e. A separate description of the categories of information the licensee discloses and the categories of third parties with which the licensee has contracted if a licensee discloses nonpublic personal financial information to a nonaffiliated third party under rule 90.12(505) and no other exception in rules 90.13(505) and 90.14(505) applies to that disclosure;

f. An explanation of the consumer's right under subrule 90.9(1) 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 Section 603(d)(2)(A)(iii) of the federal Fair Credit Reporting Act;

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

i. Any disclosure that the licensee makes under subrule 90.5(2).

90.5(2) If a licensee discloses nonpublic personal financial information as authorized under rules 90.13(505) and 90.14(505), the licensee is not required to list those exceptions in the initial or annual privacy notices required by rules 90.3(505) and 90.4(505). When describing the categories of parties to which disclosure is made, the licensee is required to state only that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable and permitted by law.

90.5(3) Examples of nonpublic personal financial information are as follows:

a. 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:

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

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

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

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

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.

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 which the licensee discloses. 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 the affiliate and nonaffiliated third parties engage.

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 business, such as life insurer, automobile insurer, consumer banking or securities brokerage.

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.

90.5(4) If a licensee discloses nonpublic personal financial information under the exception in rule 90.12(505) 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 paragraph 90.5(1)*"e"* if it does the following:

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 paragraph 90.5(1)*"b"* 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 which the licensee has a joint marketing agreement.

90.5(5) 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 rules 90.13(505) and 90.14(505), the licensee may simply state that fact, in addition to the information it shall provide under paragraphs 90.5(1)*"a," "h,"* and *"i"* and subrule 90.5(2).

90.5(6) A licensee shall describe 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.

90.5(7) A licensee may satisfy the initial notice requirements in 90.3(1)*"b"* and 90.6(4) 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 rule 90.6(505).

a. The short-form initial notice shall be clear and conspicuous, state that the licensee's privacy notice is available upon request and explain a reasonable means by which the consumer may obtain that notice.

b. The licensee shall deliver its short-form initial notice according to rule 90.8(505). 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 rule 90.8(505).

c. The licensee provides a reasonable means by which a consumer may obtain a copy of its privacy notice if the licensee provides a toll-free telephone number that the consumer may call to request the notice or, 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.

90.5(8) The licensee's notice may include categories of nonpublic personal financial information that the licensee reserves the right to disclose in the future but does not currently disclose and categories of affiliates or nonaffiliated third parties to which the licensee reserves the right in the future to disclose, but to which the licensee does not currently disclose, nonpublic personal financial information. Sample clauses are found in Appendix A.

191—90.6(505) Form of opt-out notice to consumers and opt-out methods.

90.6(1) A licensee required to provide an opt-out notice under subrule 90.9(1) shall provide a clear and conspicuous notice to each of its consumers that accurately explains the right to opt out under that rule. The notice shall state the following:

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

b. The consumer has the right to opt out of that disclosure; and

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

90.6(2) Examples of the opt-out notice include the following:

a. *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 does the following:

(1) 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 paragraphs 90.5(1)*"b"* and *"c,"* and states that the consumer can opt out of the disclosure of that information; and

(2) Identifies the insurance products or services that the consumer obtains from the licensee, either singly or jointly, to which the opt-out direction applies.

b. *Reasonable opt out.* A licensee provides a reasonable means to exercise an opt-out right if it provides the following:

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

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

(3) 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

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

c. *Unreasonable opt out.* A licensee does not provide a reasonable means of opting out in the following circumstances:

(1) The only means of opting out is for the consumer to write the consumer's own letter to exercise that opt-out right; or

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

90.6(3) 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 rule 90.3(505).

90.6(4) If a licensee provides the opt-out notice later than required for the initial notice in accordance with rule 90.3(505), the licensee shall also include in writing or, if the consumer agrees, electronically a copy of the initial notice with the opt-out notice.

90.6(5) If two or more consumers jointly obtain an insurance product or service from a licensee, the licensee may provide a single opt-out notice. The licensee's opt-out notice shall explain how the licensee will treat an opt-out direction by a joint consumer.

a. Any of the joint consumers may exercise the right to opt out. The licensee may do either of the following:

(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.

b. The licensee shall permit one of the joint consumers to opt out on behalf of all the joint consumers if a licensee permits each joint consumer to opt out separately.

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

d. Examples of opt-out notice requirements for joint consumers. If John and Mary are both names of 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 of the following opt-out policies the licensee will follow:

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

(2) 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.

