806 KAR 3:210. Privacy of consumer financial and health information.

RELATES TO: KRS 304.2-105, 15 U.S.C. 6801-6809, the Gramm-Leach-Bliley Act

STATUTORY AUTHORITY: KRS 304.2-105, 304.2-110, 304.17A-609, 304.17A.846, 15 U.S.C. 6801(b), 6805, the Gramm-Leach-Bliley Act

NECESSITY, FUNCTION, AND CONFORMITY: KRS 304.2-110 provides that the commissioner of the Department of Insurance may make reasonable rules and administrative regulations necessary for or as an aid to the effectuation of any provisions of the Kentucky Insurance Code. The Gramm-Leach-Bliley Act, 15 U.S.C. 6801(b) and 6805, requires state insurance commissioners to establish standards for insurers, agencies, and agents to safeguard the security and confidentiality of consumer records and information. 15 U.S.C. 6801 to 6809 applies to financial institutions engaging in financial activities such as "Insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death, or providing and issuing annuities, and acting as principal, agent, or broker for the purpose of the foregoing, in any State." This administrative regulation extends the application to protect individuals "who obtain or are claimants or beneficiaries of products or services primarily for personal, family, or household purposes from licensees," in harmony with the federal regulations. This stricter standard will hold all Kentucky licensees to the same standard, protect the privacy of Kentucky citizens, and promote uniformity of state insurance administrative regulations across state borders because this administrative regulation is based on a national model adopted by the National Association of Insurance Commissioners. Although federal law does not prohibit financial institutions from discriminating against individuals who have used their right to opt out or refused to grant authorization to disclose nonpublic personal financial information, this administrative regulation protects Kentucky citizens from discrimination. This administrative regulation establishes security requirements for an insurer's, agency's, or agent's use of consumers' financial and health information.

Section 1. Definitions.

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

(2) "Annually" means at least once in a period of twelve (12) consecutive months during which a customer relationship exists.

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

(4) "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.

(5) "Commissioner" means the Commissioner of the Kentucky Department of Insurance.

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

(7) "Consumer":

(a)

1. Means an 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

2. Means that individual's legal representative.

(b) Does include:

1. 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, regardless of whether the licensee establishes an ongoing advisory relationship;

2. An applicant for insurance prior to the inception of insurance coverage; and

3. An individual subject to disclosure by a licensee of nonpublic personal financial information to a nonaffiliated third party, other than as permitted under Sections 14, 15, and 16 of this administrative regulation, if:

a. The individual is a beneficiary of a life insurance policy underwritten by the licensee;

b. The individual is a claimant under an insurance policy issued by the licensee;

c. The individual is an insured or annuitant under an insurance policy or an annuity issued by the licensee; or

d. The individual is a mortgagor of a mortgage covered under a mortgage insurance policy.

(c) Does not mean an individual is a "consumer" solely on the basis that:

1. An individual is a consumer of another financial institution and the licensee is acting as agent for, or provides processing or other services to, that financial institution;

2. An individual is a beneficiary of a trust for which the licensee is a trustee; or

3. An individual has designated the licensee as trustee for a trust.

(d) Does not mean an individual is a "consumer" solely based on the status listed in subparagraph 2a through c of this paragraph, if:

1. The licensee provides the initial, annual, and revised notices under Sections 5, 6, and 9 of this administrative regulation to the plan sponsor, group, or blanket insurance policyholder, group annuity contract holder, or workers' compensation plan participant; and

2. The licensee does not disclose to a nonaffiliated third party nonpublic personal financial information, other than as permitted under Sections 14, 15, and 16 of this administrative regulation, about an individual who is:

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

b. Covered under a group or blanket life insurance policy or group annuity contract issued by the licensee; or

c. A beneficiary in a workers' compensation plan.

(e) Does mean the individuals described in paragraph (d)2a through c of this subsection are consumers of a licensee if the licensee fails to meet all the conditions of paragraph (d)1 and 2 of this subsection.

(8) "Consumer reporting agency" is defined in 15 U.S.C. 1681a(f) of the federal Fair Credit Reporting Act.

