INSURANCE DEPARTMENT OF THE STATE OF NEW YORK

(11 NYCRR 420)

REGULATION 169

PRIVACY OF CONSUMER FINANCIAL AND HEALTH INFORMATION

I, GREGORY V. SERIO, Superintendent of Insurance of the State of New York, pursuant to the authority granted by Sections 201, 301, 1505, 1608, 1712, and 3217, and Article 24 of the Insurance Law, and in accordance with the provisions of 12 U.S.C. 1831x, 15 U.S.C. 6801(b), 6802, 6803, 6805(b), 6805(c) and 6807 and 15 U.S.C. Chapter 94, do hereby promulgate a new Part 420 of Title 11 of the Official Compilation of Codes, Rules and Regulations of the State of New York (Regulation No. 169). A new Chapter XIX, entitled "Privacy of Consumer Financial and Health Information", is added, and Part 420 is added as a part thereof, all the above to take effect on November 21, 2001, after publication in the State Register. Part 420 shall read as follows:

(ALL MATERIAL IS NEW)

TABLE OF CONTENTS

EXCEPTIONS TO LIMITS ON DISCLOSURE OF FINANCIAL INFORMATION

RULES FOR HEALTH INFORMATION

ADDITIONAL PROVISIONS

APPENDIX A – SAMPLE CLAUSES

GENERAL PROVISIONS

Section 420.0 Preamble.

(a) Title V of the Gramm-Leach-Bliley Act ("GLBA") (15 U.S.C. 6801, et. seq.) requires financial institutions, including insurers, to protect the privacy of consumers and customers. Title V of GLBA requires that state insurance authorities establish appropriate consumer privacy standards for insurance providers.

(b) Section 505 (c) (15 U.S.C. §6805(c)) of GLBA provides: "If a State insurance authority fails to adopt regulations to carry out this subtitle, such State shall not be eligible to override, pursuant to section 47(g)(2)(B)(iii) of the Federal Deposit Insurance Act (12 U.S.C. 1831x), the insurance customer protections prescribed by a Federal banking agency under section 45(a) of such Act."

(c) Sections 502 and 503 of GLBA (15 U.S.C. §§ 6802 and 6803) list specific protections that regulators shall implement. These include requirements that financial institutions maintain a

privacy policy that is clearly communicated to consumers and customers, that no nonpublic personal financial information be disclosed to nonaffiliated third parties unless a consumer has been given a chance to "opt out" of having his or her information disclosed, and that no specific account information be given to direct marketing firms. The Act also provides numerous exceptions to specific consumer protections.

(d) This Part provides that a licensee subject to the supervision of the Superintendent of Insurance who, in the conduct of the business of insurance in this State, violates the provisions of this Part shall be deemed to have engaged in an unfair method of competition or an unfair or deceptive act and practice in the conduct of the business of insurance in this State. Such act shall be deemed to be a trade practice constituting a determined violation, as defined in section 2402(c) of the Insurance Law, in violation of section 2403 of such law.

(e) In addition to the foregoing, the Superintendent of Insurance possesses the authority pursuant to sections 201 and 301 of the Insurance Law to promulgate a regulation to delineate the responsibility of an Insurance Department licensee regarding the privacy of consumer and customer financial and health information which the licensee receives. Such authority is an exercise of the superintendent's power to promulgate regulations to effectuate any power given to the superintendent under the Insurance Law, including the provisions regarding transactions within a holding company system affecting controlled insurers (section 1505); relations and transactions between parent and subsidiary companies for life and property/casualty insurers (sections 1608 and 1712); minimum standards in the form, content, and sale of accident and health insurance policies and contracts (section 3217); and, as noted above, unfair methods of competition or unfair or deceptive acts and practices (Article 24).

Section 420.1 Purpose and scope.

(a) Purpose. This Part governs the treatment of nonpublic personal information about individuals (defined in this Part as consumers or customers) in this State by all licensees of the Insurance Department. This Part:

(1) Requires a licensee to provide notice to individuals about its privacy policies and practices;

(2) Describes the conditions under which a licensee may disclose nonpublic personal health information and nonpublic personal financial information about individuals to nonaffiliated third parties;

(3) Provides methods for individuals to prevent a licensee from disclosing that information; and

(4) Provides a method for individuals to prevent a licensee from disclosing nonpublic personal health information by not affirmatively consenting to such disclosure, subject to the exceptions in section 420.17(b) of this Part.

(b) Scope. This Part applies to:

(1) Nonpublic personal financial information about individuals who obtain, seek to obtain or are claimants or beneficiaries of products or services primarily for personal, family or household purposes from licensees. This Part does not apply to information about companies or about individuals who obtain products or services for business, commercial, or agricultural purposes.

(2) All nonpublic personal health information.

Section 420.2 Rule of construction.

The examples in this Part and the sample clauses in Appendix A of this Part are not exclusive. Compliance with an example or use of a sample clause, to the extent applicable, constitutes compliance with this Part.

Section 420.3 Definitions.

As used in this Part, unless the context requires otherwise:

(a) "Affiliate" means any company that controls, is controlled by, or is under common control with another company.

(b)(1) "Clear and conspicuous" means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

(2) Examples:

(i) Reasonably understandable. A licensee makes its notice reasonably understandable if it:

(*a*) Presents the information contained in the notice in clear, concise sentences, paragraphs and sections;

(*b*) Uses short explanatory sentences or bullet lists whenever possible;

(*c*) Uses definite, concrete, everyday words and active voice whenever possible;

(*d*) Avoids multiple negatives;

(*e*) Avoids legal and highly technical business terminology whenever possible; and

(*f*) Avoids explanations that are imprecise and readily subject to different interpretations.

(ii) Designed to call attention. A licensee designs its notice to call attention to the nature and significance of the information in it if the licensee:

(*a*) Uses a plain-language heading to call attention to the notice;

(*b*) Uses a typeface and type size that are easy to read;

(*c*) Provides wide margins and ample line spacing;

(*d*) Uses boldface or italics for key words; and

(*e*) In a form that combines the licensee's notice with other information, uses distinctive type size, style, and graphic devices, such as shading or sidebars.

(iii) Notices on web sites. If a licensee provides a notice on a web page, the licensee designs its notice to call attention to the nature and significance of the information in it if the licensee uses text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice, and the licensee either:

(*a*) Places the notice on a web page that consumers frequently access, such as a homepage or a page on which transactions are conducted; or

(*b*) Places a link on a web page that consumers frequently access, such as a homepage or a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature, and relevance of the notice.

(c) "Collect" means to obtain information that the licensee organizes or can retrieve by the name of an individual or by identifying number, symbol or other identifying particular assigned to the individual, irrespective of the source of the underlying information.

(d)"Company" means a corporation, limited liability company, business trust, general or limited partnership, association, sole proprietorship or similar organization.

(e)(1) "Consumer" means an individual who, in this State, seeks to obtain, obtains or has obtained an insurance product or service, directly or through a legal representative, from a licensee that is to be used primarily for personal, family, or household purposes, and about whom the licensee has nonpublic personal information.

(2) Examples:

(i) An individual who provides nonpublic personal information to a licensee in connection with seeking to obtain or obtaining financial, investment or economic

advisory services in this State relating to an insurance product or service is a consumer regardless of whether the licensee establishes an ongoing advisory relationship.

(ii) An applicant for insurance prior to the inception of insurance coverage is a licensee's consumer.

(iii) An individual who is a consumer of another financial institution is not a licensee's consumer solely because the licensee is acting as agent for, or provides processing or other services to, that financial institution.

(iv) An individual is a licensee's consumer if:

(*a*)(I) the individual is a beneficiary of a life insurance policy underwritten by the licensee;

(II) the individual is a claimant under an insurance policy issued by the licensee;

(III) the individual is an insured or an annuitant under an insurance policy or annuity, respectively, issued by the licensee; or

(IV) the individual is a mortgagor of a mortgage covered under a mortgage insurance policy issued by the licensee and

(*b*)The licensee discloses nonpublic personal financial information about the individual to a nonaffiliated third party other than as permitted under sections 420.13, 420.14, or 420.15 of this Part.