(3) Permit John and Mary to make different opt-out directions. If the licensee does so, it shall provide for the following:

1. Permit John and Mary to opt out for each other;

2. Permit both of them to notify the licensee in a single response such as on a form or through a telephone call if both opt out; and

3. Allow the licensee to disclose nonpublic personal financial information about one of them such as Mary but not about John if John opts out and Mary does not and not about John and Mary jointly.

90.6(6) A licensee shall comply with a consumer's opt-out direction as soon as reasonably practicable after the licensee receives it.

90.6(7) A consumer may exercise the right to opt out at any time.

90.6(8) A consumer's direction to opt out under this rule is effective until the consumer revokes it in writing or electronically, if the consumer agrees to revoke electronically.

90.6(9) 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.

90.6(10) When a licensee is required to deliver an opt-out notice by this rule, the licensee shall deliver it according to rule 90.8(505).

191—90.7(505) Revised privacy notices.

90.7(1) Except as otherwise authorized in this rule, 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 rule 90.3(505) unless the following occur:

a. The licensee has provided to the consumer a clear and conspicuous revised privacy 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.

Except as permitted by rules 90.12(505, 90.13(505), and 90.14(505), a licensee shall provide a revised notice before the licensee does any of the following:

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

90.7(2) A revised privacy 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.

90.7(3) When a licensee is required to deliver a revised privacy notice by this rule, the licensee shall deliver it according to rule 90.8(505).

191—90.8(505) Delivery of notice.

90.8(1) A licensee shall provide any notices that these rules require so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically.

a. Examples of reasonable expectation of actual notice by a licensee are as follows:

(1) Hand delivery of a printed copy of the notice to the consumer;

(2) Mailing 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, posting the notice on the Web site and requiring the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular insurance product or service;

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

b. Examples of unreasonable expectation of actual notice by a licensee are as follows:

(1) Only posting a sign in its office or generally publishing advertisements of its privacy policies and practices; or

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

90.8(2) A licensee may reasonably expect that a customer will receive actual notice of the licensee's annual privacy notice if one of the following occurs:

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.

90.8(3) A licensee may not provide any notice required by this rule solely by orally explaining the notice, either in person or over the telephone.

90.8(4) For customers only, a licensee shall provide the initial notice required by paragraph 90.3(1)*"a,"* the annual notice required by subrule 90.4(1) and the revised notice required by rule 90.7(505) so that the customer can retain them or obtain them later in writing or, if the customer agrees, electronically.

A licensee provides a privacy notice to the customer so that the customer can retain the notice or obtain the notice later if the licensee does any of the following:

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.

90.8(5) 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 may also provide a notice on behalf of another financial institution.

90.8(6) If two or more consumers jointly obtain an insurance product or service from a licensee, the licensee may satisfy the initial, annual and revised notice requirements of subrules 90.3(1), 90.4(1) and 90.7(1), respectively, by providing one notice to those consumers jointly.

191—90.9(505) Limits on disclosure of nonpublic personal financial information to nonaffiliated third parties.

90.9(1) A licensee may not directly or through any affiliate disclose any nonpublic personal financial information about a consumer to a nonaffiliated third party except as otherwise authorized in these rules unless the following occur:

a. The licensee has provided to the consumer an initial notice as required under rule 90.3(505);

b. The licensee has provided to the consumer an opt-out notice as required in rule 90.6(505);

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

d. The consumer does not opt out.

90.9(2) A licensee provides a consumer with a reasonable opportunity to opt out under the following methods:

a. The licensee mails the notices required in 90.9(1) to the consumer and allows the consumer to opt out by mailing a form, calling a toll-free telephone number or any other reasonable means within 30 days from the date the licensee mailed the notices.

b. A customer opens an on-line account with a licensee and agrees to receive the notices required in 90.9(1) electronically, and the licensee allows the customer to opt out by any reasonable means within 30 days after the date that the customer acknowledges receipt of the notices in conjunction with opening the account.

c. For an isolated transaction such as providing the customer with an insurance quote, a licensee provides the consumer with a reasonable opportunity to opt out if the licensee provides the notice required in 90.9(1) 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.

90.9(3) A licensee shall comply with this rule regardless of whether the licensee and the consumer have established a customer relationship.

90.9(4) Unless a licensee complies with this rule, 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.

90.9(5) 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.

191—90.10(505) Limits on redisclosure and reuse of nonpublic personal financial information.

90.10(1) In the event a licensee receives nonpublic personal financial information from a nonaffiliated financial institution under an exception to rules 90.13(505) and 90.14(505), 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 rule 90.13(505) or 90.14(505) in the ordinary course of business to carry out the activity covered by the exception under which the licensee received the information.

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.

