PRIVACY OF CONSUMER FINANCIAL AND HEALTH INFORMATION ~~REGULATION~~ ACT

Table of Contents

ARTICLE I. GENERAL PROVISIONS

Section 1. Authority
Section 2. Purpose and Scope
Section 3. Rule of Construction
Section 4. Definitions

ARTICLE II. DATA MINIMIZATION AND CONTRACT OBLIGATIONS

Section 5. Data Minimization
Section 6. Third Party Service Provider Arrangements

ARTICLE III. CONSUMER REQUESTS

Section 7. Access, Correction, and Deletion of Nonpublic Personal Information
Section 8. Request Procedures

ARTICLE IV~~I~~. PRIVACY AND OPT OUT NOTICES FOR FINANCIAL INFORMATION

Section 9~~5~~. Initial Privacy Notice to Consumers Required
Section 10~~6~~. Annual Privacy Notice to Customers Required
Section 11~~7~~. Information to be Included in Privacy Notices
Section 12~~8~~. Form of Opt Out Notice to Consumers and Opt Out Methods
Section 13~~9~~. Revised Privacy Notices
Section 14~~10~~. Privacy Notices to Group Policyholders
Section 15~~11~~. Delivery

ARTICLE V~~III~~. LIMITS ON DISCLOSURES OF FINANCIAL INFORMATION

Section 16~~12~~. Limitation on Disclosure of Nonpublic Personal Financial Information to Nonaffiliated Third Parties
Section 17. Limits on Processing Sensitive Personal Information
Section 18. Limits on Targeted Advertising
Section 19~~13~~. Limits on Redisclosure and Reuse of Nonpublic Personal Financial Information
Section 20~~14~~. Limits on Sharing Account Number Information for Marketing Purposes

ARTICLE ~~I~~VI. EXCEPTIONS TO LIMITS ON DISCLOSURES OF FINANCIAL INFORMATION

Section 21~~15~~. Exception to Opt Out Requirements for Disclosure of Nonpublic Personal Financial Information for Service Providers and Joint Marketing
Section 22~~16~~. Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Financial Information for Processing and Servicing Transactions
Section 23~~17~~. Other Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Financial Information

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 24~~18~~. When Authorization Required for Disclosure of Nonpublic Personal Health Information
Section 25~~19~~. Authorizations
Section 26~~20~~. Authorization Request Delivery
Section 27~~21~~. Relationship to Federal Rules
Section 28~~22~~. Relationship to State Laws

ARTICLE VI~~I~~I. ADDITIONAL PROVISIONS

Section 29. Limited Exemption
Section 30~~23~~. Protection of Fair Credit Reporting Act
Section 31~~24~~. Nondiscrimination
Section 32~~25~~. Violation
Section 33. Individual Remedies
Section 34~~26~~. Severability
Section 35~~27~~. Effective Date
Appendix A Sample Clauses
Appendix B Federal Model Privacy Form

DRAFT

ARTICLE I. GENERAL PROVISIONS

Section 1. Authority

This act ~~regulation~~ is promulgated pursuant to the authority granted by Sections [insert applicable sections] of the Insurance Law.

Section 2. Purpose and Scope

A. Purpose. This ~~regulation~~ act governs the treatment of nonpublic personal health information and nonpublic personal financial information about individuals by all licensees of the state insurance department. This ~~regulation~~act:

(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 affiliates and nonaffiliated third parties; and

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

B. Scope. This ~~regulation~~ act applies to:

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

(2) All nonpublic personal health information.

C. Compliance. A licensee domiciled in this state that is in compliance with this regulation in a state that has not enacted laws or regulations that meet the requirements of Title V of the Gramm-Leach-Bliley Act (PL 102-106) may nonetheless be deemed to be in compliance with Title V of the Gramm-Leach-Bliley Act in the other state.

Drafting Note: Subsection C is intended to give licensees some guidance for complying with Title V of the Gramm-Leach-Bliley Act in those states that do not have laws or regulations that meet GLBA's privacy requirements.

Section 3. Rule of Construction

The examples in this ~~regulation~~act, the sample clauses in Appendix A, and the Federal Model Privacy Form in Appendix B of this ~~regulation~~ act are not exclusive. Compliance with an example, use of a sample clause, or the Federal Privacy Model Form, to the extent applicable, constitutes compliance with this ~~regulation~~act.

Licensees may rely on use of the Federal Privacy Form in Appendix B, consistent with the attached instructions, as a safe harbor of compliance with the privacy notice content requirements of this regulation.

Use of the Federal Model Privacy Form is not required. Licensees may continue to use other types of privacy notices, including notices that contain the examples in this ~~regulation~~ act and/or the sample clauses in Appendix A, provided that such notices accurately describe the Licensee's privacy practices and otherwise meet the notice content requirements of this ~~regulation~~act. However, while Licensees may continue to use privacy notices that contain the examples in this ~~regulation~~ act and/or the sample clauses in Appendix A, Licensees may not rely on use of privacy notices with the sample clauses in Appendix A as a safe harbor of compliance with the notice content requirements of this ~~regulation~~ act after July 1, 2019.

Drafting Note: ~~Safe harbor of compliance with this regulation for use of sample clauses in Appendix A sunsets on July 1, 2019.~~

*[**Working Note for Continued IP Discussion:** There would need to be a decision made as to whether to develop a new Appendix with model wording that could serve as a safe harbor for some period of time. This would aid all parties. If this is not done, it appears the final paragraph above would need to be revised.]*

DRAFT

Section 4. Definitions

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

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

"Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. "Biometric data" does not include a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.

(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.

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

(i) Presents the information in the notice in clear, concise sentences, paragraphs and sections;

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

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

(iv) Avoids multiple negatives;

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

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

(b) 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:

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

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

(iii) Provides wide margins and ample line spacing;

(iv) Uses boldface or italics for key words; and

(v) 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.