(v) Provided that the licensee provides the initial, annual and revised notices under sections 420.4, 420.5 and 420.8 of this Part to the plan sponsor, workers' compensation plan participant, group or blanket insurance policyholder or group annuity contractholder, and further provided that the licensee does not disclose to a nonaffiliated third party nonpublic personal financial information about such an individual other than as permitted under sections 420.13, 420.14 or 420.15 of this Part, an individual is not the licensee's consumer solely because he or she is:

(*a)* a participant or a beneficiary of an employee benefit plan that the licensee administers or sponsors or for which the licensee acts as a trustee, insurer or fiduciary;

(*b)* covered under a group or blanket insurance or group annuity contract issued by the licensee; or

(c) a beneficiary in a workers' compensation plan.

(vi)(*a*) The individuals described in clauses (*a)*, (*b*) and (*c*) of subparagraph (v) of this paragraph are consumers of a licensee if the licensee does not meet all the conditions of subparagraph (v).

(*b*) In no event shall the individuals, solely by virtue of the status described in clauses (a), (b) or (c) of subparagraph (v) of this paragraph, be deemed to be customers for purposes of this Part.

(vii) An individual is not a licensee's consumer solely because he or she is a beneficiary of a trust for which the licensee is a trustee.

(viii) An individual is not a licensee's consumer solely because he or she has designated the licensee as trustee for a trust.

(f) "Consumer reporting agency" has the same meaning as in Section 603(f) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(f)) and Section 380-a(e) of the New York Fair Credit Reporting Act (N.Y. Gen. Bus. Law Article 25).

(g) "Control" means:

(1) Ownership, control or power to vote 25% or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;

(2) Control in any manner over the election of a majority of the directors, trustees or general partners (or individuals exercising similar functions) of the company; or

(3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company, as the superintendent determines.

(h) "Customer" means a consumer who has a customer relationship with a licensee.

(i)(1) "Customer relationship" means a continuing relationship between a consumer and a licensee under which the licensee provides one or more insurance products or services in this State to the consumer that are to be used primarily for personal, family, or household purposes.

(2) Examples:

(i) Continuing relationship. A consumer has a continuing relationship with a licensee if:

(*a*) The consumer is a current policyholder of an insurance product issued by or through the licensee; or

(*b*) The consumer obtains financial, investment or economic advisory services relating to an insurance product or service from the licensee for a fee;

(ii) No continuing relationship. A consumer does not have a continuing relationship with a licensee if:

(*a*) The consumer applies for insurance but does not purchase the insurance;

(*b*) The licensee sells the consumer airline travel insurance in an isolated transaction;

(*c*) The individual is no longer a current policyholder of an insurance product or no longer obtains insurance services with or through the licensee;

(*d*) The consumer is a beneficiary or claimant under a policy;

(*e*) The customer's policy is lapsed, expired, or otherwise inactive or dormant under the licensee's business practices, and the licensee has not communicated with the customer about the relationship for a period of 12 consecutive months, other than annual privacy notices, material required by law or regulation, communication at the direction of a state or federal authority, or promotional materials; or

(*f*) The individual is an insured or an annuitant under an insurance policy or annuity, respectively, but is not the policyholder or owner of the insurance policy or annuity.

(j)(1) "Financial institution" means any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in Section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial institution does not include:

(i) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 *et seq.);*

(ii) The Federal Agricultural Mortgage Corporation or any entity charged and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 *et seq.);* or

(iii) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar

transactions related to a transaction of a consumer, as long as the institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party.

(k)(1) "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)).

(2) Financial service includes a financial institution's evaluation or brokerage of information that the financial institution collects in connection with a request or an application from a consumer for a financial product or service.

(l) "Health care" means:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, services, procedures, tests or counseling that:

(i) Relates to the physical, mental or behavioral condition of an individual; or

(ii) Affects the structure or function of the human body or any part of the human body, including the banking of blood, sperm, organs, or any other tissue; or

(2) Prescribing, dispensing, or furnishing to an individual drugs or biologicals, or medical devices or health care equipment and supplies.

(m) "Health care provider" means a physician or other health care practitioner licensed, accredited or certified to perform specified health services consistent with state law, or a health care facility.

(n) "Health information" means any information or data except age or gender, whether oral or recorded in any form or medium, created by or derived from a health care provider or the consumer that relates to:

(1) The past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family;

(2) The provision of health care to any individual; or

(3) Payment for the provision of health care to any individual.

(o)(1) "Insurance product or service" means any product or service that is offered by a licensee pursuant to the insurance laws of this state.

(2) Insurance service includes a licensee's evaluation, brokerage or distribution of information that the licensee collects in connection with a request or an application from a consumer for an insurance product or service.

(p)(1) "Licensee" means a person 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; a health maintenance organization holding, or required to hold, a certificate of authority pursuant to Article 44 of the Public Health Law; or an unauthorized insurer in regard to the excess line business conducted pursuant to section 2118 of the Insurance Law and Part 27 of this Title (Regulation 41); but shall not include a registered service contract provider, charitable annuity society, or a licensed viatical settlement company or viatical settlement broker.

(2)(i) A licensee is not subject to the notice and opt out requirements for nonpublic personal financial information set forth in sections 420.4 through 420.9 of this Part if the licensee is an employee, agent, sublicensee, or other representative of another licensee ("the principal") and:

(*a*) The principal otherwise complies with, and provides the notices required by, the provisions of this Part; and

(*b*) The licensee does not disclose any nonpublic personal information of a consumer or customer to any person other than the principal from or through which such consumer or customer seeks to obtain or has obtained a product or service, or its affiliates in a manner permitted by this Part.

(ii) Examples of employee, agent or other representative of a principal:

(*a*) An insurance broker, public adjuster or other licensee who is employed by another insurance broker, public adjuster or other licensee;

(*b*) An independent adjuster adjusting a claim or benefit on behalf of an insurer;

(*c*) An insurance agent of an insurer;

(*d*) An insurance broker that has binding authority for an insurer; or

(*e*) A sublicensee of a licensee, whether or not the sublicensee is licensed in any other capacity.

(3) An excess line broker or unauthorized insurer shall be deemed to be in compliance with the notice and opt out requirements for nonpublic personal financial information set forth in sections 420.4 through 420.9 of this Part provided:

(*a*) The broker or insurer does not disclose nonpublic personal information of a consumer or a customer to nonaffiliated third parties for any purpose, including joint servicing or marketing under section 420.13 of this Part, except as permitted by sections 420.14 and 420.15 of this Part; and

(*b*) The broker or insurer delivers a notice to the consumer at the time a customer relationship is established on which the following clear and conspicuous notice is set forth:

PRIVACY NOTICE

"NEITHER THE U.S. BROKER(S) THAT HANDLED THIS INSURANCE NOR THE INSURER(S) THAT HAS (HAVE) UNDERWRITTEN THIS INSURANCE WILL DISCLOSE NONPUBLIC PERSONAL INFORMATION CONCERNING THE BUYER TO NONAFFILIATES OF THE BROKER(S) OR THE INSURER(S) EXCEPT AS PERMITTED BY LAW."

(q)(1) "Nonaffiliated third party" means any person except:

(i) A licensee's affiliate; or

(ii) A person employed jointly by a licensee and any company that is not the licensee's affiliate (but nonaffiliated third party includes the other company that jointly employs the person).

(2) Nonaffiliated third party includes any company that is an affiliate solely by virtue of the licensee's or its affiliate's direct or indirect ownership or control of the company in conducting:

(i) merchant banking or investment banking activities of the type described in Section 4(k)(4)(H) of the federal Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)(4)(H)); or

(ii) insurance company investment activities of the type described in Section 4(k)(4)(I) of the federal Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)(4)(I)).

(r) "Nonpublic personal information" means nonpublic personal financial information and nonpublic personal health information.

(s)(1) "Nonpublic personal financial information" means:

(i) Personally identifiable financial information; and

(ii) Any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information other than publicly available information.

(2) Nonpublic personal financial information does not include:

(i) Health information;

(ii) Publicly available information, except as included on a list described in subparagraph (ii) of paragraph (1) of this subdivision; or

(iii) Any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information other than publicly available information.

(3) Examples of lists.

(i) Nonpublic personal financial information includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information other than publicly available information, such as account numbers.

(ii) Nonpublic personal financial information does not include any list of individuals' names and addresses that contains only publicly available information, is not derived in whole or in part using personally identifiable financial information other than publicly available information, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.

