Approved: 3-20-01
Date

MINUTES OF THE SENATE COMMITTEE ON FINANCIAL INSTITUTIONS AND INSURANCE.

The meeting was called to order by Chairperson Sandy Praeger at 9:30 a.m. on March 15, 2001 in Room 234-N of the Capitol.

All members were present except:

Committee staff present: Dr. Bill Wolff, Kansas Legislative Research Department
Ken Wilke, Office of the Revisor of Statutes
JoAnn Bunten, Committee Secretary

Conferees appearing before the committee:

Kathleen Sebelius, Kansas Commissioner of Insurance
Matthew D. All, Assistant Commissioner, Kansas Insurance Department
Reynold E. Becker, Vice President, Alliance of American Insurers
Ann M. Weber, General Counsel, National Association of Independent Insurers

Others attending: See attached list.

Hearing on HB 2480 - Adoption of model regulation concerning privacy of financial and health information of consumers

Kathleen Sebelius, Kansas Commissioner of Insurance, testified before the Committee in support of **HB 2480**. She pointed out that passage of the bill would protect the privacy of financial and health information of the consumer. The bill would also amend the Insurance Commissioner's authority to adopt privacy rules and regulations regarding the disclosure of nonpublic personal information described in Title V of the Gramm-Leach-Bliley Act of 1999. Commissioner Sebelius emphasized the fact that privacy belongs to the consumer and not the insurance companies, and she would like to see universal language adopted throughout the country to protect such privacy.

Matthew D. All, Assistant Commissioner, Kansas Insurance Department, by way of a power-point presentation, also testified in support of **HB 2480** and emphasized that this legislation would allow the Insurance Department to adopt strong, effective, privacy standards to protect consumers. He noted that insurance commissioners across the country determined that it would be important to develop a Model Regulation to deal with new challenges in privacy. The NAIC put together a working group last year which developed a Model Regulation which was passed by all insurance commissioners throughout the country. The Model Regulation would be (1) uniform from state to state; (2) generally uniform with the federal regulations; (3) translate Title V into insurance terminology and the realities of the insurance market; and (4) provide enhanced protection for health information, since insurers, unlike banks, are likely to have health information. Other facts relating to the Model Regulation were outlined in his written testimony. (Attachment 1) During Committee discussion KID noted that approximately 41 states may consider adopting the NAIC model, and that the privacy regulation is preferred by insurance commissioners throughout the country in order to keep uniformity state by state rather than by statute.

Speaking in opposition to **HB 2480** was Reynold E. Becker, Vice President, Alliance of American Insurers, who felt that this legislation would go far beyond the scope of GLBA, and the bill would explicitly sanction the use of the recently adopted National Association of Insurance Commissioners Model Privacy Regulation. He noted that the Alliance of American Insurers and its member companies oppose this explicit designation of the NAIC model regulation by name for three reasons: (1) the legislation would cede authority to KID; (2) should the NAIC amend their model regulation in the future, this would have the effect of bypassing constitutional roles in the process; and (3) the NAIC model regulation will place insurers writing in Kansas at a competitive disadvantage compared to banks and securities firms doing business in the state. (Attachment 2) Mr. Becker also provided a copy of the *Privacy of Consumer Financial and Health Information Regulation* to the Committee. (Attachment 3)

Ann M. Weber, General Counsel, National Association of Independent Insurers, also expressed her opposition to the bill. She noted that GLBA does not include health information privacy and therefore does not require any action on the state's part on this issue. Ms. Weber pointed out that the NAIC Model Privacy Regulation includes health information privacy provisions that are inconsistent with and not required for compliance with GLBA, and this is of grave concern to the NAII which could result in dual compliance standards for property/casualty insurers and confusion and frustration for the consumer. She further pointed out that workers' compensation coverage is included in the Model, and that the definition of "consumer" expressly references workers' compensation. GLBA excludes workers' compensation coverage in that it is limited to products or services used primarily for personal, family or household purposes. She felt that the Model goes beyond GLBA and adoption of the Model in Kansas would subject workers' compensation carriers and the businesses they insure to new privacy practices and procedures. Other concerns with the bill were outlined in her written testimony. (Attachment 4)

Ms. Weber also provided the Committee with a copy of a letter from D. Joseph Olson, Vice President and General Counsel of Amerisure Companies, to Commissioner Sebelius that expressed his concerns with the NAIC Model Privacy Regulation. (Attachment 5)

The Chair noted that because of the time, hearing on **HB 2480** would be continued next week.

