

FLORIDA

Title XXXIII

REGULATION OF TRADE, COMMERCE, INVESTMENTS, AND SOLICITATIONS

Chapter 501

CONSUMER PROTECTION

Section 501.171 Security of confidential personal information.—

(1) DEFINITIONS.—As used in this section, the term:

(a) “Breach of security” or “breach” means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of the covered entity does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

(b) “Covered entity” means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. For purposes of the notice requirements in subsections (3)-(6), the term includes a governmental entity.

(c) “Customer records” means any material, regardless of the physical form, on which personal information is recorded or preserved by any means, including, but not limited to, written or spoken words, graphically depicted, printed, or electromagnetically transmitted that are provided by an individual in this state to a covered entity for the purpose of purchasing or leasing a product or obtaining a service.

(d) “Data in electronic form” means any data stored electronically or digitally on any computer system or other database and includes recordable tapes and other mass storage devices.

(e) “Department” means the Department of Legal Affairs.

(f) “Governmental entity” means any department, division, bureau, commission, regional planning agency, board, district, authority, agency, or other instrumentality of this state that acquires, maintains, stores, or uses data in electronic form containing personal information.

(g)1. “Personal information” means either of the following:

a. An individual’s first name or first initial and last name in combination with any one or more of the following data elements for that individual:

(I) A social security number;

(II) A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;

(III) A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual’s financial account;

(IV) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

(V) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

b. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

2. The term does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

(h) "Third-party agent" means an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity or governmental entity.

(2) REQUIREMENTS FOR DATA SECURITY.—Each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information.

(3) NOTICE TO DEPARTMENT OF SECURITY BREACH.—

(a) A covered entity shall provide notice to the department of any breach of security affecting 500 or more individuals in this state. Such notice must be provided to the department as expeditiously as practicable, but no later than 30 days after the determination of the breach or reason to believe a breach occurred. A covered entity may receive 15 additional days to provide notice as required in subsection (4) if good cause for delay is provided in writing to the department within 30 days after determination of the breach or reason to believe a breach occurred.

(b) The written notice to the department must include:

1. A synopsis of the events surrounding the breach at the time notice is provided.
2. The number of individuals in this state who were or potentially have been affected by the breach.
3. Any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions as to how to use such services.
4. A copy of the notice required under subsection (4) or an explanation of the other actions taken pursuant to subsection (4).
5. The name, address, telephone number, and e-mail address of the employee or agent of the covered entity from whom additional information may be obtained about the breach.

(c) The covered entity must provide the following information to the department upon its request:

1. A police report, incident report, or computer forensics report.

2. A copy of the policies in place regarding breaches.

3. Steps that have been taken to rectify the breach.

(d) A covered entity may provide the department with supplemental information regarding a breach at any time.

(e) For a covered entity that is the judicial branch, the Executive Office of the Governor, the Department of Financial Services, or the Department of Agriculture and Consumer Services, in lieu of providing the written notice to the department, the covered entity may post the information described in subparagraphs (b)1.-4. on an agency-managed website.

(4) NOTICE TO INDIVIDUALS OF SECURITY BREACH.—

(a) A covered entity shall give notice to each individual in this state whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of the breach. Notice to individuals shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than 30 days after the determination of a breach or reason to believe a breach occurred unless subject to a delay authorized under paragraph (b) or waiver under paragraph (c).

(b) If a federal, state, or local law enforcement agency determines that notice to individuals required under this subsection would interfere with a criminal investigation, the notice shall be delayed upon the written request of the law enforcement agency for a specified period that the law enforcement agency determines is reasonably necessary. A law enforcement agency may, by a subsequent written request, revoke such delay as of a specified date or extend the period set forth in the original request made under this paragraph to a specified date if further delay is necessary.

(c) Notwithstanding paragraph (a), notice to the affected individuals is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed. Such a determination must be documented in writing and maintained for at least 5 years. The covered entity shall provide the written determination to the department within 30 days after the determination.