(t) "Nonpublic personal health information" means health information:

(1) That identifies an individual who is the subject of the information; or

(2) With respect to which there is a reasonable basis to believe that the information could be used to identify an individual.

(u)(1) "Personally identifiable financial information" means any information:

(i) A consumer provides to a licensee to obtain an insurance product or service from the licensee;

(ii) About a consumer resulting from a transaction involving an insurance product or service between a licensee and a consumer; or

(iii) A licensee otherwise obtains about a consumer in connection with providing an insurance product or service to that consumer.

(2) Examples:

(i) Information included. Personally identifiable financial information includes:

(*a*) Information a consumer provides to a licensee on an application to obtain an insurance product or service;

(*b*) Account balance information and payment history;

(*c*) 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;

(*d*) Any information about a licensee's consumer if it is disclosed in a manner that indicates that the individual is or has been the licensee's consumer;

(*e*) Any information that a consumer provides to the licensee or that the licensee or its agent otherwise obtains in connection with collecting on a policy loan or servicing a policy loan;

(*f*) Any information the licensee collects through an Internet "cookie" (an information collecting device from a web server) to the extent that such information constitutes personally identifiable information; and

(*g*) Information from a consumer report.

(ii) Information not included. Personally identifiable financial information does not include:

(*a*) Health information;

(*b*) A list of names and addresses of customers of an entity that is not a financial institution; and

(c) 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.

(v)(1) "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from:

(i) Federal, state, or local government records;

(ii) Widely distributed media; or

(iii) Disclosures to the general public that are required to be made by Federal, state or local law.

(2) Reasonable basis. A licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine:

(i) That the information is of the type that is available to the general public; and

(ii) Whether an individual can direct that the information not be made available to the general public and, if so, that the licensee's consumer has not done so.

(3) Examples:

(i) Government records. Publicly available information in government records includes information in Department of Motor Vehicles records that are made available to the public (even if such access requires the payment of a fee), government real estate records and security interest filings.

(ii) Widely distributed media. Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper or a web site that is available to the general public on an unrestricted basis. A web site is not restricted merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.

(iii) Reasonable basis.

(*a*) A licensee has a reasonable basis to believe that motor vehicle or mortgage information is lawfully made available to the general public if the licensee has determined that the information is of the type made available to the public as part of the public record.

(*b*) The licensee has a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if the licensee has located the telephone number in the telephone book or the consumer has informed the licensee that the telephone number is not unlisted.

PRIVACY AND OPT OUT NOTICES FOR FINANCIAL INFORMATION

Section 420.4 Initial privacy notice to consumers required.

(a) Initial notice requirement. A licensee shall provide a clear and conspicuous notice that accurately reflects the licensee's privacy policies and practices to:

(1) Customer. An individual who becomes a licensee's customer, not later than when the licensee establishes a customer relationship, except as provided in subdivision (e) of this section; and

(2) Consumer. A consumer, before a licensee discloses any nonpublic personal financial information about the consumer to any nonaffiliated third party, if a licensee makes such a disclosure other than as authorized by sections 420.14 and 420.15 of this Part.

(b) When initial notice to a consumer is not required. A licensee is not required to provide an initial notice to a consumer under subdivision (a)(2) of this section if:

(1) The licensee does not disclose any nonpublic personal financial information about the consumer to any nonaffiliated third party, other than as authorized by sections 420.14 and 420.15 of this Part and the licensee does not have a customer relationship with the consumer; or

(2) A notice has been provided by an affiliated licensee, as long as the notice clearly identifies all licensees to whom the notice applies and is accurate with respect to the licensee and the other institutions.

(c) When a licensee establishes a customer relationship.

(1) General rule. A licensee establishes a customer relationship at the time the licensee and the consumer enter into a continuing relationship.

(2) Examples of establishing customer relationship. A licensee establishes a customer relationship when the consumer:

(i) Becomes a policyholder of a licensee that is an insurer. This occurs when the insurer delivers an insurance policy or contract to the customer;

(ii) In the case of a licensee that is an insurance agent or insurance broker, obtains insurance through that licensee; or

(iii) Agrees to obtain financial, economic or investment advisory services relating to insurance products or services for a fee from the licensee.

(d) Existing customers. When an existing customer obtains a new insurance product or service from a licensee that is to be used primarily for personal, family, or household purposes, the licensee satisfies the initial notice requirements of subdivision (a) of this section as follows:

(1) The licensee shall provide a revised policy notice, under section 420.8 of this Part, that covers the customer's new insurance product or service and that clearly states whether any existing opt-out direction applies to the new product or service; or

(2) If the initial, revised, or annual notice that the licensee most recently provided to that customer was accurate with respect to the new insurance product or service, a licensee does not need to provide a new privacy notice under subdivision (a) of this section.

(e) Exceptions to allow subsequent delivery of notice.

(1) A licensee may provide the initial notice required by subdivision (a)(1) of this section within a reasonable time after the licensee establishes a customer relationship if:

(i) Establishing the customer relationship is not at the customer's election; or

(ii) Providing notice not later than when the licensee establishes the customer relationship would substantially delay the customer's transaction and the customer agrees to receive the notice at a later time.

(2) Examples of exceptions.

(i) Not at customer's election. Establishing a customer relationship is not at the customer's election if a licensee acquires or is assigned a customer's policy from another institution or residual market mechanism and the customer does not have a choice about the licensee's acquisition or assignment.

(ii) Substantial delay of customer's transaction. Providing notice not later than when a licensee establishes a customer relationship would substantially delay the customer's transaction when the licensee and the individual agree over the telephone to enter into a customer relationship involving prompt delivery of the insurance product or service.

(iii) No substantial delay of customer's transaction. Providing notice not later than when a licensee establishes a customer relationship would not substantially delay the customer's transaction when the relationship is initiated in person at the licensee's office or through other means by which the customer may view the notice, such as on a web site.

(f) Delivery. When a licensee is required to deliver an initial privacy notice by this section, the licensee shall deliver it according to section 420.9 of this Part. If the licensee uses a short-form initial notice for non-customers according to section 420.6(c) of this Part, the licensee may deliver its privacy notice according to section 420.6(c)(3) of this Part.

Section 420.5 Annual privacy notice to customers required.

(a)(1) General rule. A licensee shall provide a clear and conspicuous notice to customers that accurately reflects its privacy policies and practices not less than annually during the continuation of the customer relationship. Annually means at least once in any period of 12 consecutive months during which that relationship exists. A licensee may define the 12-consecutive-month period, but the licensee must apply it to the customer on a consistent basis.

(2) Example. A licensee provides a notice annually if it defines the 12-consecutive-month period as a calendar year and provides the annual notice to the customer once in each calendar year following the calendar year in which the licensee provided the initial notice. For example, if a customer buys an insurance policy on any day of year 1, the licensee shall provide an annual notice to that customer by December 31 of year 2, but thereafter, shall provide each subsequent annual notice within 12 calendar months of the prior annual notice.

(b)(1) Termination of customer relationship. A licensee is not required to provide an annual notice to a former customer. A former customer is an individual with whom a licensee no longer has a continuing relationship.

(2) Examples.

(i) A licensee no longer has a continuing relationship with an individual if the individual no longer is a current policyholder of an insurance product or no longer obtains insurance services with or through the licensee.

(ii) A licensee no longer has a continuing relationship with an individual if the individual's policy is lapsed, expired or otherwise inactive or dormant under the licensee's business practices, and the licensee has not communicated with the customer about the relationship for a period of 12 consecutive months, other than to provide annual privacy notices, material required by law or regulation, or promotional materials.

(iii) For the purposes of this Part, a licensee no longer has a continuing relationship with an individual if the individual's last known address according to the licensee's records is deemed invalid. An address of record is deemed invalid if mail sent to that address by the licensee has been returned by the postal authorities as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.

(iv) A licensee no longer has a continuing relationship with a customer in the case of providing real estate settlement services, at the time the customer completes execution of all documents related to the real estate closing, payment for those services has been received, or the licensee has completed all of its responsibilities with respect to the settlement, including filing documents on the public record, whichever is later.

(c) Delivery. When the licensee is required by this section to deliver an annual privacy notice, the licensee shall deliver it according to section 420.9 of this Part.

Section 420.6 Information to be included in privacy notices.