Adjournment

The meeting was adjourned at 10:30 a.m. The next meeting of the Committee is scheduled for March 20 2001.

SENATE FINANCIAL INSTITUTIONS & INSURANCE COMMITTEE GUEST LIST

DATE: 3-15-01

Dr. NAME	REPRESENTING
David Hanson	NAII
Rey Becker	Alliance of American Insurers
Alan Weber	NAII
Carrie Donovan	NAII
Rick Gilliam	Health Midwest
Lee Wright	Farmers Ins
Chip Wheelen	Assn of Osteopathic Med.
Kyle Brock	Farm Bureau Mutual Ins Co.
Lou Ann Gebhards	SRS - Health Care Policy
Kevin Davis	Am Family Ins
Ken Hursh	Division of Workers Compensation
John Peterson	Security Benefit Group
Karrie Ann Rower	KAHP
Allen Mullen	Kathy Damron + Assoc
LARRY MAGILL	KAIA
ANNE SPIESS	KAIFA
Steve Montgomery	United Healthcare
Dick Lamprut	AARP
Darrell Donahue	AARP

SENATE FINANCIAL INSTITUTIONS & INSURANCE COMMITTEE GUEST LIST

DATE: 3-15-01

NAME	REPRESENTING
Roger Fraude	KGC
Chris Collins	KMS
Linda McCloskey	KY Ins. Dept
George Barbee	KAFS / CBA
Jeff Federico	Humana / CMK + Assoc
Brad Smoot	BCBS / AIA
BUD BURKE	AHIOS
Kathleen Sebelius	KID
Paul Davis	"
Matt All	"
Nancy Stanghaessy	Federico Consult.

Testimony on House Bill 2480
Before the Senate Committee on Financial Institutions & Insurance

MATTHEW D. ALL
Assistant Commissioner
Kansas Insurance Department
March 15, 2001

To the Chairperson and Members of the Committee:

Thank you for allowing me to testify this morning on House Bill No. 2480, which would allow the Kansas Insurance Department to adopt strong, effective, privacy standards to protect consumers financial and health information from disclosures by insurance companies.

You may ask why we should adopt privacy standards this legislative session. There are several answers to that question. First, protecting the privacy of consumers' personal financial and health information is crucial to upholding the fundamental Kansas values of individual integrity and dignity. We no not believe that this is an issue owned by either party or other political persuasion. All Kansans of all types care about protecting their personal information, and all Kansans deserve to have their personal information protected.

Second, Kansans' personal information is vulnerable to disclosure by insurance companies. Today there is no general, comprehensive Kansas law stopping an insurer from trading consumers' personal information. This is always been a problem, but with more advanced technology and a greater role for managed care in today's insurance market, the problem is much more serious today. These trends have made it much easier for insurers to concentrate and disclose consumers personal financial and health

information to anyone who seeks it. Moreover, new technology has set the stage for the growth of the target marketing industry, in which businesses compile personal information about consumers and sell consumer profiles to other businesses for the purposes of marketing. All of these things make protecting Kansans personal information more important today than ever before.

The immediate cause of this bill, however, is the passage of the Gramm-Leach-Bliley Act ("GLBA") in November 1999. GLBA advanced the concept of "financial services modernization" by breaking down many of the Depression-era barriers between banks, insurance companies, and securities firms. Because of GLBA, these financial institutions can affiliate within a financial holding company for the first time. Because each of these financial institutions possess large amounts of sensitive personal information, many in Congress became concerned about how these new financial conglomerates would concentrate, share, and disclose this information.

In response, Congress included privacy standards in Title V of GLBA. These privacy standards, however, are quite modest. They create an "opt-out" right for disclosure of consumer's private information to nonaffiliated third parties. That means that if a bank, insurance company, or securities firm wishes to disclose a consumers personal information to anyone except those other firms with whom they are affiliated, they must give the consumer an opportunity to opt-out of these disclosures.