(9) "Continuing relationship":

(a) Means a relationship between a consumer and a licensee if:

1. The consumer is a current policyholder of an insurance product issued by or through the licensee; or

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

(b) Does not mean that a consumer has a continuing relationship with the licensee if:

1. The consumer applies for insurance but does not purchase the insurance;

2. The licensee sells the consumer airline travel insurance in an isolated transaction;

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

4. The consumer is a beneficiary or claimant under a policy and has submitted a claim under that policy choosing a settlement option involving an ongoing

relationship with the licensee;

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

6. The customer's policy has lapsed, expired, or is 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 administrative regulation, communication at the direction of a state or federal authority, or promotional materials;

7. 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

8. The individual's last known address according to the licensee's records is invalid. An address of record is invalid if mail sent to that address by the licensee is returned by the postal authorities as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual are unsuccessful.

(10) "Control" means:

(a) Ownership, control, or power to vote twenty-five (25) percent or more of the outstanding shares of any class of voting security of the company, or acting through one (1) or more other persons;

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

(c) The power to exercise a controlling influence over the management or policies of the company.

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

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

(13)

(a) "Designed to call attention" means that the notice:

1. Uses a plain-language heading;

2. Uses a typeface and type size that are easy to read;

3. Provides wide margins and ample line spacing;

4. Uses boldface or italics for key words; and

5. Is in a form that combines the licensee's notice with other information and uses distinctive type size, style, and graphic devices, such as shading or sidebars.

(b) If a licensee provides a notice on an Internet Web page, "designed to call attention" means that the notice uses text or visual cues to encourage scrolling down the page to view the entire notice, if necessary, and ensures that other elements on the Web site do not distract attention from the notice, and the licensee either:

1. Places the notice on a screen that consumers frequently access, including a page on which transactions are conducted; or

2. Places a link on a screen that consumers frequently access, including 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.

(14) "Financial institution":

(a) Means any institution engaging in activities that are financial in nature or incidental to financial activities as described in Section 4(k) of the Bank Holding Company Act of 1956 at 12 U.S.C. 1843(k).

(b) Does not mean:

1. Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under 7 U.S.C. 1 to 27f

of the Commodity Exchange Act;

2. The federal Agricultural Mortgage Corporation or any entity charged and operating under 12 U.S.C. 2001-2279cc of the Farm Credit Act of 1971; or

3. Institutions chartered by U.S. 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.

(15) "Financial product or service" means:

(a) Any product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to a financial activity described in Section 4(k) of the Bank Holding Company Act of 1956 at 12 U.S.C. 1843(k); and

(b) 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.

(16) "Former customer" means an individual with whom a licensee no longer has a continuing relationship.

(17) "Health care" means 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;

(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

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

(18) "Health care provider" is defined by KRS 304.17A-005(23).

(19) "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:

(a) The past, present, or future physical, mental, or behavioral health or condition of an individual;

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

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

(20) "Insurance product or service" means:

(a) Any product or service that is offered by a licensee, pursuant to KRS Chapter 304: and

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

(21) "Joint agreement" means a written contract pursuant to which a licensee and one (1) or more financial institutions jointly offer, endorse, or sponsor a financial product or service.

(22) "Licensee":

(a) Means all insurers holding a certificate of authority, licensed producers, companies, or business entities licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to the Kentucky Insurance Code, KRS Chapter 304.

(b) Does not mean registered service contract makers as defined in 806 KAR 5:060.

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

(a) Required;

(b) Is one (1) 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

(c) Is a usual, appropriate, or acceptable method:

1. To carry out the transaction, the product, or the 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;

2. To administer or service benefits or claims relating to the transaction, product, or service business of which it is a part;

3. 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;

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

5. To underwrite insurance at the consumer's request or for any of the following purposes as they relate to a consumer's insurance:

a. Account administration;

b. Reporting;

c. Investigating or preventing fraud or material misrepresentation;

d. Processing premium payments;

e. Processing insurance claims;

f. Administering insurance benefits, such as utilization review activities;

g. Participating in research projects; or

h. As otherwise required or specifically permitted by federal or state law; or

6. In connection with:

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

b. The transfer of receivables, accounts, or interests; or

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

(24) "Nonaffiliated third party":

