STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION MODEL REGULATION

Table of Contents

Section 1.   Preamble

A.   This regulation establishes standards for developing and implementing administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer information, pursuant to Sections 501, 505(b), and 507 of the Gramm-Leach-Bliley Act, codified at 15 U.S.C. 6801, 6805(b) and 6807.

B.   Section 501(a) provides that it is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. Section 501(b) requires the state insurance regulatory authorities to establish appropriate standards relating to administrative, technical and physical safeguards: (1) to ensure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of records or information that could result in substantial harm or inconvenience to a customer.

C.   Section 505(b)(2) calls on state insurance regulatory authorities to implement the standards prescribed under Section 501(b) by regulation with respect to persons engaged in providing insurance.

D.   Section 507 provides, among other things, that a state regulation may afford persons greater privacy protections than those provided by subtitle A of Title V of the Gramm-Leach-Bliley Act. This regulation requires that the safeguards established pursuant to this regulation shall apply to nonpublic personal information, including nonpublic personal financial information and nonpublic personal health information.

Section 2.   Definitions

For purposes of this regulation, the following definitions apply:

A.   "Customer" means a customer of the licensee as the term customer is defined in [cite applicable section of state regulation that corresponds with the NAIC Privacy of Consumer Financial and Health Information Model Regulation].

B.   "Customer information" means nonpublic personal information as defined in Section [cite applicable section of state regulation that corresponds with Section 4S of the NAIC Privacy of Consumer Financial and Health Information Model Regulation] about a customer, whether in paper, electronic or other form, that is maintained by or on behalf of the licensee.

C.   "Customer information systems" means the electronic or physical methods used to access, collect, store, use, transmit, protect or dispose of customer information.

D. "Licensee" means a licensee as that term is defined in Section [cite applicable section of state regulation that corresponds with Section 4Q of the NAIC Privacy of Consumer Financial and Health Information Model Regulation], except that "licensee" shall not include: a purchasing group; or an unauthorized insurer in regard to the excess line business conducted pursuant to [cite applicable regulation or section of state insurance law].

Drafting Note: Service contract providers and extended warranty providers are "licensees" under the insurance laws of many states. Regulators should consider whether they wish to subject these entities to the requirements of this regulation.

E. "Service provider" means a person that maintains, processes or otherwise is permitted access to customer information through its provision of services directly to the licensee.

Section 3. Information Security Program

Each licensee shall implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of customer information. The administrative, technical and physical safeguards included in the information security program shall be appropriate to the size and complexity of the licensee and the nature and scope of its activities.

Section 4. Objectives of Information Security Program

A licensee's information security program shall be designed to:

A. Ensure the security and confidentiality of customer information;

B. Protect against any anticipated threats or hazards to the security or integrity of the information; and

C. Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.

Section 5. Examples of Methods of Development and Implementation

The actions and procedures described in Sections 6 through 9 of this regulation are examples of methods of implementation of the requirements of Sections 3 and 4 of this regulation. These examples are non-exclusive illustrations of actions and procedures that licensees may follow to implement Sections 3 and 4 of this regulation.

Section 6. Assess Risk

The licensee:

A. Identifies reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems;

B. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and

C. Assesses the sufficiency of policies, procedures, customer information systems and other safeguards in place to control risks.

Section 7. Manage and Control Risk

The licensee:

A. Designs its information security program to control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities;

B. Trains staff, as appropriate, to implement the licensee's information security program; and

C.   Regularly tests or otherwise regularly monitors the key controls, systems and procedures of the information security program. The frequency and nature of these tests or other monitoring practices are determined by the licensee's risk assessment.

Section 8.   Oversee Service Provider Arrangements

The licensee:

A.   Exercises appropriate due diligence in selecting its service providers; and

B.   Requires its service providers to implement appropriate measures designed to meet the objectives of this regulation, and, where indicated by the licensee's risk assessment, takes appropriate steps to confirm that its service providers have satisfied these obligations.

Section 9.   Adjust the Program

The licensee monitors, evaluates and adjusts, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer 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 customer information systems.

Section 10.   Determined Violation

Drafting Note: Cite Unfair Trade Practices Act or other applicable state law.

Section 11.   Effective Date

Each licensee shall establish and implement an information security program, including appropriate policies and systems pursuant to this regulation by [insert date].

_____

Chronological Summary of Actions (all references are to the *Proceedings of the NAIC).*

2002 Proc. 1st Quarter 99, 101-103 (model adopted later is printed here).
2002 Proc. 2nd Quarter 7-8 (adopted).

This page is intentionally left blank

STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION MODEL REGULATION

This chart is intended to provide readers with additional information to more easily access state statutes, regulations, bulletins or administrative rulings related to the NAIC model. Such guidance provides readers with a starting point from which they may review how each state has addressed the model and the topic being covered. The NAIC Legal Division has reviewed each state's activity in this area and has determined whether the citation most appropriately fits in the Model Adoption column or Related State Activity column based on the definitions listed below. The NAIC's interpretation may or may not be shared by the individual states or by interested readers.

This chart does not constitute a formal legal opinion by the NAIC staff on the provisions of state law and should not be relied upon as such. Nor does this state page reflect a determination as to whether a state meets any applicable accreditation standards. Every effort has been made to provide correct and accurate summaries to assist readers in locating useful information. Readers should consult state law for further details and for the most current information.

STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION MODEL REGULATION

This page is intentionally left blank

STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION MODEL REGULATION

<u>**KEY:**</u>

MODEL ADOPTION: States that have citations identified in this column adopted the most recent version of the NAIC model in a **substantially similar manner**. This requires states to adopt the model in its entirety but does allow for variations in style and format. States that have adopted portions of the current NAIC model will be included in this column with an explanatory note.

