insurance product or service from the Licensee;
- (6) Any information about the Licensee’s Consumer if it is disclosed in a manner that indicates that the individual is or has been the Licensee’s Consumer;
- (7) Any information that a Consumer provides to a Licensee or that the Licensee or its agent otherwise obtains in connection with collecting on a loan or servicing a loan;
- (8) Any information the Licensee collects through an Internet cookie (an information-collecting device from a web server); and
- (9) Information from a Consumer report.
- (10) Health information:
 - (a) That identifies an individual who is the subject of the information; or
 - (b) With respect to which there is a reasonable basis to believe that the information could be used to identify an individual.
- (11) Nonpublic Personal Information does not include:
 - (a) Publicly available information; or
 - (b) Information that does not identify a Consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names or addresses.

G.J. “Personally Identifiable Information” means Nonpublic Personal Information used by the Licensee or under the Licensees possession, custody or control or provided by a Licensee to a Third-Party Service Provider and includes:

- (1) A financial account number relating to a ~~C~~econsumer, including a 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 financial account; or
- (2) ~~Information including:~~ The first name or first initial and last name of a ~~C~~econsumer in combination with:
 - (a) ~~Three or more digits of The the C~~econsumer’s ~~non-truncated~~-social security number;

PRELIMINARY WORKING AND DISCUSSION DRAFT

- (b) The Consumer's driver's license number, passport number, military identification number, or other similar number on a government-issued document;
- (c) A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online or financial account of the Consumer;
- (d) Biometric data of the eConsumer that would permit access to financial accounts of the Consumer;
- (e) Any information of the Consumer that the Licensee has a legal or contractual duty to protect from unauthorized access or public disclosure;
- ~~(f)~~ The Consumer's date of birth;
- ~~(f)(g)~~ The insurance policy number or subscriber identification number;
- ~~(h)~~ Any information or data except age or gender, that relates to:
 - ~~(i)~~ The past, present or future physical, mental or behavioral health or condition of a Consumer;
 - ~~(ii)~~ The provision of health care to a Consumer; or
 - ~~(iii)~~ Payment for the provision of health care to a Consumer; or
- ~~(i)~~ Any other information that would be sufficient to permit the fraudulent assumption of the Consumer's identity or unauthorized access to an account of the Consumer.
- ~~(g)~~ Information that the consumer provides to a licensee to obtain an insurance product or service used primarily for personal, family, or household purposes from the licensee;
- ~~(h)~~ Information about the consumer resulting from a transaction involving an insurance product or service used primarily for personal, family, or household purposes between a licensee and the consumer;
- ~~(i)~~ Information the licensee obtains about the consumer in connection with providing an insurance product or service used primarily for personal, family, or household purposes to the consumer; or
- ~~(j)~~ A list, description, or other grouping of consumers (and publicly available information pertaining to them), that is derived using the information described in Section 3H(2)(g) through (i), that is not publicly available.
- (3) Any of the data elements identified ~~in Section 3H(2)(a) through (f) above~~ when not in connection with the Consumer's first name or initial and last name, if those elements would be sufficient to permit the fraudulent assumption of the Consumer's identity or unauthorized access to an account of the Consumer.
- (4) The term "Personally Identifiable Information" does not include publicly available information that is lawfully made available to the general public and obtained from federal, state, or local government records; or widely distributed media.

~~Any information or data except age or gender, that relates to: The past, present or future physical, mental or behavioral health or condition of a consumer;~~

~~The provision of health care to a consumer; or~~

~~Payment for the provision of health care to a consumer.~~

PRELIMINARY WORKING AND DISCUSSION DRAFT

The term “~~personal Personally Identifiable Information~~” does not include publicly available information that is lawfully made available to the general public and obtained from federal, state, or local government records; or widely distributed media.

“Third-Party ~~S~~Service Provider” means a person or entity, not otherwise defined as a Licensee, that contracts with a Licensee to maintain, process, store or otherwise have access to Nonpublic personal Personal Information under the Licensee’s possession, custody or control.

Section 4. Information Security Program

A. Implementation of an Information Security Program

Commensurate with the size and complexity of the Licensee, the nature and scope of the Licensee’s activities and the sensitivity of the Nonpublic personal Personal Information used by the Licensee or in the licensee’s the Licensee’s possession, custody or control, each Licensee shall develop, implement, and maintain a comprehensive written Information Ssecurity Pprogram that contains administrative, technical, and physical safeguards for the protection of Nonpublic Ppersonal Iinformation. The Licensee shall document, on an ongoing basis, compliance with its Information Ssecurity Pprogram. This documentation shall occur whenever any substantive changes to the Information Security Program occur but no less than on an annual basis.