(a) Means any person who is not:

1. A licensee's affiliate; or

2. Employed jointly by a licensee and a company that is not the licensee's affiliate.

(b) Includes:

1. 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 12 U.S.C. 1843(k)(4)(H) and (I) of the federal Bank Holding Company Act; and

2. A company that is not the licensee's affiliate that jointly employs a person who is also employed by the licensee.

(25) "Nonpublic personal financial information":

(a) Means:

1. Personally-identifiable financial information; and

2. Any list, description, or other grouping of consumers, and publicly-available information pertaining to them that is derived using personally-identifying financial information that is not publicly available.

(b) 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.

(c) Does not mean:

1. Health information subject to Section 18 of this administrative regulation;

2. Publicly-available information, except as included on a list described in paragraph (a)2 or (b) of this subsection; or

3. 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:

a. Publicly available, including any list of individuals' names and addresses that contains only publicly-available information;

b. Derived in whole or in part using personally-identifiable financial information that is not publicly available; and

c. Disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.

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

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

(b) With a reasonable basis to believe that the information may be used to identify an individual.

(27) "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 14, 15, and 16 of this administrative regulation.

(28) "Personally-identifiable financial information":

(a) Means information:

1. That a consumer provides to a licensee to obtain an insurance product or service from the licensee;

2. About a consumer resulting from a transaction involving an insurance product or service between a licensee and a consumer; or

3. That the licensee otherwise obtains about a consumer in connection with providing an insurance product or service to a consumer.

(b) Includes:

1. Information a consumer provides to a licensee on an application to obtain an insurance product or service;

2. Account balance information and payment history;

3. That an individual is or has been one (1) of the licensee's customers or has obtained an insurance product or service from the licensee;

4. 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;

5. 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;

6. Any information the licensee collects through an Internet cookie, an information-collecting device from a Web server; and

7. Information from a consumer report.

(c) Does not mean:

1. Health information subject to Section 18 of this administrative regulation;

2. A list of names and addresses of customers of an entity that is not a financial institution; and

3. 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.

(29) "Publicly-available information" means any 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.

(30) "Reasonable basis" to believe that information is lawfully made available to the general public means the licensee has taken steps to determine:

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

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

(31) "Reasonably understandable" means a notice:

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

(b) Uses short explanatory sentences or bullet lists, if possible;

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

(d) Avoids multiple negatives;

(e) Avoids legal and highly technical business terminology, if possible; and

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

Section 2. Purpose and Scope. This administrative regulation governs the treatment of nonpublic personal health information and nonpublic personal financial information about individuals by all licensees.

(1) This administrative regulation:

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

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

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

(2) This administrative regulation applies to:

(a) 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; and

(b) All nonpublic personal health information.

(3) This administrative regulation shall not apply to information about companies or about individuals who obtain products or services for business, commercial or agricultural purposes.

Section 3. Compliance. A licensee domiciled in this state that is in compliance with this administrative regulation in a state that has not enacted laws or regulations that meet the requirements of Title V of the Gramm-Leach-Bliley Act (Pub.L. 102-106) may be found to be in compliance with Title V of the Gramm-Leach-Bliley Act in the other state.

Section 4. Rules of Construction.

(1) The Sample Clauses and Examples, and the Model Privacy Forms and General Instructions in the material incorporated by reference are not exclusive. Compliance with an example, use of a sample clause, or model privacy form, to the extent applicable, shall constitute compliance with this administrative regulation.

(2) Licensees may rely on use of the model privacy form, consistent with the instructions, as a safe harbor compliance with the privacy notice content requirements of this administrative regulation.