(d) The notice to an affected individual shall be by one of the following methods:

1. Written notice sent to the mailing address of the individual in the records of the covered entity; or

2. E-mail notice sent to the e-mail address of the individual in the records of the covered entity.

(e) The notice to an individual with respect to a breach of security shall include, at a minimum:

1. The date, estimated date, or estimated date range of the breach of security.

2. A description of the personal information that was accessed or reasonably believed to have been accessed as a part of the breach of security.

3. Information that the individual can use to contact the covered entity to inquire about the breach of security and the personal information that the covered entity maintained about the individual.

(f) A covered entity required to provide notice to an individual may provide substitute notice in lieu of direct notice if such direct notice is not feasible because the cost of providing notice would exceed \$250,000, because the affected individuals exceed 500,000 persons, or because the covered entity does not have an e-mail address or mailing address for the affected individuals. Such substitute notice shall include the following:

1. A conspicuous notice on the Internet website of the covered entity if the covered entity maintains a website; and

2. Notice in print and to broadcast media, including major media in urban and rural areas where the affected individuals reside.

(g) Notice provided pursuant to rules, regulations, procedures, or guidelines established by the covered entity's primary or functional federal regulator is deemed to be in compliance with the notice requirement in this subsection if the covered entity notifies affected individuals in accordance with the rules, regulations, procedures, or guidelines established by the primary or functional federal regulator in the event of a breach of security. Under this paragraph, a covered entity that timely provides a copy of such notice to the department is deemed to be in compliance with the notice requirement in subsection (3).

(5) NOTICE TO CREDIT REPORTING AGENCIES.—If a covered entity discovers circumstances requiring notice pursuant to this section of more than 1,000 individuals at a single time, the covered entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act, 15 U.S.C. s. 1681a(p), of the timing, distribution, and content of the notices.

(6) NOTICE BY THIRD-PARTY AGENTS; DUTIES OF THIRD-PARTY AGENTS; NOTICE BY AGENTS.—

(a) In the event of a breach of security of a system maintained by a third-party agent, such third-party agent shall notify the covered entity of the breach of security as expeditiously as practicable, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred. Upon receiving notice from a third-party agent, a covered entity shall provide notices required under subsections (3) and

(4). A third-party agent shall provide a covered entity with all information that the covered entity needs to comply with its notice requirements.

(b) An agent may provide notice as required under subsections (3) and (4) on behalf of the covered entity; however, an agent's failure to provide proper notice shall be deemed a violation of this section against the covered entity.

(7) ANNUAL REPORT.—By February 1 of each year, the department shall submit a report to the President of the Senate and the Speaker of the House of Representatives describing the nature of any reported breaches of security by governmental entities or third-party

agents of governmental entities in the preceding calendar year along with recommendations for security improvements. The report shall identify any governmental entity that has violated any of the applicable requirements in subsections (2)-(6) in the preceding calendar year.

(8) REQUIREMENTS FOR DISPOSAL OF CUSTOMER RECORDS.—Each covered entity or third-party agent shall take all reasonable measures to dispose, or arrange for the disposal, of customer records containing personal information within its custody or control when the records are no longer to be retained. Such disposal shall involve shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

(9) ENFORCEMENT.—

(a) A violation of this section shall be treated as an unfair or deceptive trade practice in any action brought by the department under s. [501.207](#) against a covered entity or third-party agent.

(b) In addition to the remedies provided for in paragraph (a), a covered entity that violates subsection (3) or subsection (4) shall be liable for a civil penalty not to exceed \$500,000, as follows:

1. In the amount of \$1,000 for each day up to the first 30 days following any violation of subsection (3) or subsection (4) and, thereafter, \$50,000 for each subsequent 30-day period or portion thereof for up to 180 days.

2. If the violation continues for more than 180 days, in an amount not to exceed \$500,000.

The civil penalties for failure to notify provided in this paragraph apply per breach and not per individual affected by the breach.

(c) All penalties collected pursuant to this subsection shall be deposited into the General Revenue Fund.

(10) NO PRIVATE CAUSE OF ACTION.—This section does not establish a private cause of action.