90.10(2) In the event a licensee received nonpublic personal financial information from a nonaffiliated financial institution other than under an exception in rules 90.13(505) and 90.14(505), the licensee may disclose the information only as follows:

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.

In the event a licensee obtains a customer list from a nonaffiliated financial institution outside of the exceptions in rule 90.13(505) or 90.14(505), the licensee may use that list for its own purposes and 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.

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 rule 90.13(505) or 90.14(505), such as to the licensee's attorneys or accountants.

90.10(3) In the event a licensee discloses nonpublic personal financial information to a nonaffiliated third party under an exception in rules 90.13(505) and 90.14(505), 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 rules 90.13(505) and 90.14(505) in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

90.10(4) In the event a licensee discloses nonpublic personal financial information to a nonaffiliated third party other than under an exception in rules 90.13(505) and 90.14(505), the third party may disclose the information only to the following:

a. The licensee's affiliates;

b. 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. Any other person, if the disclosure would be lawful if the licensee made it directly to that person.

191—90.11(505) Limits on sharing account number information for marketing purposes.

90.11(1) 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 marketing through electronic mail to the consumer.

90.11(2) The above subrule does not apply if a licensee discloses a policy number or similar form of access number or access code to any of the following:

a. A 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. A licensee who is a producer solely in order to perform marketing for the licensee's own products or services; or

c. 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.

A policy number or similar form of access number or access code does not include a number or code in encrypted form as long as the licensee does not provide the recipient with a means to decode the number or code.

For purposes of this subrule, 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.

191—90.12(505) Exception to opt-out requirements for disclosure of nonpublic personal financial information for service providers and joint marketing.

90.12(1) The opt-out requirements in rules 90.6(505) and 90.9(505) do not apply when a licensee provides nonpublic personal financial information to a nonaffiliated third party to perform services for the licensee or functions for the licensee on the licensee's behalf, if the licensee does the following:

a. Provides the initial notice in accordance with rule 90.3(505); 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 rules 90.13(505) and 90.14(505) in the ordinary course of business to carry out those purposes.

For example, if a licensee discloses nonpublic personal financial information under this rule to a financial institution with which the licensee performs joint marketing, the licensee's contractual agreement with that institution meets the requirements of paragraph *"b"* of this subrule 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 rules 90.13(505) and 90.14(505) in the ordinary course of business to carry out that joint marketing.

90.12(2) The services a nonaffiliated third party performs for a licensee under subrule 90.12(1) 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.

90.12(3) For purposes of this rule, "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.

191—90.13(505) Exceptions to notice and opt-out requirements for disclosure of nonpublic personal financial information for processing and servicing transactions.

90.13(1) The requirements for initial notice in paragraph 90.3(1)*"b,"* for the opt out in rules 90.6(505) and 90.9(505), and for service providers and joint marketing in rule 90.12(505) 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 the following:

a. Servicing or processing an insurance product or service that a consumer requests or authorizes;

b. 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;

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

d. Reinsurance or stop loss or excess loss insurance.

90.13(2) For purposes of this rule, "necessary to effect, administer or enforce a transaction" means that the disclosure is as follows:

a. 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

b. Required, or is a usual, appropriate or acceptable method, for the following transactions:

(1) 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;

(2) To administer or service benefits or claims relating to the transaction or the 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: 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

(6) To disclose in connection with the following:

1. 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;

2. The transfer of receivables, accounts or interests therein; or

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

191—90.14(505) Other exceptions to notice and opt-out requirements for disclosure of nonpublic personal financial information.

90.14(1) The requirements for initial notice to consumers in paragraph 90.3(1)*"b,"* for the opt out in rules 90.6(505) and 90.9(505), and for service providers and joint marketing in rule 90.12(505) do not apply when a licensee discloses nonpublic personal financial information as follows:

a. With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;

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

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

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

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

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

g. 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;

h. 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, 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, and 12 U.S.C. Chapter 21, a state insurance authority, and the Federal Trade Commission, self-regulatory organizations or for an investigation on a matter related to public safety;

i. To a consumer reporting agency in accordance with the federal Fair Credit Reporting Act;

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

k. 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 unit;

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

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

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

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

90.14(2) A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal financial information as permitted under subrule 90.6(7).

191—90.15(505) Notice through a Web site. If a licensee provides a notice on a Web site, the licensee shall comply with the above requirements 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. In addition, the licensee shall either place the notice on a screen that consumers frequently access, such as a page on which transactions are conducted, or place a link on a screen that consumers frequently access that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

191—90.16(505) Licensee exception to notice requirement.