(3) The Sample Clauses and Examples contains sample clauses and examples for the following:

(a) Establishment of a customer relationship, referenced in Section 5 of this administrative regulation;

(b) Exceptions to the required Initial Privacy Notices to Consumers, referenced in Section 5 of this administrative regulation;

(c) The annual privacy notice to customers, referenced in Section 6 of this administrative regulation;

(d) Customer terminations, referenced in Section 6 of this administrative regulation;

(e) Obtaining privacy notices, referenced in Section 7 of this administrative regulation;

(f) Samples clauses of the notice content required by Section 7 of this administrative regulation; and

(g) Joint consumer opt outs, referenced in Section 8 of this administrative regulation.

(4) Use of the Model Privacy Forms and General Instructions is not required. Licensees may continue to use other types of privacy notices, including notices that contain examples and sample clauses from the Sample Clauses and Examples if the notices accurately describe the licensee's privacy practices and otherwise meet the notice content requirements of this administrative regulation. However, while licensees may continue to use privacy notices that contain examples or sample clauses, licensees may not rely on use of privacy notices with the sample clauses from the Sample Clauses and Examples as a safe harbor of compliance with the notice content requirements of this administrative regulation after July 1, 2019.

Section 5. Initial Privacy Notice to Consumers Required.

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

(a) Customer. An individual who becomes the licensee's customer, not later than when the licensee establishes a customer relationship, except as provided in subsection (5) of this section; and

(b) Consumer. A consumer, before the licensee discloses 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 15 and 16 of this administrative regulation.

(2) When initial notice to a consumer is not required. A licensee shall not be required to provide an initial notice to a consumer under subsection (1)(b) of this section if:

(a)

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 15 and 16 of this administrative regulation; and

2. The licensee does not have a customer relationship with the consumer; or

(b) 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.

(3) General rule of when the licensee establishes a customer relationship. A licensee establishes a customer relationship when the licensee and the consumer enter into a continuing relationship.

(4) Existing customers. If 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 (1) of this section as follows:

(a) The licensee may provide a revised policy notice, under Section 9 of this administrative regulation, that covers the customer's new insurance product or service; or

(b) 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 shall not be required to provide a new privacy notice under subsection (1) of this section.

(5) Exceptions to allow subsequent delivery of notice. A licensee may provide the initial notice required by subsection (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

(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.

(6) Delivery. When a licensee is required to deliver an initial privacy notice by this section, the licensee shall deliver it according to Section 10 of this administrative regulation. If the licensee uses a short-form initial notice for noncustomers according to Section 7(4) of this administrative regulation, the licensee may deliver its privacy notice according to Section 7(4)(c) of this administrative regulation.

Section 6. Annual Privacy Notice to Customers Required.

(1) General rule. Except as provided in subsection (3) of this section, 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. A licensee may define the twelve (12) consecutive month period, but the licensee shall apply it to the customer on a consistent basis.

(2) Termination of customer relationship. A licensee shall not be required to provide an annual notice to a former customer.

(3) Exception to annual privacy notice requirement.

(a) A licensee that provides nonpublic personal information to nonaffiliated third parties only in accordance with Sections 14, 15, or 16 of this administrative regulation 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 of this administrative regulation shall not be required to provide an annual disclosure under this section.

(b) If a licensee fails to comply with any of the exception criteria described in paragraph (a) of this subsection, the licensee shall be required to provide the annual privacy notice required under subsection (1) of this section.

(4) Delivery. When a licensee is required by this section to deliver an annual privacy notice, the licensee shall deliver it according to Section 10 of this administrative regulation.

Section 7. Information to be Included in Privacy Notices.

(1) General rule. The initial, annual and revised privacy notices that a licensee provides under Sections 5, 6, and 9 of this administrative regulation 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:

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

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

(c) 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 15 and 16 of this administrative regulation;

(d) 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 15 and 16 of this administrative regulation;

(e) If a licensee discloses nonpublic personal financial information to a nonaffiliated third party under Section 14 of this administrative regulation, and no other exception in Sections 15 and 16 of this administrative regulation 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;

(f) An explanation of the consumer's right under Section 11 of this administrative regulation to opt out of the disclosure of nonpublic personal financial information to nonaffiliated third parties, including the methods by which the consumer may exercise that right at that time;

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

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

(i) Any disclosure that the licensee makes under subsection (2) of this section.