(11) PUBLIC RECORDS EXEMPTION.—

(a) All information received by the department pursuant to a notification required by this section, or received by the department pursuant to an investigation by the department or a law enforcement agency, is confidential and exempt from s. [119.07](#)(1) and s. 24(a), Art. I of the State Constitution, until such time as the investigation is completed or ceases to be active. This exemption shall be construed in conformity with s. [119.071](#)(2)(c).

(b) During an active investigation, information made confidential and exempt pursuant to paragraph (a) may be disclosed by the department:

1. In the furtherance of its official duties and responsibilities;

2. For print, publication, or broadcast if the department determines that such release would assist in notifying the public or locating or identifying a person that the department

believes to be a victim of a data breach or improper disposal of customer records, except that information made confidential and exempt by paragraph (c) may not be released pursuant to this subparagraph; or

3. To another governmental entity in the furtherance of its official duties and responsibilities.

(c) Upon completion of an investigation or once an investigation ceases to be active, the following information received by the department shall remain confidential and exempt from s. [119.07\(1\)](#) and s. 24(a), Art. I of the State Constitution:

1. All information to which another public records exemption applies.
2. Personal information.
3. A computer forensic report.
4. Information that would otherwise reveal weaknesses in a covered entity's data security.
5. Information that would disclose a covered entity's proprietary information.

(d) For purposes of this subsection, the term "proprietary information" means information that:

1. Is owned or controlled by the covered entity.
2. Is intended to be private and is treated by the covered entity as private because disclosure would harm the covered entity or its business operations.
3. Has not been disclosed except as required by law or a private agreement that provides that the information will not be released to the public.
4. Is not publicly available or otherwise readily ascertainable through proper means from another source in the same configuration as received by the department.
5. Includes:
 - a. Trade secrets as defined in s. [688.002](#).
 - b. Competitive interests, the disclosure of which would impair the competitive business of the covered entity who is the subject of the information.

(e) This subsection is subject to the Open Government Sunset Review Act in accordance with s. [119.15](#) and shall stand repealed on October 2, 2019, unless reviewed and saved from repeal through reenactment by the Legislature.



December 1, 2016

Via Email and U.S. Mail

The Honorable Adam Hamm
Chairman
Cyber Security Task Force
National Association of Insurance Commissioners
110 Walnut Street, Suite 1500
Kansas City, MO 64106-2197

Re: Proposed NAIC Insurance Data Security Model Law ("Data Security Law")

Dear Commissioner Hamm:

These comments are filed on behalf of the National Risk Retention Association ("NRRA"). NRRA is a 501(c)(6) non-profit and non-partisan trade association that is dedicated to the development, education and promotion of U.S.-domiciled alternatives to traditional liability insurance. NRRA represents risk retention groups ("RRGs") and risk purchasing groups ("RPGs") before legislative bodies, executive agencies, and the courts. There are 235 RRGs currently in operation in the United States. RRGs provide a significant portion of the commercial liability insurance in the United States. In 2015, RRGs received a little over \$3 billion in premiums.

The proposed Data Security Law would impose on any "Licensee" a substantial series of obligations, which would be difficult for any small insurer to sustain and are not generally appropriate for an RRG, which is required by federal law to only offer commercial liability insurance to its members. 15 U.S.C. § 3901(a)(2); 3901(a)(4)(G).

The definition of "Licensee" would presumably cover an RRG because it would be a "licensed insurer" in its state of domicile and because it would have (1) registered with the Commissioner of Insurance, as required by 15 U.S.C. § 3902(a)(c)(D) and (2) "filed a plan of operation or a feasibility study...." with the Commissioner, as required by 15 U.S.C. § 3902(d).

However, RRGs are exempt from all the laws of any state (except the state in which it is chartered), except those laws expressly set forth in 15 U.S.C. § 3901(a). The Data Security Law clearly would *not* fall under any of the laws referenced in 15 U.S.C. § 3901(a).