(a) General rule. The initial, annual, and revised privacy notices that a licensee provides under sections 420.4, 420.5 and 420.8 of this Part shall include each of the following items of information that applies to the licensee and to the consumers to whom the licensee sends its privacy notice, in addition to any other information the licensee wishes to provide:

(1) The categories of nonpublic personal financial information that the licensee collects;

(2) The categories of nonpublic personal financial information that the licensee discloses;

(3) The categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal financial information, other than those parties to whom the licensee discloses information under sections 420.14 or 420.15 of this Part;

(4) The categories of nonpublic personal financial information about the licensee's former customers that the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal financial information about the licensee’s former customers, other than those parties to whom the licensee discloses information under sections 420.14 or 420.15 of this Part;

(5) If a licensee discloses nonpublic personal financial information to a nonaffiliated third party under section 420.13 of this Part (and no other exception in sections 420.14 or 420.15 of this Part applies to that disclosure), a separate description of the categories of information the licensee discloses and the categories of third parties with whom the licensee has contracted;

(6) An explanation of the consumer’s right under section 420.10(a) of this Part to opt out of the disclosure of nonpublic personal financial information to nonaffiliated third parties, including the methods by which the consumer may exercise that right at that time;

(7) Any disclosures that the licensee makes under section 603(d)(2)(A)(iii) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii))(that is, notices regarding the ability to opt out of disclosures of information among affiliates);

(8) The licensee's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; and

(9) Any disclosure that the licensee makes under subdivision (b) of this section.

(b) Description of parties subject to exceptions. If a licensee discloses nonpublic personal financial information as authorized under sections 420.14 or 420.15 of this Part, the licensee is not required to list those exceptions in the initial or annual privacy notices required by sections

420.4 and 420.5 of this Part. When describing the categories of parties to whom disclosure is made, the licensee is required to state only that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.

(c) Examples:

(1) Categories of nonpublic personal financial information that the licensee collects. A licensee satisfies the requirement to categorize the nonpublic personal financial information that it collects if the licensee categorizes it according to the source of the information, as applicable:

(i) Information from the consumer;

(ii) Information about the consumer's transactions with the licensee or its affiliates;

(iii) Information about the consumer's transactions with nonaffiliated third parties; and

(iv) Information from a consumer reporting agency.

(2) Categories of nonpublic personal financial information a licensee discloses.

(i) A licensee satisfies the requirement to categorize nonpublic personal financial information it discloses if the licensee categorizes the information according to source, as described in paragraph (1) of this subdivision, as applicable, and provides a few examples to illustrate the types of information in each category. These might include:

(a) Information from the consumer, including application information, such as assets and income and identifying information, such as name, address and social security number;

(*b*) Transaction information, such as information about balances, payment history and parties to the transaction; and

(c) Information from consumer reports, such as a consumer's creditworthiness and credit history.

(ii) A licensee does not adequately categorize the information that it discloses if the licensee uses only general terms, such as transaction information about the consumer.

(iii) If a licensee reserves the right to disclose all of the nonpublic financial information about consumers that it collects, the licensee may simply state that

fact without describing the categories or examples of nonpublic personal financial information that the licensee discloses.

(3) Categories of affiliates and nonaffiliated third parties to whom the licensee discloses.

(i) A licensee satisfies the requirement to categorize the affiliates and nonaffiliated third parties to which the licensee discloses nonpublic personal financial information about consumers if the licensee identifies the types of businesses in which they engage.

(ii) Types of businesses may be described by general terms only if the licensee uses a few illustrative examples of significant lines of business. For example, a licensee may use the term financial products or services if it includes appropriate examples of significant lines of businesses, such as life insurer, automobile insurer, consumer banking or securities brokerage.

(iii) A licensee also may categorize the affiliates and nonaffiliated third parties to which it discloses nonpublic personal financial information about consumers using more detailed categories.

(4) Disclosures under exception for service providers and joint marketers. If a licensee discloses nonpublic personal financial information under the exception in section 420.13 of this Part to a nonaffiliated third party in order to market products or services that the licensee offers alone or jointly with another financial institution, the licensee satisfies the disclosure requirement of subdivision (a)(5) of this section if it:

(i) Lists the categories of nonpublic personal financial information the licensee discloses, using the same categories and examples the licensee used to meet the requirements of subdivision (a)(2) of this section, as applicable; and

(ii) States whether the third party is:

(*a*) A service provider that performs marketing services on the licensee's behalf or on behalf of the licensee and another financial institution; or

(*b*) A financial institution with whom the licensee has a joint marketing agreement.

(5) Simplified notices. If a licensee does not disclose, and does not wish to reserve the right to disclose, nonpublic personal financial information about customers or former customers to affiliates or nonaffiliated third parties except as authorized under sections 420.14 and 420.15 of this Part, the licensee may simply state that fact, in addition to the information the licensee shall provide under subdivisions (a)(1), (a)(8), (a)(9), and subdivision (b) of this section.

(6) Confidentiality and security. A licensee describes its policies and practices with respect to protecting the confidentiality and security of nonpublic personal financial information if the licensee does both of the following:

(i) Describes in general terms who is authorized to have access to the information; and

(ii) States whether the licensee has security practices and procedures in place to ensure the confidentiality of the information in accordance with the licensee's policy. The licensee is not required to describe technical information about the safeguards it uses.

(d) Short-form initial notice with opt out notice for non-customers.

(1) The licensee may satisfy the initial notice requirements in sections 420.4(a)(2), 420.7(b) and 420.7(c) of this Part for a consumer who is not a customer by providing a short form initial notice at the same time as the licensee delivers an opt out notice as required in section 420.7 of this Part.

(2) A short form initial notice shall:

(i) Be clear and conspicuous;

(ii) State that a licensee's privacy notice is available upon request; and

(iii) Explain a reasonable means by which the consumer may obtain that notice.

(3) The licensee shall deliver its short form notice according to section 420.9 of this Part. A licensee is not required to deliver its privacy notice with its short-form initial notice. A licensee may instead simply provide the consumer with a reasonable means to obtain the licensee's privacy notice. If a consumer who receives the licensee's short-form notice requests the licensee's privacy notice, the licensee shall deliver its privacy notice according to section 420.9 of this Part.

(4) Examples of obtaining privacy notice. The licensee provides a reasonable means by which a consumer may obtain a copy of its privacy notice if the licensee:

(i) Provides a toll-free telephone number the consumer may call to request the notice; or

(ii) For a consumer who conducts business in person at the licensee's office, maintains copies of the notice on hand that the licensee provides to the consumer immediately upon request.

(e) Future disclosures. The licensee's notice may include:

(1) Categories of nonpublic personal financial information that the licensee reserves the right to disclose in the future, but does not currently disclose; and

(2) Categories of affiliates or nonaffiliated third parties to whom the licensee reserves the right in the future to disclose, but to whom it does not currently disclose, nonpublic personal financial information.

(f) Sample clauses. Sample clauses illustrating some of the notice content required by this section are included in Appendix A of this Part.

Section 420.7 Form of opt out notice to consumers and opt out methods.

(a)(1) Form of opt out notice. If a licensee is required to provide an opt out notice under section 420.10(a) of this Part, the licensee shall provide a clear and conspicuous notice to each of its consumers that accurately explains the right to opt out under that section. The notice shall state:

(i) That the licensee discloses or reserves the right to disclose nonpublic personal financial information about its consumer to a nonaffiliated third party;

(ii) That the consumer has the right to opt out of that disclosure; and

(iii) A reasonable means by which the consumer may exercise the opt out right.

(2) Examples:

(i) Adequate opt out notice. A licensee provides adequate notice that the consumer can opt out of the disclosure of nonpublic personal financial information to a nonaffiliated third party if the licensee:

(a) Identifies all of the categories of nonpublic personal financial information that the licensee discloses or reserves the right to disclose, and all of the categories of nonaffiliated third parties to which the licensee discloses the information, as described in section 420.6(a)(2) and (3) of this Part, and states that the consumer may opt out of the disclosure of that information;

(*b*) Identifies the insurance products or services that the consumer (either individually or jointly) obtains from the licensee to which the opt out direction would apply; and

(*c*) In the case of a written opt out notice, prominently provides the address to which the completed opt out notice should be sent.