(2) Description of parties subject to exceptions. If a licensee discloses nonpublic personal financial information as authorized under Sections 15 and 16 of this administrative regulation, the licensee shall not be required to list those exceptions in the initial or annual privacy notices required by Sections 5 and 6 of this administrative regulation. If describing the categories of parties to whom disclosure is made, the licensee shall state only that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.

(3) Examples.

(a) Categories of nonpublic personal financial information that the licensee collects. A licensee shall satisfy 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:

1. Information from the consumer;
2. Information about the consumer's transactions with the licensee or its affiliates;
3. Information about the consumer's transactions with nonaffiliated third parties; and
4. Information from a consumer reporting agency.

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

1. A licensee shall satisfy the requirement to categorize nonpublic personal financial information it discloses if the licensee categorizes the information according to source, as described in subparagraph 3 of this paragraph, as applicable, and provides a few examples to illustrate the types of information in each category. These may include:

a. Information from the consumer, including application information, such as assets and income and identifying information, such as name, address, and Social Security number;

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

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

2. A licensee shall not categorize the information that it discloses by using only general terms, such as transaction information about the consumer.

3. 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.

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

1. A licensee shall satisfy 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.

2. 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.

3. 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 14 of this administrative regulation to a nonaffiliated third party to market products or services that it offers alone or jointly with another financial institution, the licensee shall satisfy the disclosure requirement of subsection (1)(e) 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 (1)(b) of this section, as applicable; and

b. States whether the third party is a service provider that performs marketing services on the licensee's behalf or on behalf of the licensee and another financial institution; or 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 15 and 16 of this administrative regulation, the licensee may simply state that fact, in addition to the information it shall provide under subsections (1)(a), (h), (i), and (2) 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 shall not be required to describe technical information about the safeguards it uses.

(4) Short-form initial notice with opt-out notice for noncustomers.

(a) A licensee may satisfy the initial notice requirements in Sections 5(1)(b) and 8(3) of this administrative regulation 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 8 of this administrative regulation.

(b) A short-form initial notice shall:

1. Be clear and conspicuous;

2. State that the licensee's privacy notice is available upon request; and

3. Explain a reasonable means by which the consumer may obtain that notice.

(c) The licensee shall deliver its short-form initial notice according to Section 10 of this administrative regulation. 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 10 of this administrative regulation.

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

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

(b) 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.

Section 8. Form of Opt-out Notice to Consumers and Opt-out Methods.

(1)

(a) Form of opt-out notice. If a licensee is required to provide an opt-out notice under Section 11(1) of this administrative regulation, 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:

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

2. That the consumer has the right to opt out of that disclosure; and

3. A reasonable means by which the consumer may exercise the opt-out right.

(b)

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

a. Identifies all of the categories of nonpublic personal financial information that 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 7(1)(b) and (c) of this administrative regulation, and states that the consumer may opt out of the disclosure of that information; and

b. 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.

2. Reasonable opt-out means. A licensee provides a reasonable means to exercise an opt-out right if it:

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

b. Includes a reply form together with the opt-out notice;

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

d. Provides a toll-free telephone number that consumers may call to opt out.

3. Unreasonable opt-out means. A licensee does not provide a reasonable means of opting out if:

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

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

4. 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.

(2) 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 5 of this administrative regulation.

(3) 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 5 of this administrative regulation, the licensee shall also include a copy of the initial notice with the opt-out notice in writing or, if the consumer agrees, electronically.

(4) Joint relationships.

(a) 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.

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

1. Treat an opt-out direction by a joint consumer as applying to all of the associated joint consumers; or

2. Permit each joint consumer to opt out separately.

(c) If a licensee permits each joint consumer to opt out separately, the licensee shall permit one (1) of the joint consumers to opt out on behalf of all of the joint consumers.

(d) A licensee may not require all joint consumers to opt out before it implements any opt-out direction.

(5) 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.

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

(7) Duration of consumer's opt-out direction.

(a) 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.

(b) 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.

(8) Delivery. When a licensee is required to deliver an opt-out notice by this section, the licensee shall deliver it according to Section 10 of this administrative regulation.