(c) 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:

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

(ii) Places a link on a screen that consumers frequently access, such as 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.

DRAFT

"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.

"Commissioner" means the insurance commissioner of the state.

Drafting Note: Use the title of the chief insurance regulatory official wherever the term "commissioner" appears. If the jurisdiction of certain health licensees, such as health maintenance organizations, lies with some state agency other than the insurance department, or if there is dual regulation, a state should add language referencing that agency to ensure the appropriate coordination of responsibilities.

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

"Consumer" means

(1) A~~a~~n individual who seeks to obtain, obtains or has obtained an insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, and about whom the licensee has nonpublic personal information, or that individual's legal representative.

(2) Examples.

(a) An individual who provides nonpublic personal information to a licensee in connection with obtaining or seeking to obtain financial, investment or economic advisory services relating to an insurance product or service is a consumer regardless of whether the licensee establishes an ongoing advisory relationship.

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

(c) 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.

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

(i) ~~(I)~~ The individual is:

(I) A~~a~~ beneficiary of a life insurance policy underwritten by the licensee;

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

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

(IV) ~~The individual is a~~A mortgagor of a mortgage covered under a mortgage insurance policy; and

(ii) The licensee discloses nonpublic personal financial information about the individual to a nonaffiliated third party other than as permitted under Sections 21~~15~~, 22~~16~~ and 23~~17~~ of this ~~regulation~~act.

(e) Provided that the licensee provides the initial, annual and revised notices under Section 14~~10~~ of this ~~regulation~~ act to the plan sponsor, group or blanket insurance policyholder or group annuity contractholder, or workers' compensation policyholder, and further provided that the licensee does not disclose to a nonaffiliated third party nonpublic personal financial information about an individual described in Item (i), (ii) or (iii), other than as permitted under Sections 21~~15~~, 22~~16~~ and 23~~17~~ of this ~~regulation~~act, such an individual is not the consumer of the licensee solely because he or she is:

DRAFT

(i) 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;

(ii) Covered under a group or blanket insurance policy or group annuity contract issued by the licensee; or

(iii) A claimant covered by a workers' compensation plan.

Drafting Note: In states where the workers' compensation self-insurance or workers' compensation state fund coverage is outside the commissioner's jurisdiction, regulators may wish to urge the applicable agency or agencies to promulgate a regulation similar to this ~~regulation~~ act in order to ensure parity in treatment of workers' compensation plans and to ensure that all workers covered by such plans have privacy protections.

(f) The individuals described in Subparagraph (e)(i) through (iii) of this paragraph are consumers of a licensee if the licensee does not meet all the conditions of Subparagraph (e).In no event shall the individuals, solely by virtue of the status described in Subparagraph (e)(i) through (iii) above, be deemed to be customers for purposes of this ~~regulation~~act.

(g) 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.

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

"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)).

"Control" means:

(1) Ownership, control or power to vote twenty-five percent (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 commissioner determines.

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

(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 to the consumer that are to be used primarily for personal, family or household purposes.

(2) Examples.

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

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

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

DRAFT

(b) A consumer does not have a continuing relationship with a licensee if:

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

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

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

(iv) The consumer is a beneficiary or claimant under a policy and has submitted a claim under a policy choosing a settlement option involving an ongoing relationship with the licensee;

(v) The consumer is a beneficiary or a claimant under a policy and has submitted a claim under that policy choosing a lump sum settlement option;

(vi) 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 twelve (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;

(vii) 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; or

(viii) For the purposes of this ~~regulation~~act, 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.

"De-identified data" means data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person.

(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:

(a) 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.*);

(b) 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

(c) 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.

"# (1) Financial product or service" means a 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.

DRAFT

"Genetic information" means the same as ascribed to it under materials regulated under the Health Insurance Portability and Accountability Act, as specified in 45 CFR 160.103.

"Health care" means:

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

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

(b) 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.

"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.

"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 an individual;

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

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

"Identified or identifiable natural person" means a person who can be readily identified, directly or indirectly.

(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 a insurance product or service.

(1) "Licensee" means all licensed insurers, producers and other persons licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to the Insurance Law of this state, [and health maintenance organizations holding a certificate of authority pursuant to Section [insert section] of this state's Public Health Law].

Drafting Note: Add bracketed language if HMOs are licensed under other than insurance statutes, and cite appropriate state law.

(2) A licensee is not subject to the notice and opt out requirements under this act for nonpublic personal financial information, ~~set forth in Articles I, II, III and IV of this regulation~~ if the licensee is an employee, agent, 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 ~~regulation~~act; and

(b) The licensee does not disclose any nonpublic personal information to any person other than the principal or its affiliates in a manner permitted by this ~~regulation~~act.

(3) (a) Subject to Subparagraph (b), "licensee" shall also include an unauthorized insurer that accepts business placed through a licensed excess lines broker in this state, but only in regard to the excess lines placements placed pursuant to Section [insert section] of this state's laws.

(b) An excess lines broker or excess lines insurer shall be deemed to be in compliance with the notice and opt out

DRAFT

requirements for nonpublic personal financial information set forth in ~~Articles I, II, III and IV of~~ this ~~regulation~~ act provided:

(i) 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 21~~15~~ of this ~~regulation~~act, except as permitted by Section 22~~16~~ or 23~~17~~ of this ~~regulation~~act; and

(ii) The broker or insurer delivers a notice to the consumer at the time a customer relationship is established on which the following is printed in 16-point type:

PRIVACY NOTICE

"Neither the U.S. brokers that handled this insurance nor the insurers that have underwritten this insurance will disclose nonpublic personal information concerning the buyer to nonaffiliates of the brokers or insurers except as permitted by law."