B. Objectives of Information Security Program

A Licensee’s Information Ssecurity Pprogram shall be designed to:

- (1) Protect the security and confidentiality of Nonpublic Ppersonal Iinformation;
- (2) Protect against any ~~anticipated~~ threats or hazards to the security or integrity of the information;
- (3) Protect against unauthorized access to or use of Nonpublic personal Personal Iinformation, and minimize the likelihood of harm or inconvenience to any Cconsumer; and
- (4) Define and periodically reevaluate a schedule for retention of Nonpublic Ppersonal information and a mechanism for its destruction when no longer needed.

C. Risk Assessment

The Licensee shall:

- (1) Designate one or more an employee or employees or an agent outside vendor and/or service provider designated to act on behalf of the Licensee who is responsible for the Information Ssecurity Pprogram;
- (2) Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of personal information Nonpublic Personal Information or personal information systems;
- (3) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information Nonpublic Personal Information;
- (4) Assess the sufficiency of policies, procedures, personal information systems and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the Licensee’s operations, including:
 - (a) Employee training and management;
 - (b) Information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and

PRELIMINARY WORKING AND DISCUSSION DRAFT

- (c) Detecting, preventing, and responding to attacks, intrusions, or other systems failures; and
- (5) Implement information safeguards to manage the threats identified in its assessment, and regularly assess the effectiveness of the safeguards' key controls, systems, and procedures.

D. Risk Management

The Licensee shall, ~~at a minimum~~:

- (1) (a) Design its Information Security Program to mitigate the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the Licensee's activities, ~~based on generally accepted cybersecurity principles, including implementing the following security measures, as appropriate: measures listed in Section 4D(2).~~
 - (b) ~~Determine appropriate security measures listed in Section 4D(2). Licensees shall use the best practices for cybersecurity protection, detection, and remediation available at the time of the data breach and commensurate with the firm's nature, scope, scale and complexity.~~
- (2) Implement the following security measures, as appropriate:
 - (a) Place access controls on information systems, including controls to authenticate and permit access only to authorized individuals ~~to protect against and controls to prevent~~ the unauthorized acquisition, ~~release or use of~~ ~~personal information~~ Nonpublic Personal Information ~~to or by employees or unauthorized individuals outside of the Licensee;~~
 - (b) Restrict access at physical locations containing ~~personal information~~ Nonpublic Personal Information, only to authorized individuals;
 - (c) ~~Encrypt~~ Protect by encryption or other appropriate means, all personal information ~~Nonpublic Personal Information~~ while being transmitted ~~wirelessly or~~ on a public internet network ~~or wirelessly~~ and all ~~personal information~~ Nonpublic Personal Information stored on a laptop computer or other portable computing or storage device or media;
 - (d) Ensure that information system modifications are consistent with the Licensee's Information Security Program;
 - (e) Utilize ~~state of the art techniques, such as~~ multi-factor authentication procedures, segregation of duties, and employee background checks for employees with responsibilities for, or access to, ~~personal information~~ Nonpublic Personal Information;
 - (f) Regularly test or monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;
 - (g) Implement response procedures that specify actions to be taken when the Licensee suspects or detects that unauthorized individuals have gained access to information systems;
 - (h) Implement measures to protect against destruction, loss, or damage of ~~personal information~~ Nonpublic Personal Information due to environmental hazards, such as fire and water damage ~~or other catastrophes~~ or technological failures; and
 - (i) Develop, implement, and maintain procedures for the secure disposal of ~~personal information~~ Nonpublic Personal Information in any format.
- (3) Include cybersecurity risks in the Licensee's enterprise risk management process; and

PRELIMINARY WORKING AND DISCUSSION DRAFT

- (4) ~~Use generally accepted cybersecurity principles to share information and s~~Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared.