Section 9. Revised Privacy Notices.

(1) General rule. Except as otherwise authorized in this administrative regulation, 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 5 of this administrative regulation, unless:

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

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

(c) 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

(d) The consumer does not opt out.

(2)

(a) Except as otherwise permitted by Sections 14, 15, and 16 of this administrative regulation, a licensee shall provide a revised notice before it:

1. Discloses a new category of nonpublic personal financial information to any nonaffiliated third party;

2. Discloses nonpublic personal financial information to a new category of nonaffiliated third party; or

3. 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.

(b) 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.

Section 10. Delivery.

(1) How to provide notices. A licensee shall provide any notices that this administrative regulation requires so that each consumer may reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically.

(2)

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

1. Hand-delivers a printed copy of the notice to the consumer;

2. 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;

3. 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; or

4. 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.

(b) Illustrations of unreasonable expectation of actual notice. A licensee shall not reasonably expect that a consumer will receive actual notice of its privacy policies and practices if it:

1. Only posts a sign in its office or generally publishes advertisements of its privacy policies and practices; or

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

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

(a) 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

(b) 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.

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

(5) Retention or accessibility of notices for customers.

(a) For customers only, a licensee shall provide the initial notice required by Section 5(1)(a) of this administrative regulation, the annual notice required by Section 6(1) of

this administrative regulation, and the revised notice required by Section 9 of this administrative regulation so that the customer may retain them or obtain them later in writing or, if the customer agrees, electronically.

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

1. Hand-delivers a printed copy of the notice to the customer;
2. Mails a printed copy of the notice to the last known address of the customer; or
3. 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.

(6) Joint notice with other financial institutions. A licensee may provide a joint notice from the licensee and one (1) 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.

(7) 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 5(1), 6(1), and 9 of this administrative regulation, respectively, by providing one (1) notice to those consumers jointly.

Section 11. Limits on Disclosure of Nonpublic Personal Financial Information to Nonaffiliated Third Parties.

(1)

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

1. The licensee has provided to the consumer an initial notice as required under Section 5 of this administrative regulation;
2. The licensee has provided to the consumer an opt-out notice as required in Section 8 of this administrative regulation;
3. 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
4. The consumer does not opt out.

(b) A licensee provides a consumer with a reasonable opportunity to opt out if:

1. By mail. The licensee mails the notices required in subsection (1)(a) of this section 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.
2. By electronic means. A customer opens an on-line account with a licensee and agrees to receive the notices required in subsection (1)(a) of this section 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.
3. 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 subsection (1)(a) of this section 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.

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

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

(b) Unless a licensee complies with this section, the licensee shall 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.

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

Section 12. Limits on Redisclosure and Reuse of Nonpublic Personal Financial Information.

(1)

(a) Information the licensee receives under an exception. If a licensee receives nonpublic personal financial information from a nonaffiliated financial institution under an exception in Section 15 or 16 of this administrative regulation, the licensee's disclosure and use of that information shall be limited as follows:

1. The licensee may disclose the information to the affiliates of the financial institution from which the licensee received the information;

2. 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

3. The licensee may disclose and use the information in the ordinary course of business to carry out the activity covered by the exception under which the licensee received the information.

(b) If a licensee receives information from a nonaffiliated financial institution for claims settlement purposes, the licensee shall 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.

(2)

(a) Information a licensee receives outside of an exception. If a licensee receives nonpublic personal financial information from a nonaffiliated financial institution other than under an exception in Section 15 or 16 of this administrative regulation, the licensee may disclose the information only:

1. To the affiliates of the financial institution from which the licensee received the information;

2. To its affiliates, but its affiliates may, in turn, disclose the information only to the extent that the licensee may disclose the information; and

3. 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.

(b) If a licensee obtains a customer list from a nonaffiliated financial institution outside of the exceptions in Section 15 or 16 of this administrative regulation:

1. The licensee may use that list for its own purposes; and

2. The licensee may disclose that list to another nonaffiliated third party only if the financial institution from which the licensee purchased the list may have lawfully disclosed the list to that third party. 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 Section 15 or 16 of this administrative regulation, such as to the licensee's attorneys or accountants.

