030286254

SENATE BILL NO. 878

Offered January 8, 2003

Prefiled January 7, 2003

A BILL to amend and reenact § 38.2-602 of the Code of Virginia and to amend the Code of Virginia by adding a section numbered 38.2-613.2, relating to insurance information security program; privacy protection.

Patron—Wampler

Referred to Committee on Commerce and Labor

Be it enacted by the General Assembly of Virginia:

1. That § 38.2-602 of the Code of Virginia is amended and reenacted, and that the Code of Virginia is amended by adding a section numbered 38.2-613.2, as follows:

§ 38.2-602. Definitions.

As used in this chapter:

"Adverse underwriting decision" means:

1. Any of the following actions with respect to insurance transactions involving insurance coverage that is individually underwritten:

a. A declination of insurance coverage;

b. A termination of insurance coverage;

c. Failure of an agent to apply for insurance coverage with a specific insurance institution that an agent represents and that is requested by an applicant;

d. In the case of a property or casualty insurance coverage:

(1) Placement by an insurance institution or agent of a risk with a residual market mechanism or an unlicensed insurer; or

(2) The charging of a higher rate on the basis of information that differs from that which the applicant or policyholder furnished; or

e. In the case of a life or accident and sickness insurance coverage, an offer to insure at higher than standard rates, or with limitations, exceptions or benefits other than those applied for.

2. Notwithstanding subdivision 1 of this definition, the following actions shall not be considered adverse underwriting decisions, but the insurance institution or agent responsible for their occurrence shall provide the applicant or policyholder with the specific reason or reasons for their occurrence:

a. The termination of an individual policy form on a class or statewide basis;

b. A declination of insurance coverage solely because such coverage is not available on a class or statewide basis;

c. The rescission of a policy.

"Affiliate" or "affiliated" means a person that directly, or indirectly through one or more intermediaries, controls, is controlled by, or is under common control with another person.

"Agent" shall have the meaning as set forth in § 38.2-1800 and shall include surplus lines brokers.

"Applicant" means any person who seeks to contract for insurance coverage other than a person seeking group insurance that is not individually underwritten.

"Clear and conspicuous notice" means a notice that is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

"Consumer report" means any written, oral, or other communication of information bearing on a natural person's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living that is used or expected to be used in connection with an insurance transaction.

"Consumer reporting agency" means any person who:

1. Regularly engages, in whole or in part, in the practice of assembling or preparing consumer reports for a monetary fee;

2. Obtains information primarily from sources other than insurance institutions; and

3. Furnishes consumer reports to other persons.

"Control," including the terms "controlled by" or "under common control with," means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person, whether through the ownership of voting securities, by contract other than a commercial contract for goods or nonmanagement services, or otherwise, unless the power is the result of an official position with or corporate office held by the person.

"Declination of insurance coverage" means a denial, in whole or in part, by an insurance institution

or agent of requested insurance coverage.

"Financial information" means personal information other than medical record information or records of payment for the provision of health care to an individual.

"Financial institution" means any institution the business of which is engaging in financial activities as described in Section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. § 1843 (k)).

"Financial product or service" means any product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under Section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. § 1843 (k)).

"Individual" means any natural person who:

1. In the case of property or casualty insurance, is a past, present, or proposed named insured or certificate holder;

2. In the case of life or accident and sickness insurance, is a past, present, or proposed principal insured or certificate holder;

3. Is a past, present or proposed policyowner;

4. Is a past or present applicant;

5. Is a past or present claimant;

6. Derived, derives, or is proposed to derive insurance coverage under an insurance policy or certificate subject to this chapter;

7. For the purposes of §§ 38.2-612.1 and 38.2-613, is a beneficiary of a life insurance policy;

8. For the purposes of §§ 38.2-612.1 and 38.2-613, is a mortgagor of a mortgage covered under a mortgage guaranty insurance policy; or

9. For the purposes of §§ 38.2-612.1 and 38.2-613, is an owner of property used as security for an indebtedness for which single interest insurance is required by a lender.

Notwithstanding any provision of this definition to the contrary, for purposes of § 38.2-612.1, "individual" shall not include any natural person who is covered under an employee benefit plan, group or blanket insurance contract, or group annuity contract when the insurance institution or agent that provides such plan or contract: (i) furnishes the notice required under § 38.2-604.1 to the employee benefit plan sponsor, group or blanket insurance contract holder, or group annuity contract holder; and (ii) does not disclose the financial information of the person to a nonaffiliated third party other than as permitted under § 38.2-613.

"Institutional source" means any person or governmental entity that provides information about an individual to an agent, insurance institution or insurance-support organization, other than:

1. An agent;

2. The individual who is the subject of the information; or

3. A natural person acting in a personal capacity rather than in a business or professional capacity.

"Insurance institution" means any corporation, association, partnership, reciprocal exchange, inter-insurer, Lloyd's type of organization, fraternal benefit society, or other person engaged in the business of insurance, including health maintenance organizations, and health, legal, dental, and optometric service plans. "Insurance institution" shall not include agents or insurance-support organizations.