RELATED STATE ACTIVITY: Examples of Related State Activity include but are not limited to: older versions of the NAIC model, statutes or regulations addressing the same subject matter, or other administrative guidance such as bulletins and notices. States that have citations identified in this column **only** (and nothing listed in the Model Adoption column) have **not** adopted the most recent version of the NAIC model in a **substantially similar manner.**

NO CURRENT ACTIVITY: No state activity on the topic as of the date of the most recent update. This includes states that have repealed legislation as well as states that have never adopted legislation.

NAIC MEMBER	MODEL ADOPTION	RELATED STATE ACTIVITY
Alabama	ALA. ADMIN. CODE r. 482-1-126 (2003).	
Alaska	ALASKA ADMIN. CODE tit. 3, § 26.705 (2005).	
American Samoa	NO CURRENT ACTIVITY	
Arizona	ARIZ. ADMIN. CODE §§ 20-6-2101 to 20-6-2104 (2004).	
Arkansas	054.00.77 ARK. CODE R. § 1-13 (2003).	BULLETIN 1-2006 (2006).
California	CAL. CODE REGS. tit. 10, §§ 2689.12 to 2689.20 (2003).	
Colorado	3 COLO. CODE REGS. § 702-6:6-4-2 (2003).	
Connecticut	CONN. AGENCIES REGS. §§ 38a-8-124 to 38a-8-126 (2004).	
Delaware	18 DEL. CODE REGS. § 905 (2002/2003).	
District of Columbia	D.C. MUN. REGS. tit 26, §§ 3613 to 3620.1 (2003).	

STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION MODEL REGULATION

NAIC MEMBER	MODEL ADOPTION	RELATED STATE ACTIVITY
Florida	FLA. ADMIN. CODE ANN. r. 69O-128.030 to 69O-128.035 (2002).	
Georgia	NO CURRENT ACTIVITY	
Guam	NO CURRENT ACTIVITY	
Hawaii	NO CURRENT ACTIVITY	
Idaho		IDAHO CODE ANN. § 28-51-105 (2006/2014).
Illinois	ILL. ADMIN. CODE tit. 50, §§ 4003.10 to 4003.110 (2003).	
Indiana	NO CURRENT ACTIVITY	
Iowa	IOWA ADMIN. CODE r. 191-90.37 to 191-90.40 (2002)	
Kansas	NO CURRENT ACTIVITY	
Kentucky	806 KY. ADMIN. REGS. 3:230 (2004).	
Louisiana	NO CURRENT ACTIVITY	
Maine	ME. CODE R. § 980 (2004).	
Maryland	NO CURRENT ACTIVITY	
Massachusetts		201 MASS. CODE REGS. 17.00 to 17.05 (2008/2009).
Michigan	MICH. ADMIN. CODE r. 500.551 to 500.560 (2004).	
Minnesota	MINN. STAT. §§ 60A.98 to 60A.982 (2005/2014).	
Mississippi	NO CURRENT ACTIVITY	
Missouri	MO. CODE REGS. ANN. tit. 20, § 100-6.110 (2003).	

STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION MODEL REGULATION

NAIC MEMBER	MODEL ADOPTION	RELATED STATE ACTIVITY
Montana	MONT. ADMIN. R. 6.6.7001 to 6.6.7019 (2005).	
Nebraska	210 NEB. ADMIN. CODE § 77 (2003).	
Nevada	NO CURRENT ACTIVITY	
New Hampshire	N.H. CODE ADMIN. R. ANN. INS. 3701.01 to 3711.01 (2004).	
New Jersey	N.J. ADMIN. CODE §§ 11:1-44.1 to 11:1-44.11 (2004).	
New Mexico	NO CURRENT ACTIVITY	
New York	N.Y. COMP. CODES R. & REGS. tit. 11, §§ 421.0 to 421.10 (Regulation 173) (2002).	
North Carolina	N.C. GEN. STAT. §§ 58-39-130 to 58-39-165 (2003).	
North Dakota	N.D. ADMIN. CODE 45-14-02-01 to 45-14-02-03 (2004).	
Northern Marianas	NO CURRENT ACTIVITY	
Ohio	NO CURRENT ACTIVITY	
Oklahoma	OKLA. ADMIN. CODE §§ 365:35-3-1 to 365:35-3-11 (2005).	
Oregon	OR. ADMIN. R. 836-081-0101 to 836-081-0126 (2003).	
Pennsylvania	31 PA. CODE §§ 146c.1 to 146c.11 (2005).	
Puerto Rico	NO CURRENT ACTIVITY	
Rhode Island	230-20 R.I. CODE R. §§ 8.1-8.12(2005).	
South Carolina	NO CURRENT ACTIVITY	

STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION MODEL REGULATION

NAIC MEMBER	MODEL ADOPTION	RELATED STATE ACTIVITY
South Dakota	S.D. ADMIN. R. §§ 20:06:45:20 to 20:06:45:26 (2003).	
Tennessee	NO CURRENT ACTIVITY	
Texas	NO CURRENT ACTIVITY	
Utah	UTAH ADMIN. CODE r. 590-216-1 to 590-216-8 (2002/2012).	
Vermont	VT. CODE R. IH-2002-3 (2003).	
Virgin Islands	NO CURRENT ACTIVITY	
Virginia	VA. CODE ANN. § 38.2-613.2 (2003) (portions of model).	Administrative Letter 2003-4 (2003).
Washington	NO CURRENT ACTIVITY	
West Virginia	W. VA. CODE §§ 114-62-1 to 114-62-6 (2002).	
Wisconsin	NO CURRENT ACTIVITY	
Wyoming	044-55 WYO. CODE R. § 1-12 (2003).	