Drafting Note: References to "excess lines broker" and "excess lines insurer" should be changed as necessary to correspond with the applicable terms used in each state.

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

(a) A licensee's affiliate; or

(b) 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 direct or indirect ownership or control of the company by the licensee or its affiliate in conducting merchant banking or investment banking activities of the type described in Section 4(k)(4)(H) or insurance company investment activities of the type described in Section 4(k)(4)(I) of the federal Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).

"Nonpublic personal information" means nonpublic personal financial information and nonpublic personal health information. Nonpublic personal information does not include de-identified information, aggregated data, and pseudonymous data.

(1) "Nonpublic personal financial information" means:

(a) Personally identifiable financial information; and

(b) Any list, description or other grouping of personally identifiable consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

(2) Nonpublic personal financial information does not include:

(a) Health information;

(b) Publicly available information, except as included on a list described in Subsection [insert number]~~T~~(1)(b) of this section; or

(c) 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 that is not publicly available.

(3) Examples of lists.

(a) 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 that is not publicly available, such as account numbers.

DRAFT

(b) 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 that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.

"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.

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

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

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

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

(2) Examples.

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

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

(ii) Account balance information and payment history;

(iii) 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;

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

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

(vi) Any information the licensee collects through an Internet cookie (an information-collecting device from a web server); and

(vii) Information from a consumer report.

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

(i) Health information;

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

(iii) 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.

DRAFT

"Process" or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

"Pseudonymous data" means personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

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

(a) Federal, state or local government records;

(b) Widely distributed media; or

(c) 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:

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

(b) 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.

(a) Government records. Publicly available information in government records includes information in government real estate records and security interest filings.

(b) 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.

(c) Reasonable basis.

(i) A licensee has a reasonable basis to believe that mortgage information is lawfully made available to the general public if the licensee has determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

(ii) A 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 you that the telephone number is not unlisted.

"Sensitive Personal Information" means personally identifiable "nonpublic personal financial information" about a consumer that is:

(1) Racial or ethnic origin, religious beliefs, sex life or sexual orientation, or citizenship or citizenship status; or

(2) Genetic or biometric data that may be processed for the purpose of uniquely identifying an individual.

Drafting Note: Health information is not included as sensitive because it is already covered and addressed separately within Model 672 (see Article VII).

(1) "Targeted advertising" means displaying online advertisements to a consumer where the advertisement is selected based upon data that is linked or reasonably linkable to an identified or identifiable natural person obtained from that consumer's activities across nonaffiliated websites or online applications over time to predict such consumer's preferences or interests.

DRAFT

(2) "Targeted advertising" does not include:

(a) Online advertisements based on activities within a Licensee's own websites or online applications;

(b) Online advertisements based on the context of a consumer's current search query, visit to a website, or online application;

(c) Online advertisements directed to a consumer in response to the consumer's request for information or feedback; or

(d) Processing personal data solely for measuring or reporting advertising performance, reach, or frequency.

DRAFT

ARTICLE II. DATA MINIMIZATION AND CONTRACT OBLIGATIONS

Section 5. Data Minimization

A. Reasonably necessary and proportionate requirement. Except as otherwise provided in this act, a Licensee's' collection, use, retention, and disclosure of a consumer's personal information shall be reasonably necessary and proportionate to achieve:

(1) The purposes for which the personal information was collected or processed,

(2) Another disclosed purpose that is compatible with the context in which the personal information was collected;

(3) The purposes done at the request, direction, or consent of the consumer; or

(4) As otherwise required or allowed by law or regulations.

B. Secure disposal requirement. A Licensee shall implement policies and procedures for the secure disposal of nonpublic personal information that is no longer necessary for business operations or for other legitimate business purposes of the licensee, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

Section 6. Third Party Service Provider Arrangements

A. Contract requirement. Commensurate with the size and complexity of the third party, the nature and scope of the third party's activities, the third party's relationship with the licensee, and the type of information collected and processed by the third party, a licensee that discloses a consumer's nonpublic personal information to a third-party service provider shall enter into a contract with the third-party service provider that:

(1) Prohibits the third-party service provider from processing the nonpublic personal information for any purpose other than those related to providing the services specified in the contract with the licensee, unless retention is necessary to comply with the law or valid and binding order of a governmental body;

(2) Obligates the third-party service provider at the licensee's direction, to delete or return all nonpublic personal information to the licensee when requested; or to delete personal information after it is no longer necessary to fulfill a legal requirement;

(3) Obligates the third-party service provider to notify the licensee if it can no longer comply with its obligations under the agreement and provides the licensee with a right to terminate the agreement in such case;

(4) Obligates the third-party service provider to enter into written agreements with subprocessors and subcontractors that include provisions requiring them to meet the obligations of the third party-service provider with respect to personal information; and

(5) Obligates the third-party service provider to provide reasonable assistance to the licensee in fulfilling obligations to respond to consumer requests under Article III of this act.

***Working Note for Continued IP Discussion**: Review contractual provision under MDL-672 Sec. 15A(1)(b) and Sec. 21A(1)(b) in this draft [with respect to limiting to the purpose]. That kind of requirement is included here in this possible new Sec. 6A(1). Should this be in both places? Consider whether/where to consolidate - here under a new TPSP section (or should some of these provisions be incorporated there)?*

B For the purpose of this section,

(1) "Third party service provider" means a person that:

(a) Provides services to the licensee; and

(b) Maintains, processes or otherwise is permitted access to nonpublic personal information through its provision of services to the licensee.