(3) Information a licensee discloses under an exception. If a licensee discloses nonpublic personal financial information to a nonaffiliated third party under an exception in Section 15 or 16 of this administrative regulation, the third party may disclose and use that information only as follows:

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

(b) 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

(c) The third party may disclose and use the information pursuant to an exception in Section 15 or 16 of this administrative regulation in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

(4) Information a licensee discloses outside of an exception. If a licensee discloses nonpublic personal financial information to a nonaffiliated third party other than under an exception in Section 15 or 16 of this administrative regulation, the third party may disclose the information only:

(a) To the licensee's affiliates;

(b) 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

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

Section 13. Limits on Sharing Account Number Information for Marketing Purposes.

(1) 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.

(2) Exceptions. Subsection (1) of this section shall not apply if a licensee discloses a policy number or similar form of access number or access code:

(a) 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;

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

(c) 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.

(3)

(a) 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.

(b) 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.

Section 14. Exception to Opt-out Requirements for Disclosure of Nonpublic Personal Financial Information for Service Providers and Joint Marketing.

(1) General rule.

(a) The opt-out requirements in Sections 8 and 11 of this administrative regulation shall 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:

1. Provides the initial notice in accordance with Section 5 of this administrative regulation; and

2. Enters into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the licensee disclosed the information, including use under an exception in Section 15 or 16 of this administrative regulation in the ordinary course of business to carry out those purposes.

(b) 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 shall meet the requirements of paragraph (a)2 of this subsection if:

1. It prohibits the institution from disclosing or using the nonpublic personal financial information except as necessary to carry out the joint marketing; or

2. Is under an exception in Section 15 or 16 of this administrative regulation in the ordinary course of business to carry out that joint marketing.

(2) Service may include joint marketing. The services a nonaffiliated third party performs for a licensee under subsection (1) 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 (1) or more financial institutions.

Section 15. Exceptions to Notice and Opt-out Requirements for Disclosure of Nonpublic Personal Financial Information for Processing and Servicing Transactions. Exceptions for processing transactions at consumer's request. The requirements for initial notice in Section 5(1)(b) of this administrative regulation, the opt out in Sections 8 and 11 of this administrative regulation, and for the service providers and joint marketing in Section 14 of this administrative regulation shall 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.

Section 16. Other Exceptions to Notice and Opt-out Requirements for Disclosure of Nonpublic Personal Financial Information.

(1) Exceptions to opt-out requirements. The requirements for initial notice to consumers in Section 5(1)(b) of this administrative regulation, the opt out in Sections 8 and 11 of this administrative regulation, and for the service providers and joint marketing in Section 14 of this administrative regulation shall not apply if a licensee discloses nonpublic personal financial information:

(a) With the consent or at the direction of the consumer, if the consumer has not revoked the consent or direction;

(b)

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

2. To protect against or prevent actual or potential fraud or unauthorized transactions;

3. For required institutional risk control or for resolving consumer disputes or inquiries;

4. To persons holding a legal or beneficial interest relating to the consumer; or

5. To persons acting in a fiduciary or representative capacity on behalf of the consumer;

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

(d) 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 to 3422, 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. 5311 to 5330, Records and Reports on Monetary Instruments and Transactions, and 12 U.S.C. 1951 to 1959, 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;

(e)

1. To a consumer reporting agency in accordance with the federal Fair Credit Reporting Act, 15 U.S.C. 1681 to 1681u; or

2. From a consumer report reported by a consumer reporting agency;

(f) 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;

(g)

1. To comply with federal, state or local laws, rules and other applicable legal requirements;

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

3. 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

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

(2) 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(6) of this administrative regulation.

(3) Licensees in liquidation or rehabilitation according to KRS Chapter 304.33 shall be exempt from the notice provisions of this administrative regulation.

Section 17. Privacy Notices to Group Policyholders. Unless a licensee is providing privacy notices directly to covered individuals described in Section 22 of this administrative regulation, 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 5 through 10 of this administrative regulation, describing the licensee's privacy practices with respect to nonpublic personal information about individuals covered under the policies, contracts, or plans.