E. Oversight by Board of Directors

If the Licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum:

- (1) Oversee the development, implementation, and maintenance of the Licensee's Information Security Program, including assigning specific responsibility for the plan to the Licensee's executive management or its delegates; and
- (2) Require the Licensee's executive management or its delegates thereof to report in writing at least annually, the following information:
 - (a) The overall status of the Information Security Program and the Licensee's compliance with this Act; and
 - (b) Material matters related to the Information Security Program, addressing issues such as risk assessment, risk management and control decisions, ~~third party service provider~~Third-Party Service Provider arrangements, results of testing, Data Breaches or violations and management's responses thereto, and recommendations for changes in the Information Security Program.
- (3) If executive management delegates responsibilities under this section it shall oversee the development, implementation and maintenance of the Licensee's Information Security Program prepared by the delegate(s) and shall receive a report from the delegate(s) complying with the requirements of the report to the Board of Directors above.

F. Oversight of Third-Party Service Provider Arrangements

- (1) ~~The Licensee shall exercise due diligence in selecting its contract only with third party service provider~~Third-Party Service Providers; and
- (2) ~~Require its Third Party Service Providers by contract to implement appropriate measures designed to meet the objectives of this section and take appropriate steps to confirm that its Third-Party Service Providers have satisfied these obligations. that are capable of maintaining appropriate safeguards for personal information in the licensee's possession, custody or control, and the licensee shall be responsible for any failure by such third party service providers to protect personal information provided by the licensee to the third party service providers consistent with this Act.~~

G. Program Adjustments

The Licensee shall monitor, evaluate and adjust, as appropriate, the Information Security Program consistent with any relevant changes in technology, the sensitivity of its Nonpublic personal information, internal or external threats to information, and the Licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to personal information systems.

Section 5. Investigation of a Data Breach

- A. If the Licensee learns that a Data Breach of Personally Identifiable Information has or may have occurred ~~in relation to personal information in the possession, custody or control of the licensee or any of the licensee's third party service providers,~~ the Licensee, or an outside vendor and/or service provider agent designated to act on behalf of the Licensee, shall conduct a prompt investigation.
- B. During the investigation, the Licensee, or an outside vendor and/or service provider agent designated to act on behalf of the Licensee, shall, at a minimum determine as much of the following information as possible:
- (1) Assess the nature and scope of the Data Breach or potential Data Breach;
 - (2) Identify any Personally Identifiable Information that may have been involved in the Data Breach;
 - (3) Determine whether ~~the P~~ersonally Identifiable Information ~~has been acquired, released or used without authorization~~ a Data Breach or a Data Breach Without Use of Personally Identifiable Information has occurred; and
 - (4) Perform or oversee reasonable measures to restore the security of the information systems compromised in the Data Breach or Data Breach Without Use of Personally Identifiable Information in order to prevent further unauthorized acquisition, release or use of Personally Identifiable Information in the Licensee's possession, custody or control.
- C. If the Licensee learns that a Data Breach has or may have occurred in a system maintained by a Third-Party Service Provider, the Licensee will confirm and document that the Third-Party Service Provider has completed the steps listed in Section 5B above.
- D. Notification to the Commissioner
- As expeditiously as possible and without unreasonable delay but no later than three (3) business days after determining that a Data Breach or a Data Breach Without Use of Personally Identifiable Information may have occurred, the Licensee shall directly or through an outside vendor and/or service provider agent designated to act on behalf of the Licensee for that purpose notify the Commissioner that a Data Breach or a Data Breach Without Use of Personally Identifiable Information may have occurred. The Licensee shall provide as much of the following information as possible: The Licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the Commissioner concerning the Data Breach.
- (1) Date of the Data Breach or a Data Breach Without Use of Personally Identifiable Information;
 - (2) Description of ~~the Data Breach, including how the information was exposed, whether lost, stolen, or breached,~~ including the specific roles and responsibilities of Third Party Service Providers;
 - (3) How the Data Breach or a Data Breach Without Use of Personally Identifiable Information was discovered;
 - (4) If the Licensee has determined the incident was a Data Breach Without Use of Personally Identifiable Information, the basis for this determination.
 - (5) In the event of a Data Breach, whether any lost, stolen, or breached information has been recovered and if so, how this was done;
 - (6) The identity of the source of the Data Breach;