"Insurance-support organization" means any person who regularly engages, in whole or in part, in the practice of assembling or collecting information about natural persons for the primary purpose of providing the information to an insurance institution or agent for insurance transactions, including (i) the furnishing of consumer reports or investigative consumer reports to an insurance institution or agent for use in connection with an insurance transaction or (ii) the collection of personal information from insurance institutions, agents or other insurance-support organizations for the purpose of detecting or preventing fraud, material misrepresentation or material nondisclosure in connection with insurance underwriting or insurance claim activity. However, the following persons shall not be considered "insurance-support organizations" for purposes of this chapter: agents, governmental institutions, insurance institutions, medical-care institutions and medical professionals.

"Insurance transaction" means any transaction involving insurance primarily for personal, family, or household needs rather than business or professional needs that entails:

1. The determination of an individual's eligibility for an insurance coverage, benefit or payment; or

2. The servicing of an insurance application, policy, contract, or certificate.

"Investigative consumer report" means a consumer report or a portion thereof in which information about a natural person's character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with the person's neighbors, friends, associates, acquaintances, or others who may have knowledge concerning such items of information.

"Joint marketing agreement" means a formal written contract pursuant to which an insurance institution jointly offers, endorses, or sponsors a financial product or service with another financial institution.

"Life insurance" includes annuities.

"Medical-care institution" means any facility or institution that is licensed to provide health care services to natural persons, including but not limited to, hospitals, skilled nursing facilities, home-health agencies, medical clinics, rehabilitation agencies, and public-health agencies or health-maintenance organizations.

"Medical professional" means any person licensed or certified to provide health care services to natural persons, including but not limited to, a physician, dentist, nurse, chiropractor, optometrist, physical or occupational therapist, psychiatric social worker, clinical dietitian, clinical psychologist, pharmacist, or speech therapist.

"Medical-record information" means personal information that:

1. Relates to an individual's physical or mental condition, medical history, or medical treatment; and

2. Is obtained from a medical professional or medical-care institution, from the individual, or from the individual's spouse, parent, or legal guardian.

"Nonaffiliated third party" means any person who is not an affiliate of an insurance institution but does not mean (i) an agent who is selling or servicing a product on behalf of the insurance institution or (ii) a person who is employed jointly by the insurance institution and the company that is not an affiliate.

"Personal information" means any individually identifiable information gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics. "Personal information" includes an individual's name and address and medical-record information, but does not include (i) privileged information or (ii) any information that is publicly available.

"Policyholder" means any person who:

1. In the case of individual property or casualty insurance, is a present named insured;

2. In the case of individual life or accident and sickness insurance, is a present policyowner; or

3. In the case of group insurance that is individually underwritten, is a present group certificate holder.

"Policyholder information" means personal information about a policyholder, whether in paper, electronic, or other form, that is maintained by or on behalf of an insurance institution, agent, or insurance-support organization.

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

"Pretext interview" means an interview whereby a person, in an attempt to obtain information about a natural person, performs one or more of the following acts:

1. Pretends to be someone he or she is not;

2. Pretends to represent a person he or she is not in fact representing;

3. Misrepresents the true purpose of the interview; or

4. Refuses to identify himself or herself upon request.

"Privileged information" means any individually identifiable information that (i) relates to a claim for insurance benefits or a civil or criminal proceeding involving an individual, and (ii) is collected in connection with or in reasonable anticipation of a claim for insurance benefits or civil or criminal proceeding involving an individual.

"Residual market mechanism" means an association, organization, or other entity defined, described, or provided for in the Virginia Automobile Insurance Plan as set forth in § 38.2-2015, or in the Virginia Property Insurance Association as set forth in Chapter 27 (§ 38.2-2700 et seq.) of this title.

"Service provider" means a person that maintains, processes or otherwise is permitted access to policyholder information through its provision of services directly to the insurance institution, agent, or insurance-support organization.

"Termination of insurance coverage" or "termination of an insurance policy" means either a cancellation or nonrenewal of an insurance policy other than by the policyholder's request, in whole or in part, for any reason other than the failure to pay a premium as required by the policy.

"Unlicensed insurer" means an insurance institution that has not been granted a license by the Commission to transact the business of insurance in Virginia.

§ 38.2-613.2. Information security program.

A. Each insurance institution, agent, and insurance-support organization shall implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of policyholder information. The administrative, technical, and physical safeguards included in the information security program shall be appropriate to the size and complexity of the insurance institution, agent, or insurance-support organization and the nature and scope of its activities.

B. The information security program shall be designed to:

1. Ensure the security and confidentiality of policyholder information;

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

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

C. Each insurance institution, agent, and insurance-support organization shall:

1. Identify reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration or destruction of policyholder information or policyholder information systems;

2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of policyholder information; and

3. Assess the sufficiency of policies, procedures, policyholder information systems and other safeguards in place to control risks.

D. Each insurance institution, agent, and insurance-support organization shall:

1. Design its information security program to control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of its activities;

2. Train staff, as appropriate, to implement the information security program; and

3. Regularly test or otherwise regularly monitor the key controls, systems and procedures of the information security program. The frequency and nature of these tests or other monitoring practices shall be determined by the insurance institution, agent, or insurance-support organization.

E. Each insurance institution, agent, and insurance-support organization shall:

1. Exercise appropriate due diligence in selecting its service providers; and

2. Require its service providers to implement appropriate measures designed to meet the objectives of this section, and, where necessary, as determined by the insurance institution, agent, or insurance-support organization, take appropriate steps to confirm that its service providers have satisfied these obligations.

F. Each insurance institution, agent, and insurance-support organization shall monitor, evaluate and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its policyholder information, internal or external threats to information, and its own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to policyholder information systems.