16133 Ventura Blvd., Suite 1055
Encino, CA 91436
(800) 928-5809 Ext. 102; Fax: (800) 421-5981
www.riskretention.org

The Honorable Adam Hamm
December 1, 2016
Page 2

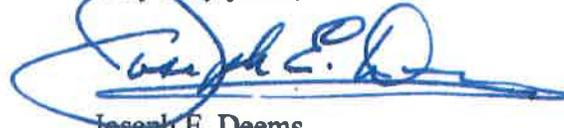
Therefore, it is the request of NRRA that the definition of "Licensee" in proposed Section 2.F be amended to expressly exclude risk retention groups not chartered in the state, as is required by federal law. Accordingly, Section 2.F should be amended to read as follows:

F. "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, except that a risk retention group as defined in 15 U.S.C. § 3901(a)(4) shall not be subject to this Act unless chartered in this State.

RPGs are groups which purchase liability insurance for their members. Unlike RRGs, the federal exemption from state law is far more limited and would not preempt the application of the proposed Data Security Law. 15 U.S.C. § 3901(a)(5); § 3903(a), (b). Nonetheless, the application of the Data Security Law would be unreasonably burdensome to RPGs.

NRRA appreciates your attention to this request. If you have any questions, please address them to the undersigned.

Very truly yours,



Joseph E. Deems
Executive Director
National Risk Retention Association



December 5, 2016

Via Email

The Honorable Adam Hamm
Chairman, Cyber Security Task Force
National Association of Insurance Commissioners
110 Walnut Street, Suite 1500
Kansas City, MO 64106-2197

Re: Proposed NAIC Insurance Data Security Model Law ("Model Law")

Dear Commissioner Hamm:

These comments regarding the proposed NAIC Insurance Data Security Model Law are filed on behalf of the Vermont Captive Insurance Association ("VCIA"). VCIA, with over 450 members, is the largest trade association for captive insurance in the world. Established in 1985, VCIA provides lobbying support on the federal and state levels for its member companies, and the association hosts and supports professional education opportunities for the industry at large.

Vermont's captive law is clear that no laws apply other than the captive law unless specifically referenced in the captive law, and we would not make this cyber law applicable to captives. Therefore, we understand that the Model Law would not pertain to captives licensed in Vermont.

However, under the Model Law the definition of "Licensee" would presumably cover a risk retention group ("RRG") because it would be a "licensed insurer" in its state of domicile and because it would have (1) registered with the Commissioner of Insurance, as required by 15 U.S.C. § 3902(a)(c)(D) and (2) "filed a plan of operation or a feasibility study" with the Commissioner, as required by 15 U.S.C. § 3902(d). VCIA strongly urges the NAIC to exempt RRGs for two reasons.

First, the Model Law would impose on any "Licensee" a substantial series of obligations, which would be difficult for any small insurer to sustain and are not appropriate for an RRG, which is required by federal law to only offer commercial liability insurance to its members. 15 U.S.C. § 3901(a)(2); 3901(a)(4)(G). The protection of policyholder data requirements would not be appropriate as policyholders of the RRG are also its owners.

The Honorable Adam Hamm
VCIA comments re: Proposed NAIC Insurance Data Security Model Law
December 5, 2016
Page 2

Second, RRGs are exempt by the federal Liability Risk Retention Act from all the laws of any state (other than the state in which it is licensed), except those laws expressly set forth in 15 U.S.C. § 3901(a). The Data Security Law clearly would not fall under any of the laws referenced in 15 U.S.C. § 3901(a).

Therefore, it is the request of VCIA that the definition of "Licensee" in proposed Section 2.F be amended to expressly exclude risk retention groups, as is required by federal law. For that reason, we suggest Section 2.F should be amended to read as follows:

F. "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, except that a risk retention group as defined in 15 U.S.C. § 3901(a)(4) shall not be subject to this Act.

VCIA appreciates your attention to this request. If you have any questions, please feel free to contact me.

Sincerely,

A handwritten signature in black ink, appearing to read "Richard Smith". The signature is written in a cursive style with a large initial "R" and "S".

Richard Smith
President