90.16(1) A licensee is not subject to the notice and opt-out requirements for nonpublic personal financial information as follows:

a. The licensee is an employee, agent or other representative of another licensee; and

b. The other licensee otherwise complies with, and provides the notices required by, the provisions of the rules and the licensee does not disclose any nonpublic personal financial information to any person other than the other licensee or its affiliates in a manner permitted by these rules.

90.16(2) An excess lines broker or excess lines insurer shall be deemed to be in compliance with the notice and opt-out requirements for nonpublic personal financial information in these rules provided the following:

a. The broker or insurer does not disclose nonpublic personal financial information of a consumer or a customer to nonaffiliated third parties for any purpose including joint servicing or marketing under rule 90.12(505) except as permitted by rule 90.13(505) or 90.14(505); and

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

PRIVACY NOTICE

NEITHER THE U.S. BROKER 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.

DIVISION II
RULES FOR HEALTH INFORMATION

191—90.17(505) Disclosure of nonpublic personal health information.

90.17(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 whose nonpublic personal health information is sought to be disclosed.

90.17(2) Nothing in this rule shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a licensee or the licensee's insurance affiliate 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; rate-making 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.

191—90.18(505) Authorizations.

90.18(1) A valid authorization to disclose nonpublic personal health information pursuant to the health information rules as required under subrule 90.17(1) shall be in written or electronic form and shall contain all of 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 nonpublic personal health information to be disclosed;

c. 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;

d. 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

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

90.18(2) An authorization for the purposes of these health information rules shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than 24 months.

90.18(3) A consumer or customer who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to these health information rules at any time, subject to the rights of an individual who acted in reliance on the authorization prior to notice of the revocation.

90.18(4) A licensee shall retain the authorization or a copy in the record of the individual who is the subject of nonpublic personal health information.

191—90.19(505) Delivery of authorization request. 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 rule 90.8(505), 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 subrule 90.17(1).

191—90.20(505) Relationship to federal rules. Irrespective of whether a licensee is subject to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services, if a licensee complies with all requirements of the federal rules except for their effective date provision, the licensee shall not be subject to the provisions of these health information rules.

191—90.21(505) Relationship to state laws. Nothing in these health information rules shall preempt or supersede existing state law related to medical records, health or insurance information privacy.

191—90.22(505) Protection of Fair Credit Reporting Act. Nothing in these rules shall be construed to modify, limit or supersede the operations of the federal Fair Credit Reporting Act, and no inference shall be drawn on the basis of the provisions of these rules regarding whether information is transaction or experience information under Section 603 of that Act.

191—90.23(505) Nondiscrimination. A licensee shall not unfairly discriminate against any consumer or customer because that consumer or customer has opted out from the disclosure of the consumer's or customer's nonpublic personal financial information pursuant to the provisions of this chapter.

191—90.24(505) Severability. If any rule or portion of a rule of this chapter or its applicability to any person or circumstance is held invalid by a court, the remainder of the rules or the applicability of the provision to other persons or circumstances shall not be affected.

191—90.25(505) Penalties. An insurer or producer or licensee that violates a requirement of these rules shall be found to have committed a violation of Iowa Code section 507B.4 in addition to any other penalties provided by the laws of this state.

191—90.26(505) Effective dates.

90.26(1) These rules became effective November 13, 2000. However, in order to provide sufficient time for licensees to establish policies and systems to comply with the requirements of these rules, the commissioner extends the time for compliance until July 1, 2001.

90.26(2) A licensee shall provide by July 1, 2001, an initial notice as required by rule 90.3(505) to consumers who are the licensee's customers on July 1, 2001. 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.

90.26(3) Until July 1, 2002, a contract that a licensee has entered into with a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf satisfies the provisions of paragraph 90.12(1)*"a,"* even if the contract does not include a requirement that the third party maintain confidentiality of nonpublic personal financial information, provided that the licensee entered into the agreement on or before July 1, 2001.

90.26(4) The rules regarding health information are effective January 2, 2002, and no administrative action against noncompliance shall be taken until January 2, 2002.

191—90.27 to **90.36** Reserved.

DIVISION III
SAFEGUARDING CUSTOMER INFORMATION

191—90.37(505) Information security program.

90.37(1) Each licensee shall implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of customer information. The administrative, technical and physical safeguards included in the information security program shall be appropriate to the size and complexity of the licensee and the nature and scope of the licensee's activities.