PRELIMINARY WORKING AND DISCUSSION DRAFT

- ~~(4)(7)~~ Whether Licensee has filed a police report or has notified any regulatory, government or law enforcement agencies and, if so, when such notification was provided;
- ~~(8)~~ Description of the specific types of information ~~lost, stolen, or breached (equipment, paper, electronic, claims, applications, underwriting forms, medical records etc.)~~ acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information or types of information allowing identification of the Consumer;
- ~~(9)~~ If the information was Encrypted, the specific encryption, method used and whether the encryption, redaction or protection process or key was also acquired without authorization;
- ~~(10)~~ The period during which the information system was compromised by the Data Breach;
- ~~(11)~~ The number of total Consumers and Consumers of each state affected by the Data Breach. The Licensee shall provide the best estimate in the initial report to the commissioner and states and update this estimate with each subsequent report to the Commissioner pursuant to this section;
- ~~(12)~~ The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed;
- ~~(13)~~ Description of efforts being undertaken to remediate the situation which permitted the Data Breach to occur;
- ~~(14)~~ A copy of the Licensee's privacy policy and a statement outlining the steps the Licensee will take to investigate and notify Consumers affected by the Data Breach; and
- ~~(15)~~ Name of a contact person who is both familiar with the Data Breach and authorized to act for the Licensee.
- ~~The Licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the Commissioner concerning the Data Breach.~~

Section 6. Notification of a Data Breach

- A. ~~If, following during an investigation under Section 5, the Licensee determines that an unauthorized acquisition of personal information Personally Identifiable Information listed in Section 3H(1), (2)(a) through (f), (3) or (4) involved in a Data Breach has occurred, the Licensee, or an outside vendor and/or service provider agent designated to act a third party acting on behalf of the Licensee, shall notify the following within three (3) business days of making such a determination:~~
- ~~(1) All consumers to whom the whose personal information relates was acquired without authorization;~~
- ~~(2)(1) The insurance commissioners of all the states in which a Consumer whose Personally Identifiable Information was or may have been compromised part of the Data Breach resides and the Licensee's domiciliary commissioner;~~
- ~~(3)(2) The relevant Federal and state law enforcement agencies, as appropriate; and~~
- ~~(4)(3) Any relevant payment card network, if the Data Breach involves payment card numbers; and~~
- ~~(5) Each consumer reporting agency, if the data breach involves personal information relating to 500 or more consumers.~~
- ~~B. Notification to the Commissioner~~

~~Notwithstanding the responsibilities prescribed in Sections 5A and 6A of this Act, no later than three (3) business days after determining that a data breach has occurred, the licensee shall notify the commissioner that a data breach has occurred. The licensee shall provide as much of the following information as possible:~~

PRELIMINARY WORKING AND DISCUSSION DRAFT

- ~~(2) — Date of the data breach;~~
- ~~(3) — Description of the data breach, including how the information was exposed, whether lost, stolen, or breached;~~
- ~~(4) — How the data breach was discovered;~~
- ~~(5) — Whether any lost, stolen, or breached information has been recovered and if so, how this was done;~~
- ~~(6) — The identity of the source of the data breach;~~
- ~~(7) — Whether licensee has filed a police report or has notified any regulatory, government or law enforcement agencies and, if so, when such notification was provided;~~
- ~~(8) — Description of the type of information lost, stolen, or breached (equipment, paper, electronic, claims, applications, underwriting forms, medical records etc.);~~
- ~~(9) — Whether, if the information was encrypted, the encryption, redaction or protection process or key was also acquired without authorization;~~
- ~~(10) — The period during which the information system was compromised by the data breach;~~
- ~~(11) — The number of total consumers and consumers of each state affected by the data breach;~~
- ~~(12) — The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed;~~
- ~~(13) — Identification of efforts being undertaken to remediate the situation which permitted the data breach to occur;~~
- ~~(14) — A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the data breach; and~~
- ~~(15) — Name of a contact person who is both familiar with the data breach and authorized to act for the licensee.~~

~~The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the commissioner concerning the data breach.~~

~~C.B.~~ Notification to Consumer Reporting Agencies

~~The Licensee directly or through an outside vendor and/or service provider agent designated to act on behalf of the Licensee shall notify, as expeditiously as possible and without unreasonable delay, and in no case later than sixty (60) calendar days after determining that a Data Breach has occurred, each Consumer Reporting Agency, if the Data Breach involves personal information Personally Identifiable Information listed in Section 3H(1), (2)(a) through (f), (3) or (4) relating to 500 or more Consumers. Notification must include the date of the Data Breach, an estimate of the number of persons affected by the Data Breach, if known, and the actual or anticipated date that persons were or will be notified of the Data Breach.~~