(ii) Reasonable opt out means. A licensee provides a reasonable means to exercise an opt out right if it:

(*a*) Designates check-off boxes in a prominent position on the relevant forms with the opt out notice;

(*b*) Includes a reply form together with the opt out notice;

(*c*) Provides an electronic means to opt out, such as a form that can be sent via electronic mail or a process at the licensee's web site, if the consumer agrees to the electronic delivery of information; or

(*d*) Provides a toll-free telephone number that consumers can call to opt out.

(iii) Unreasonable opt out means. A licensee does not provide a reasonable means of opting out if:

(*a*) The only means of opting out is for the consumer to write his or her own letter to exercise that opt out right; or

(*b*) The only means of opting out as described in any notice subsequent to the initial notice is to use a check-off box that the licensee provided with the initial notice but did not include with the subsequent notice.

(iv) Specific opt out means. A licensee may require each consumer to opt out through a specific means, as long as the means is reasonable for that consumer.

(b) Same form as initial notice permitted. The licensee may provide the opt out notice together with or on the same written or electronic form as the initial notice the licensee provides in accordance with section 420.4 of this Part.

(c) Initial notice required when opt out notice delivered subsequent to initial notice. If a licensee provides the opt out notice later than required for the initial notice in accordance with section 420.4 of this Part, the licensee shall also include a copy of the initial notice in writing or, if the consumer agrees, electronically.

(d) Joint relationships.

(1) If two or more consumers jointly obtain an insurance product or service from a licensee, the licensee may provide a single opt out notice. The licensee's opt out notice shall explain how the licensee will treat an opt out direction by a joint consumer (as explained in paragraph (d)(2) of this subdivision).

(2) Any of the joint consumers may exercise the right to opt out. The licensee may either:

(i) Treat an opt out direction by a joint consumer as applying to all of the associated joint consumers; or

(ii) Permit each joint consumer to opt out separately.

(3) If a licensee permits each joint consumer to opt out separately, the licensee shall permit one of the joint consumers to opt out on behalf of all of the joint consumers.

(4) A licensee may not require all joint consumers to opt out before the licensee implements any opt out direction.

(5) Example. If John and Mary are both named policyholders on a homeowner's insurance policy issued by a licensee and the licensee sends all correspondence about the policy to John's address, the licensee may do any of the following, but the licensee shall explain in its opt out notice which opt out policy it will follow:

(i) Send a single opt out notice to John's address, but the licensee shall accept an opt out direction from either John or Mary;

(ii) Treat an opt out direction by either John or Mary as applying to the entire account. If the licensee does so, and John opts out, the licensee may not require Mary to opt out as well before implementing John's opt out direction; or

(iii) Permit John and Mary to make different opt out directions. If the licensee does so:

(*a*) It shall permit John and Mary to opt out for each other;

(*b*) If both opt out, the licensee shall permit both of them to notify it in a single response (such as on a form or through a telephone call); and

(*c*) If John opts out and Mary does not, the licensee may only disclose nonpublic personal financial information about Mary, but not about John and not about John and Mary.

(e) Time to comply with opt out. A licensee shall comply with a consumer's opt out direction as soon as reasonably practicable after the licensee receives it.

(f) Continuing right to opt out. A consumer may exercise the right to opt out at any time.

(g) Duration of consumer's opt out direction.

(1) A consumer's direction to opt out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, revokes it electronically, or revokes it by calling a toll-free telephone number, if such number is provided by the licensee.

(2) When a customer relationship terminates, the customer's opt out direction continues to apply to the nonpublic personal financial information the licensee collected during or related to that relationship. If the individual subsequently establishes a new customer relationship with the licensee, the opt out direction that applied to the former relationship does not apply to the new relationship.

(h) Delivery. When a licensee is required to deliver an opt out notice by this section, the licensee shall deliver it according to section 420.9 of this Part.

Section 420.8 Revised privacy notices.

(a) General rule. Except as otherwise authorized in this Part, a licensee shall not, directly or through any affiliate, disclose any nonpublic personal financial information about a consumer to a nonaffiliated third party, other than as described in the initial notice that the licensee provided to that consumer under section 420.4 of this Part, unless:

(1) The licensee has provided to the consumer a clear and conspicuous revised notice that accurately describes the licensee's policies and practices;

(2) The licensee has provided to the consumer a new opt out notice;

(3) The licensee has given the consumer a reasonable opportunity, before the licensee discloses the information to the nonaffiliated third party, to opt out of the disclosure; and

(4) The consumer does not opt out.

(b) Examples:

(1) Except as otherwise permitted by sections 420.13, 420.14, and 420.15 of this Part, the licensee shall provide a revised notice before the licensee:

(i) Discloses a new category of nonpublic personal financial information to any nonaffiliated third party;

(ii) Discloses nonpublic personal financial information to a new category of nonaffiliated third party; or

(iii) Discloses nonpublic personal financial information about a former customer to a nonaffiliated third party, if that former customer has not had the opportunity to exercise an opt out right regarding that disclosure.

(2) A revised notice is not required if the licensee discloses nonpublic personal financial information to a new nonaffiliated third party that the licensee adequately described in the licensee’s prior notice.

(c) Delivery. When the licensee is required to deliver a revised privacy notice by this section, the licensee shall deliver it according to section 420.9 of this Part.

Section 420.9 Delivery.

(a) How to provide notices. A licensee shall provide any notices that this Part requires so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically. A licensee may provide any and all privacy and opt out notices, including short-form initial notices through an affiliate or agent, but remains responsible for compliance with this Part.

(b)(1) Examples of reasonable expectation of actual notice. A licensee may reasonably expect that a consumer will receive actual notice if the licensee:

(i) Hand-delivers a printed copy of the notice to the consumer;

(ii) Mails a printed copy of the notice to the last known address of the consumer separately, or in a policy, billing or other written communication;

(iii) For a consumer who conducts transactions electronically, clearly and conspicuously posts the notice on the electronic site and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular insurance product or service;

(iv) For the consumer who consents to receiving such notices electronically, electronically mails a copy of the notice, return receipt, to the consumer's electronic mail address;

(v) For an isolated transaction with a consumer, such as the licensee providing an insurance quote or selling the consumer travel insurance, provides or posts the notice and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular insurance product or service.

(2) Examples of unreasonable expectation of actual notice. A licensee may not, however, reasonably expect that a consumer will receive actual notice of the licensee's privacy policies and practices if the licensee:

(i) Only posts a sign in its office or generally publishes advertisements of its privacy policies and practices; or

(ii) Sends the notice via electronic mail to a consumer who does not obtain an insurance product or service from the licensee electronically.

(c) Annual notices only. A licensee may also reasonably expect that a customer will receive actual notice of the licensee's annual privacy notice if:

(1) The customer uses the licensee's web site to access insurance products and services electronically and agrees to receive notices at the web site, and the licensee posts its current privacy notice continuously in a clear and conspicuous manner on the web site; or

(2) The customer has requested that the licensee refrain from sending any information regarding the customer relationship, and the licensee's current privacy notice remains available to the customer upon request.

(d) Oral description of notice insufficient. A licensee may not provide any notice required by this Part solely by orally explaining the notice, either in person or over the telephone.

(e) Retention or accessibility of notices for customers.

(1) For customers only, a licensee shall provide the initial notice required by section 420.4(a)(1) of this Part, the annual notice required by section 420.5(a) of this Part, and the revised notice required by section 420.8 of this Part so that the customer can retain them or obtain them later in writing or, if the customer agrees, electronically.

(2) Examples of retention or accessibility. The licensee provides a privacy notice to the customer so that the customer can retain it or obtain it later if the licensee:

(i) Hand-delivers a printed copy of the notice to the customer;

(ii) Mails a printed copy of the notice to the last known address of the customer; or

(iii) Makes the licensee's current privacy notice available on a web site (or a link to another web site) for the customer who obtains an insurance product or service electronically and agrees to receive the notice at the web site.

(f) Joint notice with other financial institutions. A licensee may provide a joint notice from the licensee and one or more of the licensee's affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to both the licensee and the other institutions. A licensee may also provide a notice on behalf of another financial institution.

(g) Treatment of invalid addresses. A licensee is not required to provide initial, annual and revised notices to a consumer or a customer if the consumer's or the customer's last known address, according to the licensee's records, is deemed invalid. An address of record is deemed invalid if mail sent to that address has been returned by the postal authorities as undeliverable and if subsequent reasonable attempts to obtain a current valid address for the consumer or the customer have been unsuccessful.