To do this, the consumer would have to read the insurers' privacy notice included in a mailing or billing statement, recognize its meaning, and take the affirmative step of sending the form back to the financial institution making the disclosure. If a consumer failed to do that, that institution could share the consumer's personal information with the rest of the world.

In addition, Title V of GLBA allows information sharing without restriction between affiliated financial institutions. This creates the possibility that a consumer will find that his health information has been

disclosed to his bank without him having the opportunity to prevent the disclosure. Wisely, Congress made Title V a "federal floor," which allows states to enact their own privacy provisions, so long as those privacy provisions offer as much or more consumer protection than Title V.

You may remember that last legislative session you passed language that allowed the insurance commissioner to adopt regulations to implement Title V of GLBA. Commissioner Sebelius has begun that process. Financial privacy regulations pursuant to last year's legislation are in the works. The hearing on these regulations is set for April 16, and they will be effective July 1st.

But certain things have changed since you passed the grant of regulatory authority last session. Specifically, in May 2000 the federal agencies charged with enforcing Title V of GLBA upon banks and securities firms issued their final regulations. In addition to extending the compliance date for these regulations from November 2000 to July 2001, these regulations made clear that Title V of GLBA applies not only to financial information, but also to health information. This troubled many of us because it left health information with only the fairly modest protections of Title V – that is, an opt-out for health information and sharing between affiliates with no restrictions at all.

Insurance commissioners across the country determined that it would be important to develop a Model Regulation to deal with these new challenges in privacy. The NAIC put together a working group on privacy and named Commissioner Sebelius its chairperson. Last year, this working group set forth to develop a Model Regulation that would be (1) uniform from state to state; (2) generally uniform with the federal regulations; (3) translate Title V into insurance terminology and the realities of the insurance market; and (4) provide enhanced protection for health information, since insurers, unlike banks, are likely to have health information.

After months of public and industry input, the Model Regulation passed unanimously by all insurance commissioners, Republicans and Democrats, appointed and elected. In general, it mirrors Title V and the federal regulations implementing Title V for financial information. But it provides enhanced protection – an opt-in – for health information.

More specifically, for financial information, like Title V, the Model Regulation provides for an opt-out right for disclosures to nonaffiliated third parties. It allows disclosures to affiliated companies without restriction. It requires that companies give an opt-out notice to "consumers" – those who may have one-time or little contact – only if the insured is going to disclose that consumer's personal information. But companies are required to give notices more frequently to "customers" – those consumers with whom they have a continuing relationship – including an annual notice and initial notice.

For health information, the Model Regulation provides greater protection. It requires that companies obtain affirmative consent from consumers in advance if they intend to disclose personal information outside of a broad set of business and functional exceptions. These exceptions were developed in conjunction with the industry and should be enough to allow the industry to provide the services that Kansans need. In addition, the Model Regulation provides an exemption for the new health privacy regulations issued by the U.S. Department of Health and Human Services. That is, if an insurer must or simply prefers to comply with the standards set forth in these new federal regulations, that insurer will be deemed compliant with the Model Regulation. And, as you can see, we have also included an interim period of good faith compliance to allow companies to bring their privacy standards up to par with these new regulations.

One issue that you may hear about today from some opponents of this bill pertains to the definition of "consumer." What you must know about this issue is that Gramm-Leach-Bliley was a banking bill written by bankers in

the banking committee for banks. When we translated this statute into insurance terminology and the realities of the insurance market, we determined that it was necessary to include all individuals who use insurance products for personal, family or household purposes. This includes claimants and beneficiaries, and not just the direct consumers of these products. A workers compensation claimant, for example, who has had to give personal health information to a workers compensation insurer, would have that information protected by this regulation.

Put simply, we did this because we believe this information deserves protection. We believe working Kansans who are hurt or made sick on the job deserve to have their personal information protected. Some may argue that this will create an undue burden on the industry, but we simply do not believe it—and, frankly, neither does the vast bulk of the industry. What you must keep in mind is that these claimants and beneficiaries only receive protection under the Model Regulation when an insurer decides to disclose those consumers private information to nonaffiliated third parties. If they merely use the information within the normal course of their business, there is no regulatory burden whatsoever.