PRELIMINARY WORKING AND DISCUSSION DRAFT

~~D.C.~~ Notification to Consumers

- (1) The Licensee ~~directly or through an outside vendor and/or service provider agent designated to act on behalf of the Licensee for that purpose~~ shall notify all Consumers whose Personally Identifiable Information ~~listed in Section 3H(1), (2)(a) through (f), (3) or (4)~~ was ~~affected part of a Data Breach~~ as expeditedly-~~soon~~ as possible and without unreasonable delay, and in no case later than sixty (60) calendar days after determining that a Data Breach has occurred. Data Breach notice requirements do not apply to incidents of Data Breach Without Use of Personally Identifiable Information.
- (2) If the Consumer is a resident of a state that requires the Licensee to provide notice of a Data Breach, the notice to the Consumer of the Data Breach required under this Section 6 may be provided under either that state's law or under this Section 6.
- (3) As soon as possible but in no event later than the date notice is sent to Consumers, Prior to sending the notification, the Licensee shall provide the Commissioner ~~with a draft copy of the proposed written~~ communication to Consumers. The Licensee's obligation under this section is limited to situations in which the Personally Identifiable Information of residents of this state is affected by the Data Breach.

As part of the Licensee's data security program, the Licensee shall prepare a draft notice for pre-approval by the commissioner so that in the event of the Data Breach the licensee need only add the information specific to the Data Breach.

~~The commissioner shall have the right to review the proposed communication before the licensee sends it to consumers, to ensure compliance with this subsection and to prescribe the appropriate level of consumer protection pursuant to Section 7.~~

The notice must be written in plain straightforward language and include the following information:

- (a) A description of the type of information involved in the Data Breach;
- (b) A description of the action that the Licensee or ~~third party service provider~~Third-Party Service Provider has taken to safeguard the information;
- (c) A summary of rights of victims of identity theft prepared under § 609(d) of the Fair Credit Reporting Act (15 U.S.C. 1681g(d));
- (d) The steps Consumers can take to protect themselves from identity theft or fraud, which shall include an explanation that Consumers shall have a right to do the following:
 - (i) Place a 90-day initial fraud alert on their consumer reports;
 - (ii) Place a seven-year extended fraud alert on their consumer reports;
 - (iii) Place a credit freeze on their consumer reports;
 - (iv) ~~Have-Receive~~ a free copy of their consumer report from each credit bureau;
 - (v) Receive fraudulent information related to the Data Breach removed (or "blocked") from their consumer reports;
 - (vi) Dispute fraudulent or ~~wrong-incorrect~~ information on their consumer reports;
 - (vii) Stop creditors and debt collectors from reporting fraudulent accounts related to the Data Breach;
 - (viii) Receive copies of documents related to the identity theft; and

PRELIMINARY WORKING AND DISCUSSION DRAFT

- (ix) Stop contacts from debt collectors related to the Data Breach;
 - (e) Contact information for the ~~three~~-nationwide Consumer Reporting Agencies;
 - (f) Contact information for the Licensee or its designated call center including email, internet and telephonic methods of contact; and
 - (g) An offer from the Licensee to the Consumer to provide appropriate identity theft protection services free of cost to the Consumer for an appropriate period of time of not less than twelve (12) months, if appropriate, or other consumer protections ordered by the Commissioner pursuant to Section 7 of this Act.
- (4) The Licensee will provide the Consumer notification:
- (a) In writing by first class mail sent to the last known address of the Consumer maintained in the records of the Licensee; or
 - ~~(a)~~(b) Electronically if the Consumer has agreed to be contacted through e-mail or other means pursuant to [insert reference to state Electronic Transactions Act.]; or
 - ~~(b)~~(c) By substitute ~~method~~notification on the Licensee's publicly accessible website and in print and broadcast media statewide in the state or states where the affected Consumers reside, if providing written or electronic notification is not feasible due to:
 - (i) Insufficient contact information for the Consumers who must be notified;
 - ~~(ii) Excessive cost to the Licensee, if the Licensee demonstrates this to the Commissioner's satisfaction; that the cost of providing notice by Section 6D(3)(a) or (b) would be excessive~~
 - (ii) Exigent circumstances providing a ~~or that another~~ legitimate reason exists for substitute notice. The substitute method must include conspicuous posting of the notice on the licensee's publicly accessible website and publication in statewide media in this state, which has been approved by the Commissioner.
 - (d) Substantive notification must be communicated to the Commissioner along with an explanation of the basis for the substitute notification.