(h) Joint relationships. If two or more consumers jointly obtain an insurance product or service from a licensee, the licensee may satisfy the initial, annual and revised notice

requirements of sections 420.4(a), 420.5(a), and 420.8(a) of this Part, respectively, by providing one notice to those consumers jointly.

LIMITS ON DISCLOSURE OF FINANCIAL INFORMATION

Section 420.10 Limits on disclosure of nonpublic personal financial information to nonaffiliated third parties.

(a)(1) Conditions for disclosure. Except as otherwise authorized in this Part, a licensee may not, directly or through any affiliate, disclose any nonpublic personal financial information about a consumer to a nonaffiliated third party unless:

(i) The licensee has provided to the consumer an initial notice as required under section 420.4 of this Part;

(ii) The licensee has provided to the consumer an opt out notice as required in section 420.7 of this Part;

(iii) The licensee has given the consumer a reasonable opportunity, before the licensee discloses the information to the nonaffiliated third party, to opt out of the disclosure; and

(iv) The consumer does not opt out.

(2) Opt out definition. Opt out means a direction by the consumer that the licensee not disclose nonpublic personal financial information about that consumer to a nonaffiliated third party, other than as permitted by sections 420.13, 420.14 or 420.15 of this Part.

(3) Examples of reasonable opportunity to opt out. A licensee provides a consumer with a reasonable opportunity to opt out if:

(i) By mail. The licensee mails the notices required in paragraph (1) of this subdivision to the consumer and allows the consumer to opt out by mailing a form, calling a toll free telephone number, or any other reasonable means within 30 days from the date the licensee mailed the notices.

(ii) By electronic means. A customer opens an on-line account with the licensee and agrees to receive the notices required in paragraph (1) of this subdivision electronically, and the licensee allows the customer to opt out by any reasonable means within 30 days after the date that the customer acknowledges receipt of the notices in conjunction with opening the account.

(iii) Isolated transaction with consumer. For an isolated transaction, such as providing the consumer with an insurance quote, a licensee provides the consumer with a reasonable opportunity to opt out if the licensee provides the consumer the notices required in paragraph (1) of this subdivision at the time of

the transaction and requests that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction**.**

(b) Application of opt out to all consumers and all nonpublic personal financial information.

(1) A licensee shall comply with this section, regardless of whether the licensee and the consumer have established a customer relationship.

(2) Unless a licensee complies with this section, the licensee may not, directly or through any affiliate, disclose any nonpublic personal financial information about a consumer that the licensee has collected, regardless of whether the licensee collected it before or after receiving the direction to opt out from the consumer.

(c) Partial opt out. A licensee may allow a consumer to select certain nonpublic personal financial information or certain nonaffiliated third parties with respect to which the consumer wishes to opt out.

Section 420.11 Limits on redisclosure and reuse of nonpublic personal financial information.

(a)(1) Information a licensee receives under an exception. If a licensee receives nonpublic personal financial information from a nonaffiliated financial institution under an exception in section 420.14 or 420.15 of this Part, the licensee's disclosure and use of that information is limited as follows:

(i) The licensee may disclose the information to the affiliates of the financial institution from which the licensee received the information;

(ii) The licensee may disclose the information to its affiliates, but the affiliates may, in turn, disclose and use the information only to the extent that the licensee may disclose and use the information; and

(iii) The licensee may disclose and use the information pursuant to an exception in section 420.14 or 420.15 of this Part, in the ordinary course of business to carry out the activity covered by the exception under which the licensee received the information.

(2) Example. If a licensee receives information from a nonaffiliated financial institution for claims settlement purposes, the licensee may disclose the information for fraud prevention, or in response to a properly authorized subpoena. The licensee may not disclose that information to a third party for marketing purposes or use that information for its own marketing purposes.

(b)(1) Information a licensee receives outside of an exception. If a licensee receives nonpublic personal financial information from a nonaffiliated financial institution other than

under an exception in section 420.14 or 420.15 of this Part, the licensee may disclose the information only:

(i) To the affiliates of the financial institution from which the licensee received the information;

(ii) To the licensee's affiliates, but the licensee's affiliates may, in turn, disclose the information only to the extent that the licensee can disclose the information; and

(iii) To any other person, if the disclosure would be lawful if made directly to that person by the financial institution from which the licensee received the information.

(2) Example. If a licensee obtains a customer list from a nonaffiliated financial institution outside of the exceptions in section 420.14 or 420.15 of this Part:

(i) The licensee may use that list for the licensee's own purposes; and

(ii) The licensee may disclose that list to another nonaffiliated third party only if the financial institution from which the licensee obtained the list could have lawfully disclosed the list to that third party. That is, the licensee may disclose the list in accordance with the privacy policy of the financial institution from which the licensee obtained the list, as limited by the opt out direction of each consumer whose nonpublic personal financial information the licensee intends to disclose, and the licensee may disclose the list in accordance with an exception in section 420.14 or 420.15 of this Part, such as to the licensee's attorneys or accountants.

(c) Information a licensee discloses under an exception. If the licensee discloses nonpublic personal financial information to a nonaffiliated third party under an exception in section 420.14 or 420.15 of this Part, the third party may disclose and use that information only as follows:

(1) The third party may disclose the information to the licensee's affiliates;

(2) The third party may disclose the information to its affiliates, but its affiliates may, in turn, disclose and use the information only to the extent that the third party may disclose and use the information; and

(3) The third party may disclose and use the information pursuant to an exception in section 420.14 or 420.15 of this Part, in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

(d) Information a licensee discloses outside of an exception. If a licensee discloses nonpublic personal financial information to a nonaffiliated third party other than under an

exception in section 420.14 or 420.15 of this Part, the third party may disclose the information only:

(1) To the licensee's affiliates;

(2) To the third party's affiliates, but the third party's affiliates, in turn, may disclose the information only to the extent the third party can disclose the information; and

(3) To any other person, if the disclosure would be lawful if the licensee made it directly to that person.

Section 420.12 Limits on sharing policy number information for marketing purposes.

(a) General prohibition on disclosure of policy numbers. A licensee shall not, directly or through an affiliate, disclose, other than to a consumer reporting agency, a policy number or similar form of access number or access code for a consumer's policy or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing through electronic mail to the consumer.

(b) Exceptions. Subdivision (a) of this section does not apply if the licensee discloses a policy number or similar form of access number or access code:

(1) To the licensee's agent or service provider solely in order to perform marketing for the licensee's own products or services, as long as the agent or service provider is not authorized to directly initiate charges to the account;

(2) To a licensee who is a producer solely in order to perform marketing for the licensee's own products or services; or

(3) To a participant in an affinity or similar program where the participants in the program are identified to the customer when the customer enters into the program.

(c) Examples:

(1) Policy number. Disclosure of a policy number in encrypted form would not be prohibited if the licensee does not provide the recipient with the means to decode the number or code.

(2) Policy or transaction account. For the purposes of this section, a policy or transaction account is an account other than a deposit account or a credit card account. A transaction account does not include an account to which third parties cannot initiate charges.

EXCEPTIONS TO LIMITS ON DISCLOSURE OF FINANCIAL INFORMATION

Section 420.13 Exception to opt out requirements for disclosure of nonpublic personal financial information for service providers and joint marketing.

(a) General rule.

(1)The opt out requirements in sections 420.7 and 420.10 of this Part do not apply when a licensee provides nonpublic personal financial information to a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf, if the licensee:

(i) Provides the initial notice in accordance with section 420.4 of this Part; and

(ii) Enters into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the licensee disclosed the information, including use under an exception in section 420.14 or 420.15 of this Part in the ordinary course of business to carry out those purposes.

(2) Example. If the licensee discloses nonpublic personal financial information under this section to a financial institution with which the licensee performs joint marketing, the licensee's contractual agreement with that institution meets the requirements of paragraph (a)(1)(ii) of this subdivision if it prohibits the institution from disclosing or using the nonpublic personal financial information except as necessary to carry out the joint marketing or under an exception in section 420.14 or 420.15 of this Part in the ordinary course of business to carry out that joint marketing.