(2) Third party service provider does not include:

DRAFT

(a) A licensee;

(b) An affiliate of the licensee; or

(c) A government entity;

DRAFT

ARTICLE III. CONSUMER REQUESTS

Section 7. Access, Correction, and Deletion of Nonpublic Personal Information

A. Access to Nonpublic Personal Information.

(1) In General. Upon receipt of an authorized request from a consumer, a licensee shall disclose:\

(a) The specific pieces of nonpublic personal information about a consumer that are requested by the consumer and maintained by the licensee;

(b) The categories of nonaffiliated third parties with whom the licensee discloses nonpublic personal information about the consumer; and

(c) The categories of nonaffiliated third parties from whom the licensee has received nonpublic personal information about the consumer.

(2) Certain Categories of Information. In response to a request submitted under this subsection, a licensee is not required to disclose a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data. The licensee may instead disclose in generic terms that it maintains these categories of nonpublic personal information about the consumer.

(3) Exception. Subparagraphs (1)(b) and (1)(c) do not apply when a licensee shares or receives nonpublic personal information about a consumer pursuant to an exception described in Section 23(A).

B. Correction of Nonpublic Personal Information.

(1) In General. A consumer may request the correction of his or her nonpublic personal information that is material to the processing of a claim or the binding of a policy.

(2) Requests. An authorized request from a consumer under this subsection shall identify the specific information that the consumer wishes to correct and explain why the consumer believes the licensee's information is incorrect.

(3) Licensee Obligations. After receiving an authorized request under this subsection, a licensee shall, within the time period set forth in Section 8 and taking into account the nature of the nonpublic personal information and the purposes for which it is collected and used, either:

(a) (i) Correct the information as requested by the consumer or delete the information in dispute; and

(ii) Notify the consumer of the action taken; or

(b) Notify the consumer of:

(i) Its refusal to make the correction as requested by the consumer;

(ii) The basis for the refusal to correct the information as requested; and

(iii) The ability of the consumer to submit an appeal to the licensee pursuant to subparagraph (D)(1)(d).

(4) Denials. A licensee may deny a request for correction if:

(a) The licensee reasonably believes the information is correct;

(b) The licensee received the information from a third party, such as a healthcare provider, who has the responsibility or authority for determining the accuracy of the information; or

(c) The information is subject to the exceptions set forth in Section 21, 22, and 23.

DRAFT

C Deletion of Nonpublic Personal Information

(1) In General. Upon receipt of an authorized request from a consumer, a licensee shall delete the nonpublic personal information about the consumer that is maintained by the licensee or the specific pieces of nonpublic personal information identified by the consumer.

(2) Scope of Deletion. In responding to a request from a consumer under this subsection, a licensee may present the consumer with the choice to delete select pieces of his or her nonpublic personal information as long as the option to delete all nonpublic personal information not covered by paragraph (3) is available.

(3) Exception. This subsection shall not require a licensee to delete nonpublic personal information if:

(a) The licensee is required by law or regulation to retain the information;

(b) The information may be necessary:

(i) To perform the contract or service requested or benefiting the consumer;

(ii) To comply with a legal obligation;

(iii) To exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law;

(iii) To engage in public or peer-reviewed scientific, historical, or statistical research;

(v) For solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the licensee and compatible with the context in which the consumer provided the information; or

(vi) For a purpose described in Sections 21, 22, or 23; or

(c) The information is maintained in reasonable anticipation of a claim or civil or criminal proceeding

(4) Archived Information. A licensee may delay fulfilling a consumer's request to delete with respect to information stored on an archived or backup system until the archived or backup system is deleted.

(5) Limitation on Retained Nonpublic Personal Information. With respect to nonpublic personal information that a licensee would be required to delete under this subsection but for the application of Paragraphs (3) or (4), the licensee may only process such nonpublic personal information for the applicable purpose described under Paragraphs (3) or (4).

Section 8. Request Procedures

(1) Guidelines for Responding to Authorized Requests. Except as otherwise provided in this regulation, a licensee shall respond to requests submitted under this section in the following manner:

(a) A licensee shall respond to an authorized request received from a consumer under this section, submitted through the means specified by the licensee, unless fulfilling the request proves impossible or involves disproportionate effort or the specific nonpublic personal information is not reasonably locatable and retrievable by the licensee.

(b) If a licensee is unable to verify a request using commercially reasonable efforts, the licensee shall not be required to consider the request and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

(c) A licensee that receives an authorized request from a consumer shall respond within 45 days of receipt of the

DRAFT

request. The response period may be extended once by 45 additional days when reasonably necessary, taking into account any concerns about the identity of the consumer and the complexity and number of the consumer's requests, so long as the licensee informs the consumer of any such extension within the initial 45-day response period, together with the reason for the extension.

(d) If a licensee declines to take action regarding the consumer's request, the licensee shall inform the consumer of the basis for declining to take action and any relevant instructions for how to appeal the decision pursuant to subparagraph (e).

(e) A licensee shall establish a process for a consumer to appeal the licensee's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision pursuant to subparagraph (d). Within 60 days of receipt of an appeal, a licensee shall inform the consumer in writing of any action taken or not taken in response to the appeal, including an explanation of the reasons for the decisions.

(2) Multiple Requests in a 12-Month Period. A consumer may make up to two requests per subsection in a 12-month period.

(3) Minors. A child's parent or legal guardian may submit a request under this section on behalf of the child regarding processing nonpublic personal information belonging to the child.

DRAFT

ARTICLE IV~~II~~. PRIVACY AND OPT OUT NOTICES FOR FINANCIAL INFORMATION

Section 9~~5~~. Initial Privacy Notice to Consumers Required

A. Initial notice requirement. A licensee shall provide a clear and conspicuous notice, in accordance with Sections 11 and 15, that accurately reflects its privacy policies and practices to:

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

~~Consumer. A~~a consumer, before the licensee ~~discloses~~ processes any nonpublic personal ~~financial~~ information about the consumer ~~to any nonaffiliated third party, if the licensee makes a disclosure other than as authorized by Sections 16 and 17~~.