E.D. Notice Regarding Data Breaches of Third-Party Service Providers

- (1) In the event of a Data Breach in a system maintained by a ~~third party service provider~~Third-Party Service Provider, the Licensee shall comply with the notice requirement of Sections 6A through 6C unless the Third-Party Service Provider sends the notices on behalf of the Licensee. In the event that the Licensee relies upon the Third-Party Service Provider to send the notices, the Licensee will confirm and document that the notices were actually sent and that the notices satisfy the requirements of this Act. If the notices sent by the Third-Party Service Provider are not in compliance with these requirements, the Licensee will be responsible for the necessary corrections or additions to the notices.
- (2) The computation of Licensee's deadlines shall begin on the day after the ~~third party service provider~~Third-Party Service Provider notifies the Licensee of the Data Breach or the Licensee otherwise has actual knowledge of the Data Breach, whichever is sooner.
- (3) Nothing in this Act shall prevent or abrogate an agreement between a Licensee and another Licensee, a Third Party Service Provider or any other party to fulfill any of the investigation requirements imposed under Section 5 or notice requirements imposed under Section 6.

PRELIMINARY WORKING AND DISCUSSION DRAFT

F.E. Notice Regarding Data Breaches of Insurers to Reinsurers

(1) In the event of a Data Breach involving Personally Identifiable Information that is used by the Licensee or in the possession, custody or control of a Licensee that is acting as an assuming insurer and that does not have a direct contractual relationship with the affected Consumers:

(a) The assuming insurer shall notify its affected ceding insurers and the Commissioner of its state of domicile; and

(b) The ceding insurers that have a direct contractual relationship with the affected Consumers shall fulfill the notification requirements imposed under Section 6A through C.

(2) In the event of a Data Breach involving Personally Identifiable Information that is used by the Licensee or in the possession, custody or control of a Third-Party Service Provider of a Licensee that is acting as an assuming insurer and does not have a direct contractual relationship with the affected Consumers, the Third-Party Service Provider shall notify the Licensee of the Data Breach immediately upon determination that a breach has occurred.

F. Notice Regarding Data Breaches of Insurers to Producers of Record

(1) In the event of a Data Breach involving Personally Identifiable Information that is used by the Licensee or in the possession, custody or control of an insurer and for which the Consumer accessed the insurer's services through an independent insurance producer, the insurer shall, without unreasonable delay, notify the producers of record of all affected Consumers.

(2) In the event of a Data Breach where two or more Licensees have notice obligations under Section 6 of this regulation, the Licensees may satisfy those obligations with a single notice to the effected Consumers. If a Licensee relies upon another Licensee to send the notices, the Licensee will confirm and document that the notices were actually sent and that the notices satisfy the requirements of this Act. If the notices sent are not in compliance with these requirements, the Licensee will be responsible for the necessary corrections or additions to the notices.

G. Notwithstanding the requirements of Section ~~6C6A~~, ~~DB~~, and ~~EC~~, notice may be delayed where requested by an appropriate state or federal law enforcement agency. The ~~C~~ommissioner shall be notified of any such request unless the Licensee is directed not to do so by an appropriate state or federal law enforcement agency.

~~Drafting Note: Section 5 and Section 6 may be duplicative of current state law. Each state should conduct its own analysis to determine whether or not Section 5 and Section 6, in whole or in part, are necessary to be included in its statutes.~~

Section 7. Consumer Protections Following a Data Breach

After reviewing the ~~L~~icensee's ~~D~~ata ~~B~~reach notification, the ~~C~~ommissioner shall prescribe the appropriate level of consumer protection required following the ~~D~~ata ~~B~~reach and how long that protection will be provided. The ~~C~~ommissioner may order the ~~L~~icensee to offer to pay for ~~twelve (12) months or more an appropriate period~~ of identity theft protection for affected ~~C~~onsumers, pay for a credit freeze, or take other action deemed necessary to protect ~~C~~onsumers. In exercising this authority, the Commissioner shall coordinate with commissioners of other states, to the extent appropriate.

Drafting Note: Many states have statutes providing that a ~~C~~onsumer ~~R~~eporting ~~A~~gency cannot charge a fee for a credit freeze on a consumer file when the consumer is a victim of identity theft, which is shown by providing a police report. For an example, *see* Tex. Bus. & Com. Code § 20.04(b). As an alternative to having the ~~L~~icensee pay for the credit freeze, a state should consider referencing that law and providing that the credit freeze is free for consumers after the data breach is reported to law enforcement by the ~~L~~icensee, by showing a data breach notification letter from the ~~L~~icensee. The state may also need to amend its free credit freeze law to ensure this is covered.