90.37(2) A licensee's information security program shall be designed to:

a. Ensure the security and confidentiality of customer information;

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

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

191—90.38(505) Examples of methods of development and implementation. The actions and procedures that follow are examples of methods a licensee may use to implement the requirements of rule 191—90.37(505) to assess, manage and control risks of disclosure:

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

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

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

4. Design an information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the licensee's activities.

5. Train staff, as appropriate, to implement the licensee's information security program.

6. Regularly test or otherwise regularly monitor the key controls, systems and procedures of the information security program. The frequency and nature of these tests or other monitoring practices are determined by the licensee's risk assessment.

7. Exercise appropriate due diligence in selecting service providers.

8. Require service providers to implement appropriate measures designed to meet the objectives of rule 191—90.37(505) and, when indicated by the licensee's risk assessment, take appropriate steps to confirm that service providers have satisfied these obligations.

9. Monitor, evaluate and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of customer information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to customer information systems.

191—90.39(505) Penalties. An insurer, producer or licensee that violates a requirement of these rules shall be subject to the penalties imposed under Iowa Code chapter 507B in addition to any other penalties provided by the laws of this state.

191—90.40(505) Effective date. Each licensee shall establish and implement an information security program, including appropriate policies and systems, by June 30, 2003.

191—90.41 to **90.50** Reserved.

APPENDIX A
SAMPLE CLAUSES

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

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

A licensee may use this clause, as applicable, to meet the requirements of paragraph 90.5(1)*"a"* to describe the categories of nonpublic personal financial information the licensee collects.

Sample Clause A-1:

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

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

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

A licensee may use one of these clauses, as applicable, to meet the requirements of paragraph 90.5(1)*"b"* to describe the categories of nonpublic personal information the licensee discloses. The licensee may use these clauses if it discloses nonpublic personal information other than as permitted by the exceptions in rules 90.14(505), 90.15(505), and 90.16(505).

Sample Clause A-2, Alternative 1:

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

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

Sample Clause A-2, Alternative 2:

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

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

A licensee may use this clause, as applicable, to meet the requirements of paragraphs 90.5(1)*"b," "c,"* and *"d"* to describe the categories of nonpublic personal information about customers and former customers that the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses. A licensee may use this clause if the licensee does not disclose nonpublic personal information to any party, other than as permitted by the exceptions in rules 90.13(505) and 90.14(505).

Sample Clause A-3:

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

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

A licensee may use this clause, as applicable, to meet the requirements of paragraph 90.5(1)*"c"* to describe the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal information. This clause may be used if the licensee discloses nonpublic personal information other than as permitted by exceptions to rules 90.12(505), 90.13(505), and 90.14(505), as well as when permitted by the exceptions in rules 90.13(505) and 90.14(505).

Sample Clause A-4:

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

- Financial service providers, such as (provide illustrative examples, such as "life insurers, automobile insurers, mortgage bankers, securities broker-dealers, and insurance agents");
- Nonfinancial companies, such as (provide illustrative examples, such as "retailers, direct marketers, airlines, and publishers"); and
- Others, such as (provide illustrative examples, such as "nonprofit organizations").

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

A-5 Service provider/joint marketing exception

A licensee may use one of these clauses, as applicable, to meet the requirements of paragraph 90.5(1)*"e"* related to the exception for service providers and joint marketers in rule 90.12(505). If a licensee discloses nonpublic personal information under this exception, the licensee shall describe the categories of nonpublic personal information the licensee discloses and the categories of third parties with which the licensee has contracted.

Sample Clause A-5, Alternative 1:

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

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

Sample Clause A-5, Alternative 2:

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

A-6 Explanation of opt-out right (institutions that disclose outside of the exception)

A licensee may use this clause, as applicable, to meet the requirement of paragraph 90.5(1)*"f"* to provide an explanation of the consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the methods by which the consumer may exercise that right. The licensee may use this clause if the licensee discloses nonpublic personal information other than as permitted by the exceptions in rules 90.12(505), 90.13(505), and 90.14(505).

Sample Clause A-6:

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

A-7 Confidentiality and security (all institutions)

A licensee may use this clause, as applicable, to meet the requirement of paragraph 90.5(1)"*h*" to describe its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Sample Clause A-7:

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

These rules are intended to implement Iowa Code section 505.8, subsection 6, and P.L. 106-102.

[Filed emergency 11/9/00—published 11/29/00, effective 11/13/00]
[Filed 4/12/01, Notice 11/29/00—published 5/2/01, effective 7/1/01]
[Filed 11/2/01, Notice 8/8/01—published 11/28/01, effective 1/2/02]
[Filed 9/27/02, Notice 7/24/02—published 10/16/02, effective 11/20/02]
[Filed 2/28/03, Notice 1/22/03—published 3/19/03, effective 4/23/03]