Another issue that opponents of privacy may put forward is a sunset on the health rules in the Model Regulation. Under this approach, the rules protecting Kansans' personal health information would expire once the HHS regulations take effect. This is a bad idea, and we oppose it strongly. Many—and perhaps most—of the licensees that would fall under the Model Regulation would not fall under the HHS regulations. Repealing the health portion of the Model Regulation would thus leave Kansans almost as vulnerable as before.

So why should you pass this bill? It's really quite simple: Kansans deserve this protection, and they need it. In addition, this Model Regulation is the only path to developing uniform privacy standards from state to state,

which is so crucial to avoiding an irrational, inefficient patchwork of standards.

If you pass this bill, you will be showing bipartisan leadership that will set an excellent example for the rest of the country.

The Model Regulation provides a balanced approach to privacy. It balances the needs of consumers and the realities of doing business in the insurance market.

Thank you for your time.

Protecting Kansans' Privacy

Testimony on House Bill 2480

Matthew D. All
Assistant Insurance Commissioner

Why should we adopt privacy standards now?

- Protecting personal information is crucial to fundamental Kansas values: individual integrity and dignity.
  - Not a Republican or Democratic, conservative or liberal issue.
  - All Kansans care about it.
  - All Kansans deserve it.

Why should we adopt privacy standards now?

- Kansans' personal information is vulnerable
  - Currently there is no general, comprehensive Kansas law stopping an insurer or bank from trading consumers' personal information.
  - New technology, concentration of information makes this even more of a problem.
  - Market for personal information.

1-7

Why should we adopt privacy standards now?

- Gramm-Leach-Bliley Act
  - Passed November 1999.
  - Advanced the concept of "financial services modernization" and "functional regulation."
  - Broke down Depression-Era barriers between banks, insurance companies, and securities firms.
  - Privacy concerns!

Why should we adopt privacy standards now?

- Title V of GLBA
  - Created "opt out" right for disclosures of consumers' private information to non-affiliated third parties.
  - But it allows affiliated companies to share consumers' private information freely.
  - Required state insurance commissioners to adopt regulations and enforce Title V upon insurers.
  - Created a "federal floor": it allowed states to offer more consumer protection, but not less.

So what did you do last year?

- Passed language that allowed the insurance commissioner to adopt regulations to implement Title V of GLBA.
- Financial privacy regulations are in the works.
  - Legislative hearing on March 19.
  - Regulatory hearing on April 16.
  - Effective July 1.

So what has changed?

- In May 2000, the federal agencies issued their final privacy regulations for banks and securities firms.
  - Extended compliance date from November 2000 to July 2001.
- The preamble to this regulation made clear that "nonpublic personal information" included health information.
  - Opt-out for health information!
  - Sharing with affiliates with no restrictions!

In the meantime . . .

- Insurance commissioners got together . . .
  - Put together a working group on privacy.
  - Developed a Model Regulation.
- Principles:
  - Uniformity from state to state.
  - Uniformity with federal regulations.
  - Translate Title V, federal regulations into insurance terminology.
  - Greater protection for health information.

What is the Model Regulation?

- Developed after months of public and industry input.
- Passed unanimously by all insurance commissioners.
  - Republican and Democrat
  - Appointed and elected
- Generally mirrors Title V, federal regs for financial information.
- Provides simple "opt in" for health information.

What does the Model Regulation do for financial information?

- Generally mirrors Title V, federal regs.
- Opt out for disclosures to non-affiliated third parties.
- No restrictions on disclosures to affiliates.
- Opt out notice for "consumers" only if insurer is going to disclose the information.
- Opt out notice for "customers" annually.

What does the Model Regulation do for health information?

- Greater protection.
- Opt in.
- Broad business and functional exceptions to allow the industry to provide service.
  - List developed in cooperation with industry.
  - Commissioner can add additional exceptions as needed.
- Exemption for HHS Regulations.
  - And a "good faith" period for health information.

Anything else you should know?

- Definition of "consumer"
  - Banking bill written by bankers in the banking committee for banks.
  - Had to conform to realities of insurance.
  - All individuals who use insurance products for personal, family, or household purposes.
  - Includes claimants and beneficiaries.
    - » Workers compensation claimants.
    - » Life insurance beneficiaries.

Why did we do that?