~~If the data breach has affected consumers in other states, the commissioner shall, consistent with the requirements of [reference to statute describing the commissioner's general powers] and with the circumstances of the data breach as they affect consumers in this state, cooperate with the insurance regulators of those states in prescribing the appropriate level of consumer protection described in the previous sentence.~~

Section 8. Power of Commissioner

The Commissioner shall have power to examine and investigate into the affairs of any Licensee to determine whether the Licensee has been or is engaged in any conduct in violation of this Act. This power is in addition to the powers which the Commissioner has under [insert applicable statutes governing the investigation or examination of insurers]. Any such investigation or examination shall be conducted pursuant to [insert applicable statutes governing the investigation or examination of insurers].

Section 9. Enforcement

Whenever the Commissioner has reason to believe that a Licensee has been or is engaged in conduct in this state which violates this Act, the Commissioner may ~~issue and serve upon such licensee a statement of charges and notice of hearing to be held at a time and place fixed in the notice. The hearing shall be conducted in accordance with [cite provisions of state administrative procedure act or insurance code applicable to administrative enforcement proceedings for serious violations]~~ take action that is necessary or appropriate to enforce the provisions of this Act.

Section 10. Confidentiality

- A. Any documents, materials or other information in the control or possession of the department of insurance that are furnished by a Licensee or an employee or agent thereof acting on behalf of Licensee pursuant to Section ~~6B5D~~(2), (3), (4), (5), (6), (89), (410), and (12), or that are obtained by the insurance eCommissioner in an investigation or examination pursuant to Section 8 of this Act shall be confidential by law and privileged, shall not be subject to [insert reference to state open records, freedom of information, sunshine or other appropriate law], shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action. However, the insurance eCommissioner is authorized to use the documents, materials or other information in the furtherance of any regulatory or legal action brought as a part of the insurance eCommissioner's duties.
- B. Neither the insurance eCommissioner nor any person who received documents, materials or other information while acting under the authority of the insurance eCommissioner shall be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to Section 10A.
- C. In order to assist in the performance of the insurance eCommissioner's duties under this Act, the insurance eCommissioner:
 - (1) May share documents, materials or other information, including the confidential and privileged documents, materials or information subject to Section 10A, with other state, federal, and international regulatory agencies, with the National Association of Insurance Commissioners, its affiliates or subsidiaries, and with state, federal, and international law enforcement authorities, provided that the recipient agrees to maintain the confidentiality and privileged status of the document, material or other information;
 - (2) May receive documents, materials or information, including otherwise confidential and privileged documents, materials or information, from the National Association of Insurance Commissioners, its affiliates or subsidiaries and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and shall maintain as confidential or privileged any document, material or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material or information; and
 - (3) [OPTIONAL] May enter into agreements governing sharing and use of information consistent with this subsection.
- D. No waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information shall occur as a result of disclosure to the Commissioner under this section or as a result of sharing as authorized in Section 10C.

PRELIMINARY WORKING AND DISCUSSION DRAFT

- E. Nothing in this Act shall prohibit the ~~insurance e~~Commissioner from releasing final, adjudicated actions including for cause terminations that are open to public inspection pursuant to [insert appropriate reference to state law] to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates or subsidiaries.

Drafting Note: States conducting an investigation or examination under their examination law may apply the confidentiality protections of that law to such an investigation or examination.

Section 11. Penalties

In the case of a violation of this Act, a Licensee may be penalized in accordance with [insert general penalty statute].

Section 12. Rules and Regulations

The Commissioner may, ~~in accordance with [the state statute setting forth the ability of the Department to adopt regulations] upon notice and opportunity for all interested persons to be heard,~~ issue such ~~rules,~~ regulations ~~and orders~~ as shall be necessary to carry out the provisions of this Act.

Section 13. Severability

If any provisions of this Act or the application thereof to any person or circumstance is for any reason held to be invalid, the remainder of the Act and the application of such provision to other persons or circumstances shall not be affected thereby.

Section 14. Effective Date

This Act shall take effect on [insert a date which allows at least a one year interval between the date of enactment and the effective date].