Section 18. When Authorization Required for Disclosure of Nonpublic Personal Health Information.

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

(2) Nothing in this section shall prohibit, restrict or require an authorization for the disclosure of such 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 function; 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 function; 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 rule which is promulgated by the U.S. Department of Health and Human Services at 45 C.F.R. 160 to 164; disclosure that is required, or is one (1) 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.

(3) 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 19. Authorizations.

(1) A valid authorization to disclose nonpublic personal health information pursuant to Section 18 of this administrative regulation shall be in written or electronic form and shall contain the following:

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

(b) A general description of the types of information to be disclosed;

(c) General descriptions of the parties to whom disclosure shall be made, the purpose of the disclosure, and how the information will be used;

(d) The signature of the affected consumer or customer or the individual who is legally empowered to grant authority and the date signed;

(e) Notice of the length of time for which the authorization is valid, not to exceed twenty-four (24) months; and

(f) Notice that the consumer or customer may revoke the authorization at any time and the procedure for making a revocation.

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

(3) A licensee shall retain the authorization or copy thereof in the record of the affected individual.

Section 20. Authorization Request Delivery. A request for authorization and an authorization form may be delivered to a consumer or customer as part of an opt-out notice pursuant to Section 10 of this administrative regulation, 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 18(1) of this administrative regulation.

Section 21. Relationship to Federal Rules. Regardless of whether a licensee is subject to the federal Health Insurance Portability and Accountability Act ("HIPAA") privacy rule as promulgated by the U.S. Department of Health and Human Services at 45 C.F.R. 160 to 164, if a licensee complies with all requirements of 45 C.F.R. 160 to 164, the licensee shall not be subject to Sections 18, 19, and 20 of this administrative regulation.

Section 22. Nondiscrimination and Exemption from Notice and Opt Out Requirements.

(1) A licensee shall not unfairly discriminate against any consumer or customer because that consumer or customer has opted out from the disclosure or has not granted authorization for the disclosure of his or her nonpublic personal financial information pursuant to the provisions of this administrative regulation.

(2) A licensee shall not be subject to the notice and opt-out requirements for nonpublic personal financial information established in this administrative regulation if:

(a) The licensee is an employee, agent, or other representative of another licensee, "the principal";

(b) The principal otherwise complies with, and provides the notices required by, the provisions of this administrative regulation; and

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

(3) Pursuant to subsection (2) of this section, "licensee" shall also include an unauthorized insurer that accepts business placed through a licensed surplus broker in Kentucky, but only for the surplus lines placements placed pursuant to KRS 304.10.

(4) A surplus lines broker or surplus lines insurer shall be in compliance with the notice and opt-out requirements for nonpublic personal financial information established in this administrative regulation if:

(a) The broker or insurer does not disclose nonpublic personal information of a consumer or a customer to nonaffiliated third parties for any purpose, including joint servicing or marketing under Section 14 of this administrative regulation, except as permitted by Section 15 or 16 of this administrative regulation; and

(b) The broker or insurer delivers a notice to a consumer when a customer relationship is established on which the following is printed in sixteen (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."

Section 23. Violation. A violation of this administrative regulation shall constitute an unfair trade practice in the business of insurance and shall subject the licensee to a civil penalty authorized by KRS 304.99-020.

Section 24. Incorporation by Reference.

(1) The following material is incorporated by reference:

(a) PVCY-01, "Sample Clauses and Examples", (Edition 11/01); and

(b) "Model Privacy Forms & General Instructions", May 2017.

(2) This material may be inspected, copied, or obtained, subject to applicable copyright law, at the Kentucky Office of Insurance, 215 West Main Street, Frankfort, Kentucky 40601, Monday through Friday, 8 a.m. to 4:30 p.m.

(28 Ky.R. 1523; Am. 1828; eff. 2-11-2002; TAm eff. 8-9-2007; 44 Ky.R. 350, 744, 938; eff. 12-1-2017; Crt eff. 3-21-2023.)