~~B. When initial notice to a consumer is not required. A licensee is not required to provide an initial notice to a consumer under Subsection 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 16 and 17, 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 the 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:~~

~~(a) Becomes a policyholder of a licensee that is an insurer when the insurer delivers an insurance policy or contract to the consumer, or in the case of a licensee that is an insurance producer or insurance broker, obtains insurance through that licensee; or~~

~~(b) 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 Subsection A of this section as follows:~~

~~(1) The licensee may provide a revised policy notice, under Section 9, that covers the customer's new insurance 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, the licensee does not need to provide a new privacy notice under Subsection A of this section.~~

~~E. Exceptions to allow subsequent delivery of notice.~~

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

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

DRAFT

~~(b) Providing notice not later than when the licensee establishes a 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.~~

~~(a) 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 financial institution or residual market mechanism and the customer does not have a choice about the licensee's acquisition or assignment.~~

~~(b) 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.~~

~~(c) 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.~~

#~~C~~. Delivery. When a licensee is required to deliver an initial privacy notice by this section, the licensee shall deliver it according to Section 15~~11~~. If the licensee uses a short-form initial notice for non-customers according to Section 11~~7~~D, the licensee may deliver its privacy notice according to Section 11~~7~~D(3).

Section 10~~6~~. 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 twelve (12) consecutive months during which that relationship exists. A licensee may define the twelve-consecutive-month period, but the licensee shall apply it to the customer on a consistent basis.

(2) Example. A licensee provides a notice annually if it defines the twelve-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 opens an account on any day of year 1, the licensee shall provide an annual notice to that customer by December 31 of year 2.

B. Exception to general rule. A licensee that provides nonpublic personal information to nonaffiliated third parties only in accordance with Sections 21~~15~~, 22~~16~~, or 23~~17~~ and has not changed its policies and practices with regard to disclosing nonpublic personal information from the policies and practices that were disclosed in the most recent disclosure sent to consumers in accordance with this section or Section 5 shall not be required to provide an annual disclosure under this section until such time as the licensee fails to comply with any criteria described in this paragraph.

C. (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.

(a) 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.

DRAFT

(b) 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 twelve (12) consecutive months, other than to provide annual privacy notices, material required by law or regulation, or promotional materials.

(c) For the purposes of this ~~regulation~~act, 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.

(d) 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.

D. Delivery. When a licensee is required by this section to deliver an annual privacy notice, the licensee shall deliver it according to Section 15~~1~~.

Section 11~~7~~. Information to be Included in Privacy Notices

A. General rule. The initial, annual and revised privacy notices that a licensee provides under Sections 5, 6 and 9 shall include each of the following items of information, in addition to any other information the licensee wishes to provide, that applies to the licensee and to the consumers to whom the licensee sends its privacy notice:

(#) The purpose(s) for which the licensee collects and discloses nonpublic personal financial information;

(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 22~~16~~ and 23~~17~~;

(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 22~~16~~ and 23~~17~~;

(5) If a licensee discloses nonpublic personal financial information to a nonaffiliated third party under Section 21~~15~~ (and no other exception in Sections 22~~16~~ and 23~~17~~ 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~~ ability ~~under Section 12A~~ to opt out under this act, along with the methods by which the consumer may exercise that option, from the following, as applicable:

(a) ~~of t~~The disclosure of nonpublic personal financial information to nonaffiliated third parties; and

(b) Targeted advertising.

(#) A description of the consumer's ability to request to access, correct, or delete nonpublic personal information about the consumer as established under this act and the instructions for exercising such options;

~~(6)~~(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);

DRAFT

~~(7)~~(8) The licensee's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; and

DRAFT

~~(8)~~(9) Any disclosure that the licensee makes under Subsection B of this section.

***[Working Note for Continued IP Discussion**: There had been a suggestion that it could be helpful to consider revising the order of some of these items and/or to consolidate some aspects. Questions on these aspects are pending.]*

B. Description of parties subject to exceptions. If a licensee discloses nonpublic personal financial information as authorized under Sections 22~~16~~ and 23~~17~~, the licensee is not required to list those exceptions in the initial or annual privacy notices required by Sections 9~~5~~ and 10~~6~~. 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 it collects if the licensee categorizes it according to the source of the information, as applicable:

(a) Information from the consumer;

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

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

(d) Information from a consumer reporting agency.

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

(a) 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), as applicable, and provides a few examples to illustrate the types of information in each category. These might include:

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

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

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

(b) 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.

(c) If a licensee reserves the right to disclose all of the nonpublic personal financial information about consumers that it collects, the licensee may simply state that fact without describing the categories or examples of nonpublic personal information that the licensee discloses.

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

(a) 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.

(b) 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.

DRAFT

(c) 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 21~~15~~ to a nonaffiliated third party to market products or services that it offers alone or jointly with another financial institution, the licensee satisfies the disclosure requirement of Subsection A(5) of this section if it:

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

(b) States whether the third party is:

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

(ii) 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 22~~16~~ and 23~~17~~, the licensee may simply state that fact, in addition to the information it shall provide under Subsections [insert]~~A(1), A(8), A(9)~~ and Subsection 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 it does both of the following:

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

(b) 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) A licensee may satisfy the initial notice requirements in Sections 9~~5~~A~~(2)~~ and 12~~8~~C 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 9~~8~~.

(2) A short-form initial notice shall:

(a) Be clear and conspicuous;

(b) State that the licensee's privacy notice is available upon request; and

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

(3) The licensee shall deliver its short-form initial notice according to Section 14~~10~~. The licensee is not required to deliver its privacy notice with its short-form initial notice. The licensee instead may simply provide the consumer a reasonable means to obtain its 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 15~~11~~.