(b) Service may include joint marketing. The services a nonaffiliated third party performs for a licensee under subdivision (a) of this section may include marketing of the licensee's own products or services or marketing of financial products or services offered pursuant to joint agreements between the licensee and one or more financial institutions.

(c) Definition of joint agreement. For purposes of this section, "joint agreement" means a written contract pursuant to which a licensee and one or more financial institutions jointly offer, endorse or sponsor a financial product or service.

Section 420.14 Exceptions to notice and opt out requirements for disclosure of nonpublic personal financial information for processing and servicing transactions.

(a) Exceptions for processing transactions at consumer's request. The requirements for initial notice to the consumer in section 420.4(a)(2) of this Part, and the opt out provisions in sections 420.7 and 420.10 of this Part and their application to service providers and joint marketing as described in section 420.13 of this Part, do not apply if the licensee discloses nonpublic personal financial information as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes, or in connection with:

(1) Servicing or processing an insurance product or service that a consumer requests or authorizes;

(2) Maintaining or servicing the consumer's account with the licensee, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity;

(3) A proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer;

(4) Reinsurance or stop loss or excess loss insurance; or

(5) The solicitation of insurance quotes on behalf of a consumer by an insurance agent or broker.

(b) "Necessary to effect, administer, or enforce a transaction" means that the disclosure is:

(1) Required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or

(2) Required, or is a usual, appropriate, or acceptable method:

(i) To carry out the transaction or the product or service business of which the transaction is a part, and record, service or maintain the consumer's account in the ordinary course of providing the insurance product or service;

(ii) To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;

(iii) To provide a confirmation, statement or other record of the transaction, or information on the status or value of the insurance product or service to the consumer or the consumer's agent or broker;

(iv) To accrue or recognize incentives or bonuses associated with the transaction that are provided by a licensee or any other party;

(v) To underwrite insurance at the consumer's request or for reinsurance purposes, or for any of the following purposes as they relate to a consumer's insurance: account administration, reporting, investigating or, preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects or as otherwise required or specifically permitted by federal or state law; or

(vi) In connection with:

(*a*) The authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited, or otherwise paid using a debit, credit, or other payment card, check, or account number, or by other payment means;

(*b*) The transfer of receivables, accounts, or interests therein; or

(*c*) The audit of debit, credit, or other payment information.

Section 420.15 Other exceptions to notice and opt out requirements for disclosure of nonpublic personal financial information.

(a) Exceptions to opt out requirements. The requirements for initial notice to consumers in section 420.4(a)(2) of this Part, and the opt out provisions in sections 420.7 and 420.10 of this Part and their application to service providers and joint marketing in as described in section 420.13 of this Part, do not apply when a licensee discloses nonpublic personal financial information:

(1) With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction (see subdivision (b) of this section);

(2)(i) To protect the confidentiality or security of a licensee's records pertaining to the consumer, service, product or transaction;

(ii) To protect against or prevent actual or potential fraud or unauthorized transactions, claims, or other liabilities;

(iii) For required institutional risk control or for resolving consumer disputes or inquiries;

(iv) To persons holding a legal or beneficial interest relating to the consumer; or

(v) To persons acting in a fiduciary or representative capacity on behalf of the consumer;

(3) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating a licensee, persons that are assessing the licensee's compliance with industry standards, and the licensee's attorneys, accountants, and auditors;

(4) To the extent specifically permitted or required under other provisions of law and in accordance with the federal Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), to law enforcement agencies (including the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, the Securities and Exchange

Commission, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping), a state insurance or banking authority and the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety;

(5)(i) To a consumer reporting agency in accordance with the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) and the New York Fair Credit Reporting Act (N.Y. Gen. Bus. Law Article 25); or

(ii) From a consumer report reported by a consumer reporting agency;

(6) In connection with a proposed or actual sale, merger, transfer or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal financial information concerns solely consumers of such business or unit;

(7) (i) To comply with federal, state, or local laws, rules and other applicable legal requirements;

(ii) To comply with a properly authorized civil, criminal or regulatory investigation, or subpoena or summons by federal, state or local authorities; or

(iii) To respond to judicial process or government regulatory authorities having jurisdiction over a licensee for examination, compliance or other purposes as authorized by law; or

(8) For purposes related to the replacement of a group benefit plan, a group health plan, a group welfare plan or a workers' compensation plan.

(b) Example of revocation of consent: A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal financial information as permitted under section 420.7(f) of this Part.

Section 420.16 Nondiscrimination regarding opting out.

A licensee shall not unfairly discriminate against any consumer or customer because that consumer or customer has opted out from the disclosure of his or her nonpublic personal financial information pursuant to the provisions of this Part.

RULES FOR HEALTH INFORMATION

Section 420.17 When authorization required for disclosure of nonpublic personal health information.

(a) A licensee shall not disclose nonpublic personal health information about a consumer or customer unless an authorization is obtained from the consumer or customer whose nonpublic personal health information is sought to be disclosed.

(b) Nothing in this section shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a licensee for the performance of the following insurance functions by or on behalf of the licensee: claims administration; claims adjustment and management; detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity; underwriting; policy placement or issuance; loss control; ratemaking and guaranty fund functions; reinsurance and excess loss insurance; risk management; case management; disease management; quality assurance; quality improvement; performance evaluation; provider credentialing verification; utilization review; peer review activities; actuarial, scientific, medical or public policy research; grievance procedures; internal administration of compliance, managerial, and information systems; policyholder service functions; auditing; reporting; database security; administration of consumer disputes and inquiries; external accreditation standards; the replacement of a group benefit plan or workers' compensation policy or program; activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit; any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services; disclosure that is required, or is one of the lawful or appropriate methods to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes; and any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with legal process. Additional insurance functions may be added with the approval of the superintendent to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable to the interest of consumers.

Section 420.18 Authorizations.

(a) A valid authorization to disclose nonpublic personal health information pursuant to this Part shall be in written or electronic form and shall contain all of the following:

(1) The identity of the consumer or customer who is the subject of the nonpublic personal health information;

(2) A general description of the types of nonpublic personal health information to be disclosed;

(3) General descriptions of the parties to whom the licensee discloses nonpublic personal health information, the purpose of the disclosure and how the information will be used;

(4) The signature of the consumer or customer who is the subject of the nonpublic personal health information or the individual who is legally empowered to grant authority and the date signed; and

(5) Notice of the length of time for which the authorization is valid and that the consumer or customer may revoke the authorization at any time and the procedure for making a revocation.

(b) An authorization shall specify a length of time, for which the authorization shall remain valid, which in no event shall be for more than 24 months.

(c) A consumer or customer who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to this Part at any time, subject to the rights of an individual who acted in reliance on the authorization prior to notice of the revocation.

(d) A licensee that is subject to examination by this Department shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information for a period of six years from the date the authorization ends or until the examination is completed, whichever is greater. A licensee that is not subject to examination by this Department shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information for a period of six years from the date the authorization ends.

Section 420.19 Authorization request delivery.

A request for authorization and an authorization form may be delivered to a consumer or a customer as part of an opt-out notice pursuant to section 420.9 of this Part, provided that the request and the authorization form are clear and conspicuous. An authorization form is not required to be delivered to the consumer or customer or included in any other notices unless the licensee intends to disclose protected health information pursuant to section 420.17(a) of this Part.

Section 420.20 Nondiscrimination regarding nonpublic personal health information.

A licensee shall not unfairly discriminate against a consumer or customer because that consumer or customer has not granted authorization for the disclosure of his or her nonpublic personal health information pursuant to the provisions of this Part.

Section 420.21 Relationship to federal rules.

Irrespective of whether a licensee is subject to the federal Health Insurance Portability and Accountability Act (PL 104-191) privacy rules and regulations as promulgated by the U.S. Department of Health and Human Services (the “federal rule”) pursuant to Sections 262 and 264 of such Act, if a licensee complies with all requirements of the federal rule, when promulgated, except for its effective date provision, the licensee shall not be subject to any provisions of sections 420.17 through 420.20 of this Subpart.

ADDITIONAL PROVISIONS

Section 420.22 Protection of fair credit reporting acts.

(a) Nothing in this Part shall be construed to modify, limit, or supersede the operation of the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), and no inference shall be drawn on the basis of the provisions of this Part regarding whether information is transaction or experience information under section 603 of that Act.