(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:

DRAFT

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

(b) 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 the licensee does not currently disclose, nonpublic personal financial information.

F. Sample Clauses and Federal Model Privacy Form. Sample clauses illustrating some of the notice content required by this section and the Federal Model Privacy Form are included in Appendix A and Appendix B, respectively, of this ~~regulation~~act.

Section 12~~8~~. 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 16~~12~~A, it 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, to the extent applicable:

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

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

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

(2) Examples.

(a) Adequate opt out notice on disclosure of nonpublic personal financial information. 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:

(i) Identifies all of the categories of nonpublic personal financial information that it 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 11~~7~~A(2) and (3), and states that the consumer can opt out of the disclosure of that information; and

~~(ii)~~ Identifies the insurance products or services that the consumer obtains from the licensee, either singly or jointly, to which the opt out direction would apply.

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

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

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

(iii) 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

DRAFT

(iv) Provides a toll-free telephone number that consumers may call to opt out.

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

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

(ii) 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.

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

B. Same form as initial notice permitted. A 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 9~~5~~.

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 9~~5~~, the licensee shall also include a copy of the initial notice with the opt out notice in writing or, if the consumer agrees, electronically.

D. Joint relationships.

(1) If two (2) 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 (5) of this subsection).

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

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

(b) 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 it 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 policy statements to John's address, the licensee may do any of the following, but it shall explain in its opt out notice which opt out policy the licensee will follow:

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

(b) Treat an opt out direction by either John or Mary as applying to the entire policy. 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.

DRAFT

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

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

(ii) 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

(iii) 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 jointly.

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, electronically.

(2) When a customer relationship terminates, the customer's opt out direction continues to apply to the nonpublic personal financial information that 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 15~~1~~.

I. Targeted advertising opt out. A licensee may comply with the targeted advertising opt-out requirement by:

(1) Providing either a cookie banner or a link on the footer of their website homepage that allows a consumer to opt-out of targeted advertising; or

~~(1)~~(2) Using another method, if such approach can effectively identify a person and remove them from targeted advertising.

Section 13~~9~~. Revised Privacy Notices

A. General rule. Except as otherwise authorized in this ~~regulation~~act, a licensee shall not, directly or through an 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 9~~5~~, unless:

(1) The licensee has provided to the consumer a clear and conspicuous revised notice that accurately describes its 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 21~~15~~, 22~~16~~ and 23~~17~~, a licensee shall provide a revised notice before it:

DRAFT

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

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

DRAFT

(c) 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 its prior notice.

C. Delivery. When a licensee is required to deliver a revised privacy notice by this section, the licensee shall deliver it according to Section 15~~11~~.

Section 14~~10~~. Privacy Notices to Group Policyholders

Unless a licensee is providing privacy notices directly to covered individuals described in Section [insert – previously 4F(2)(e)(i), (ii) or (iii)], a licensee shall provide initial, annual and revised notices to the plan sponsor, group or blanket insurance policyholder or group annuity contractholder, or workers' compensation policyholder, in the manner described in Sections 9~~5~~ through 13~~9~~ of this ~~regulation~~act, describing the licensee's privacy practices with respect to nonpublic personal information about individuals covered under the policies, contracts or plans. Compliance with this section satisfies the licensee's initial and annual notice of consumer information practices in Sections 9 and 10 of this act.

Section 15~~11~~. Delivery

A. How to provide notices. A licensee shall provide any notices that this ~~regulation~~ act requires so that each consumer can reasonably be expected to receive or have access to the ~~actual~~ notice in writing ~~or, if the consumer agrees, electronically~~.

B. (1) Examples of reasonable expectation of ~~actual~~ notice. A licensee may reasonably expect that a consumer will receive ~~actual~~ or have access to the notice if the licensee:

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

(b) 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;

(#) Posts the notice on its Internet web site, if it complies with all of the following:

(i) The licensee provides the consumer with the Internet address where the notice is posted and the opportunity to request a paper copy of the notice at no charge;

(ii) The notice is posted in a manner that enables the consumer to print or save it using programs or applications widely available on the Internet and free of charge to use; and

(iii) The notice is easily accessible on the Internet website so long as it is in force;

(#) Delivers the notice by any electronic means permitted by law; or

(#) Provides the notice by any other means authorized by the commissioner.

~~(c) For a consumer who conducts transactions electronically, 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;~~

~~(d) For an isolated transaction with a consumer, such as the licensee providing an insurance quote or selling the consumer travel insurance, 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.~~

DRAFT

~~(2)~~ Examples of unreasonable expectation of actual notice. A licensee may not~~, however,~~ reasonably expect that a consumer will receive ~~actual~~ or have access to the notice of its privacy policies and practices if it~~:~~

~~O~~only posts a sign in its office or generally publishes advertisements of its privacy policies and practices~~; or~~

~~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 reasonably expect that a customer will receive ~~actual~~ or have access to 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

DRAFT

(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 regulation 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 5A(1), the annual notice required by Section 6A, and the revised notice required by Section 9 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. A licensee provides a privacy notice to the customer so that the customer can retain it or obtain it later if the licensee:~~

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

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

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

~~G.~~F. Joint relationships. If two (2) 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 5A, 6A and 9A, respectively,~~ by providing one notice to those consumers jointly.

DRAFT

ARTICLE VIII. LIMITS ON DISCLOSURES OF FINANCIAL INFORMATION

Section 1612. Limits on Disclosure of Nonpublic Personal Financial Information to Nonaffiliated Third Parties

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

(a) The licensee has provided to the consumer an initial notice as required under Section 95;

(b) The licensee has provided to the consumer an opt out notice as required in Section 812;

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

(d) 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 2115, 2216 and 2317.