(b) Nothing in this Part shall be construed to modify, limit or supersede the operation of the New York Fair Credit Reporting Act (N.Y. Gen. Bus. Law Article 25).

Section 420.23 Determined violation.

A contravention of this Part shall be deemed to be an unfair method of competition or an unfair or deceptive act and practice in the conduct of the business of insurance in this State, and shall be deemed to be a trade practice constituting a determined violation, as defined in section 2402(c) of the Insurance Law, in violation of section 2403 of such law.

Section 420.24 Effective date; transition rule.

(a) Effective date. This Part is effective November 13, 2000. In order to provide sufficient time for insurers and other licensees to establish policies and systems to comply with the requirements of this Part, time for compliance with this Part is extended until July 1, 2001, except that time for compliance with sections 420.17 through 420.21 of this Part is extended until December 31, 2001.

(b)(1) Notice requirement for consumers who are the licensee's customers on the compliance date. By July 1, 2001, the licensee shall provide an initial notice, as required by section 420.4 of this Part, to consumers who are the licensee’s customers on July 1, 2001.

(2) Example. A licensee meets the requirement in section (b)(1) of this subdivision, if, by July 1, 2001, a licensee has established a system for providing an initial notice to all new customers and has mailed the initial notice to all the licensee’s existing customers.

(c) Two year grandfathering of service agreements. Until July 1, 2002, a contract that a licensee has entered into with a nonaffiliated third party to perform services for the licensee or functions on the licensee’s behalf satisfies the provisions of section 420.13(a)(2) of this Part even if the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information, as long as the licensee entered into the agreement on or before July 1, 2000.

APPENDIX A TO PART 420--SAMPLE CLAUSES

Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the following sample clauses, if the clause is accurate for each institution that uses the notice. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt out of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.) Under the FCRA, a licensee may be deemed a credit reporting agency if it makes disclosures of certain types of information to nonaffiliated third parties.

A-1 Categories of information the licensee collects (all institutions).

A licensee may use this clause, as applicable, to meet the requirement of section 420.6(a)(1) of this Part to describe the categories of nonpublic personal financial information the licensee collects.

Sample Clause A-1:

We collect nonpublic personal financial information about you from the following sources:

- Information we receive from you on applications or other forms;
-
- Information about your transactions with us, our affiliates, or others; and
-
- Information we receive from a consumer reporting agency.

A-2 Categories of information a licensee discloses (institutions that disclose outside of the exceptions).

A licensee may use one of these clauses, as applicable, to meet the requirement of section 420.6(a)(2) of this Part to describe the categories of nonpublic personal financial information the licensee discloses. The licensee may use these clauses if it discloses nonpublic personal financial information other than as permitted by the exceptions in sections 420.13, 420.14, and 420.15 of this Part.

Sample Clause A-2, Alternative 1:

We may disclose the following kinds of nonpublic personal financial information about you:

- Information we receive from you on applications or other forms, such as [provide illustrative examples, such as “your name, address, social security number, assets, income and beneficiaries”];
-

- Information about your transactions with us, our affiliates, or others, such as [provide illustrative examples, such as "your policy coverage, premiums and payment history"]; and
-
- Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as "your creditworthiness and credit history"].

Sample Clause A-2, Alternative 2:

We may disclose all of the information that we collect, as described [describe location in the notice, such as "above "or "below"].

A-3 Categories of information a licensee discloses and parties to whom the licensee discloses (institutions that do not disclose outside of the exceptions).

A licensee may use this clause, as applicable, to meet the requirements of section 420.6(a)(2), (3), and (4) of this Part to describe the categories of nonpublic personal financial information about customers and former customers that the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses. A licensee may use this clause if it does not disclose nonpublic personal financial information to any party, other than as permitted by the exceptions in sections 420.14, and 420.15 of this Part.

Sample Clause A-3:

We do not disclose any nonpublic personal financial information about our customers or former customers to anyone, except as permitted by law.

A-4 Categories of parties to whom a licensee discloses (institutions that disclose outside of the exceptions).

A licensee may use this clause, as applicable, to meet the requirement of section 420.6(a)(3) of this Part to describe the categories of affiliates and nonaffiliated third parties to whom a licensee discloses nonpublic personal financial information. This clause may be used if the licensee discloses nonpublic personal financial information other than as permitted by the exceptions in sections 420.13, 420.14, and 420.15 of this Part, as well as when permitted by the exceptions in sections 420.14 and 420.15 of this Part.

Sample Clause A-4:

We may disclose nonpublic personal financial information about you to the following types of third parties:

- Financial service providers, such as [provide illustrative examples, such as "life insurers, automobile insurers, mortgage bankers, securities broker-dealers, and insurance agents"];
-

- Non-financial companies, such as [provide illustrative examples, such as "retailers, direct marketers, airlines, and publishers"]; and
-
- Others, such as [provide illustrative examples, such as "non-profit organizations"].
-

We may also disclose nonpublic personal financial information about you to nonaffiliated third parties as permitted by law.

A-5 Service provider/joint marketing exception.

A licensee may use one of these clauses, as applicable, to meet the requirements of section 420.6(a)(5) of this Part related to the exception for service providers and joint marketers in section 420.13 of this Part. If a licensee discloses nonpublic personal financial information under this exception, the licensee shall describe the categories of nonpublic personal financial information the licensee discloses and the categories of third parties with which the licensee has contracted.

Sample Clause A-5, Alternative 1:

We may disclose the following information to companies that perform marketing services on our behalf or to other financial institutions with which we have joint marketing agreements:

- Information we receive from you on applications or other forms, such as [provide illustrative examples, such as "your name, address, social security number, assets, income, and beneficiaries"];
-
- Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as "your policy coverage, premium, and payment history"]; and
-
- Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as "your creditworthiness and credit history"].
-

Sample Clause A-5, Alternative 2:

We may disclose all of the information we collect, as described [describe location in the notice, such as "above" or "below"] to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

A-6 Explanation of opt out right (licensees that disclose outside of the exceptions).

A licensee may use this clause, as applicable, to meet the requirement of section 420.6(a)(6) of this Part to provide an explanation of the consumer's right to opt out of the disclosure of nonpublic personal financial information to nonaffiliated third parties, including the

method(s) by which the consumer may exercise that right. The licensee may use this clause if the licensee discloses nonpublic personal financial information other than as permitted by the exceptions in sections 420.13, 420.14, and 420.15 of this Part.

Sample Clause A-6:

If you prefer that we not disclose nonpublic personal financial information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt out of disclosures to nonaffiliated third parties, you may [describe a reasonable means of opting out, such as "call the following toll-free number: (insert number)"].

A-7 Confidentiality and security (all institutions).

A licensee may use this clause, as applicable, to meet the requirement of section 420.6(a)(8) of this Part to describe its policies and practices with respect to protecting the confidentiality and security of nonpublic personal financial information.

Sample Clause A-7:

We restrict access to nonpublic personal financial information about you to [provide an appropriate description, such as "those employees who need to know that information to provide products or services to you"]. We maintain physical, electronic, and procedural safeguards that comply with federal and state regulations to guard your nonpublic personal financial information.

I, Gregory V. Serio, Superintendent of Insurance of the State of New York, do hereby certify that the foregoing is the new Part 420 of Title 11 of the Official Compilation of Codes, Rules and Regulations of the State of New York (Regulation 169), entitled "Privacy of Consumer Financial and Health Information", promulgated by me on October 30, 2001, pursuant to the authority granted by Sections 201, 301, 1505, 1608, 1712, and 3217, and Article 24 of the Insurance Law, and in accordance with the provisions of 12 U.S.C. 1831x, 15 U.S.C. 6801(b), 6802, 6803, 6805(b), 6805(c) and 6807 and 15 U.S.C. Chapter 94, to take effect on November 21, 2001, after publication in the State Register. This regulation was previously promulgated on an emergency basis on November 13, 2000, February 6, 2001 and March 30, 2001, with some different provisions, and May 30, 2001, July 20, 2001, and September 20, 2001, with the same provisions.

Pursuant to the provisions of the State Administrative Procedure Act, prior notice of the proposed regulation was published in the State Register on August 2, 2000 and notice of continuation of the proposed regulation was published in the January 17, 2001 issue of the State Register. No other publication or prior notice is required by statute.

_____

Gregory V. Serio
Superintendent of Insurance

October 30, 2001