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

(a) By mail. The licensee mails the notices required in Paragraph (1) of this subsection 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 thirty (30) days from the date the licensee mailed the notices.

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

(c) 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 notices required in Paragraph (1) of this subsection 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.

DRAFT

Section 17. Limits on Processing Sensitive Personal Information

*[**Working Note for Continued IP Discussion**: Continued discussions toward consensus language are necessary on the topic of a possible path forward for new regulatory requirements related to the use of sensitive personal information. While specific possible legislative text is not yet ready to share, these conversations have been productive and have focused on a framework that would:*

- *Permit licensees to utilize sensitive personal information for certain identified purposes and uses, including those purposes and uses identified in Article VI (Exceptions to Limits on Disclosures of Financial Information);*
- *Enable a consumer to direct a licensee that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to the authorized purposes and uses;*
- *Require a licensee that uses or discloses a consumer's sensitive personal information for purposes other than those specified in this section to provide notice to consumers that sensitive personal information may be used or disclosed for additional, specified purposes and that consumers have the right to limit the use or disclosure of their sensitive personal information; and*
- *Require a licensee that has received direction from a consumer not to use or disclose the consumer's sensitive personal information, except as authorized, to halt the use or disclosure of a consumer's sensitive personal information for any other purpose after the receipt of the consumer's direction unless the consumer subsequently provides consent.]*

Section 18. Limits on Targeted Advertising

A. Limitation on targeted advertising. A consumer has the right to opt-out of Targeted Advertising.

B. Request procedures.

(1) A licensee shall act on the request within 15 days of receipt.

(2) A licensee shall not be obligated to act on any request where the personal data in the opt-out request does not match the licensee's records.

(3) A licensee is under no obligation to obtain additional data to execute the opt-out request .

(4) A licensee may not solicit the consumer to change their opt-out selection for twelve months.

DRAFT

Section 19~~13~~. Limits on Redisclosure and Reuse of Nonpublic Personal Financial Information

A. (1) Information the licensee receives under an exception. If a licensee receives nonpublic personal financial information from a nonaffiliated financial institution under an exception in Sections 22~~16~~ or 23~~17~~ of this ~~regulation~~act, the licensee's disclosure and use of that information is limited as follows:

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

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

(c) The licensee may disclose and use the information pursuant to an exception in Sections 22~~16~~ or 23~~17~~ of this ~~regulation~~act, 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 Sections 22~~16~~ or 23~~17~~ of this ~~regulation~~act, the licensee may disclose the information only:

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

(b) To its affiliates, but its affiliates may, in turn, disclose the information only to the extent that the licensee may disclose the information; and

(c) 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 Sections 22~~16~~ or 23~~17~~:

(a) The licensee may use that list for its own purposes; and

(b) The licensee may disclose that list to another nonaffiliated third party only if the financial institution from which the licensee purchased 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 received 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 Sections 22~~16~~ or 23~~17~~, such as to the licensee's attorneys or accountants.

C. Information a licensee discloses under an exception. If a licensee discloses nonpublic personal financial information to a nonaffiliated third party under an exception in Sections 22~~16~~ or 23~~17~~ of this ~~regulation~~act, 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

DRAFT

(3) The third party may disclose and use the information pursuant to an exception in Sections 22~~16~~ or 23~~17~~ 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 Sections 22~~16~~ or 23~~17~~ of this ~~regulation~~act, 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 20~~14~~. Limits on Sharing Account Number Information for Marketing Purposes

A. General prohibition on disclosure of account 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. Subsection A of this section does not apply if a licensee discloses a policy number or similar form of access number or access code:

(1) To the licensee's service provider solely in order to perform marketing for the licensee's own products or services, as long as the 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. A policy number, or similar form of access number or access code, does not include a number or code in an encrypted form, as long as the licensee does not provide the recipient with a 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 policy or transaction account does not include an account to which third parties cannot initiate charges.

DRAFT

ARTICLE ~~I~~VI. EXCEPTIONS TO LIMITS ON DISCLOSURES OF FINANCIAL INFORMATION

Section 21~~15~~. 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 12~~8~~ and 16~~12~~ 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:

(a) Provides the initial notice in accordance with Section 9~~5~~; and

(b) 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 Sections 22~~16~~ or 23~~17~~ in the ordinary course of business to carry out those purposes.

*[**Working Note for Continued IP Discussion:** TPSP section (Sec. 6) also includes contractual agreement.]*

(2) Example. If a 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 (1)(b) of this subsection 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 Sections 22~~16~~ or 23~~17~~ 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 Subsection 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 22~~16~~. 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 in Section 9~~5~~A(2), the opt out in Sections 12~~8~~ and 16~~12~~, and service providers and joint marketing in Section 21~~15~~ 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 a 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; or

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

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

DRAFT

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

(a) 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;

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

(c) 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;

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

(e) To underwrite insurance at the consumer's request 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

(f) In connection with:

(i) 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;

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

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

Section 23~~17~~. 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 5A(2), the opt out in Sections 8 and 12, and service providers and joint marketing in Section 15 do not apply when a licensee discloses or processes 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;

(2) (#) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information;

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

(b) To protect against or prevent actual or potential fraud or unauthorized transactions;

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

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

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

~~(2)~~(3) To provide information to insurance rate advisory organizations, guaranty funds or agencies,

DRAFT

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;

DRAFT

~~(3)~~(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 authority, and the Federal Trade Commission), self-regulatory organizations or for an investigation on a matter related to public safety, or to aid in taking steps to protect the life and physical safety of the consumer or of another natural person;

~~(4)~~(5) (a) To a consumer reporting agency in accordance with the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); or

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

~~(5)~~(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 the business or unit;

~~(6)~~(7) (a) To comply with federal, state or local laws, rules and other applicable legal requirements;

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

(c) 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

~~(7)~~(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.

***[Working Note for Continued Discussion**: In response to a suggestion about reorganizing the list of exceptions above, additional work may be done.]*

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 information as permitted under Section ~~8~~12F.

Drafting Note: Because the notice requirements of this ~~regulation~~ act could be a financial burden on a company in liquidation or receivership and negatively impact the ability of the liquidator or receiver to pay claims, regulators may want to consider adding an additional exception providing that licensees in liquidation or receivership are not subject to the notice provisions of this ~~regulation~~act.

DRAFT

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 2418. 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 commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable to the interest of consumers.

Section 2519. Authorizations

A. A valid authorization to disclose nonpublic personal health information pursuant to this Article VII 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 for the purposes of this Article VII shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than twenty-four (24) months.

C. A consumer or customer who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to this Article VII 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 shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information.

DRAFT

Section 2620. 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 1511, 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 2418A.

Section 2721. Relationship to Federal Rules

A Licensee which is subject to and governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), and which maintains Nonpublic Personal Information in the same manner as Protected Health Information shall be deemed to comply with the requirements of this Act. ~~Irrespective of whether a licensee is subject to the federal Health Insurance Portability and Accountability Act privacy rule as promulgated by the U.S. Department of Health and Human Services [insert cite] (the "federal rule"), if a licensee complies with all requirements of the federal rule except for its effective date provision, the licensee shall not be subject to the provisions of this Article V.~~

Drafting Note: The drafters note that the effective date of this regulation is July 1, 2001. The HHS regulation is anticipated to be promulgated in late 2000, thereby becoming effective in late 2002. As of July 1, 2001, if the licensee is in compliance with all requirements of the HHS regulation except its effective date provision, the licensee is not subject to the provisions of this article. If the licensee comes into compliance with the HHS regulation after that date, the licensee is no longer subject to the provisions of this article as of the date the licensee comes into compliance with the HHS regulation.

Section 2822. Relationship to State Laws

Nothing in this article shall preempt or supercede existing state law related to medical records, health or insurance information privacy.

DRAFT

ARTICLE VIII. ADDITIONAL PROVISIONS

Section 29. Limited Exemption

A licensee that processes the nonpublic personal information of less than thirty-five thousand resident consumers of this state during a calendar year is exempt from Article II [Data Minimization and Contract Obligations], Article III [Consumer Requests], and Section 18 [Targeted Advertising] of this act.

Section 3023. Protection of Fair Credit Reporting Act

Nothing in this ~~regulation~~ act 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 ~~regulation~~ act regarding whether information is transaction or experience information under Section 603 of that Act.

Section 3124. Nondiscrimination

A. 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 ~~regulation~~act.

B. 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 ~~regulation~~act.

Section 3225. Violation

Drafting Note: Cite state unfair trade practices act or other applicable state law.

Section 33. Individual Remedies

Nothing in this act shall be construed to create or imply a private cause of action for violation of its provisions.

Section 3326. Severability

If any section or portion of a section of this regulation or its applicability to any person or circumstance is held invalid by a court, the remainder of the regulation or the applicability of the provision to other persons or circumstances shall not be affected.

Section 3427. Effective Date

*[**Working Note for Continued IP Discussion**: In terms of implementation, additional consideration is needed to understand whether this is timeline achievable generally? And, for those not doing business in California, this may be an even more crucial question.]*

DRAFT

A. General e~~E~~ffective date. This act shall take effect two years from the date of enactment~~regulation is effective November 13, 2000. In order to provide sufficient time for licensees to establish policies and systems to comply with the requirements of this regulation, the commissioner has extended the time for compliance with this regulation until July 1, 2001~~.

Drafting Note: Existing state regulation/law should remain in place until this takes effect. It should be affirmatively repealed to coincide with this effective date.

B. Transition periods. Licensees shall have additional transition time from the general effective date set forth in subsection (A) of this section to comply with the requirements of certain provisions of this act, as follows:

(1) One year from the general effective date to comply with Article III [Consumer Requests (access, correction, and deletion)];

(2) Eighteen months from the general effective date to comply with Sections 17 [Limits on Processing SPI] and 18 [Targeted Advertising] and any notice and opportunity to opt out relating targeted advertising; and

(3) Two years from the general effective date to comply with Section 5 [Data Minimization].

~~B. (1) Notice requirement for consumers who are the licensee's customers on the compliance date. By July 1, 2001, a licensee shall provide an initial notice, as required by Section 5, to consumers who are the licensee's customers on July 1, 2001.~~

~~(2) Example. A licensee provides an initial notice to consumers who are its customers on July 1, 2001, if, by that date, the 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~~ Pre-existing service agreements. Until two years from the general effective date, ~~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 Sections 6 and 15A(1)(b) of this ~~regulation~~act, even if the contract does not include ~~a~~ requirements for and restriction on ~~that~~ the third party with respect to nonpublic personal information as provide in that section~~maintain the confidentiality of nonpublic personal information~~, as long as the licensee entered into the agreement on or before the general effective date~~July 1, 2000~~.

***[Working Note for Continued IP Discussion**: Review the contractual requirements under MDL-672 Sec. 15 (here Sec. 21) as well as the possible new TPSP provision (Sec. 6) for how they interact and which would be most appropriate to reference here. Would it be Section 6 only?]*

DRAFT

APPENDIX A – SAMPLE CLAUSES

*[**Working Note**: Development of optional safe harbor examples of wording may ease implementation and offer common understandings of privacy notices/forms.]*

APPENDIX B – FEDERAL MODEL PRIVACY FORM

*[**Working Note**: Continued availability of the safe harbors and optional templates, including a federal model privacy form, is essential to some insurers*

DRAFT

DRAFT