- We believe these individuals' information deserves protection.
  - Working Kansans who are hurt or made sick on the job deserve to have their personal information protected.
- Some will argue that this is a problem . . .
- Don't believe it.
  - These individuals only receive protection if an insurer decides to share their information with a non-affiliated third party.

Anything else?

- Sunset on health rules
  - Some may propose that, after HHS regs take effect, the Kansas health rules would expire.
- Really, really bad idea.
  - Many, perhaps most, licensees will not fall under the HHS regs.
  - This would leave Kansans vulnerable.

Any changes?

- A minor one.
- The effective date of the HHS regs has been delayed from February 26, 2003 to April 14, 2003.
  - February 26, 2002-03 are no longer relevant dates.
- It makes sense to change the effective date and the period for "good faith" compliance.
  - Effective date: February 1, 2002.
  - Good faith compliance period: February 1, 2002 – April 14, 2003.

1-11

Why should we pass this bill?

- Kansans deserve it, and need it.
- Uniformity.
  - Substantial majority of states will adopt Model Regulation.
- Bipartisan leadership.
- Balanced approach.

Who says it's a balanced approach?

- ACLI
  - September 27, 2000 statement of support by President and CEO Carroll Campbell: "The bottom line is that the NAIC model balances consumers' competing demands for financial and medical information privacy and the benefits resulting from responsible information sharing."

Who else?

- The Council of Insurance Agents & Brokers, Independent Insurance Agents of America, National Association of Insurance and Financial Advisers, National Association of Professional Insurance Agents.
  - September 26, 2000 joint letter: "We … appreciate your willingness to work with the industry to draft a product that not only provides meaningful protections for consumers' private financial and health information, but that still allows the industry to [be] able to perform the services and functions that are necessary to the sale and servicing of insurance policies for consumers. We believe this regulation represents a thoughtful and balanced approach."

Anyone else?

- Prudential
  - November 10, 2000 letter: "A uniform, national approach, such as that suggested in the NAIC model regulation, would ensure that insurers and our customers not be disadvantaged by a costly patchwork of differing state laws."
- AIA
  - September 28, 2000 testimony to NCOIL: "There is a simple solution to the federal challenge, providing NCOIL an opportunity to perform an enlightened leadership role in the states. The solution would recognize the achievement of the NAIC in fashioning a practical model regulation addressing privacy protection in detail …."

Anyone else?

- AARP
- AFL-CIO
- Others . . .

Questions?

Alliance
of American Insurers®

TESTIMONY ON HOUSE BILL 2480
KANSAS SENATE FINANCIAL INSTITUTIONS & INSURANCE COMMITTEE
MARCH 15, 2001

REYNOLD E. BECKER
VICE PRESIDENT-PROPERTY/CASUALTY
ALLIANCE OF AMERICAN INSURERS

The Alliance of American Insurers is a national trade association with 326 property/casualty insurance company members. Alliance members write both personal and commercial lines policies in Kansas. Thank you for the opportunity to speak as to House Bill 2480.

The Department Already Has Necessary Authority

Both Alliance member companies and the insurance consumers of Kansas need regulations in place to implement the *financial* privacy provisions of the Gramm-Leach-Bliley (GLB) Act. Last year, the Legislature wisely gave the Insurance Department all the authority it needs to adopt such regulations under K.S.A. 40-2404(15). Why are we here today?

The Department Wants to Bypass the Legislature & Disadvantage Insurers

We are here today because the Department would like to adopt regulations that go far beyond the scope of GLB. HB 2480 would explicitly sanction the use of the recently adopted National Association of Insurance Commissioners (NAIC) model privacy regulation. The Alliance and its member companies oppose this explicit designation of the NAIC model regulation by name for three reasons:

- This approach asks you as legislators to cede your authority to the department. For an issue this controversial, it is almost unheard of to incorporate a mere model *regulation* by reference into the Kansas statute books.
- Should the NAIC amend their model *regulation* in the future, this would have the effect of bypassing your constitutional roles in the process.
- The NAIC model regulation will place insurers writing in Kansas at a competitive disadvantage compared to banks and securities firms doing business in the state, who face no similar over-reaching regulations at the federal level. Since your committee also handles financial institution issues, we urge you to maintain a level playing field.

What Are Other States Doing?

To date, 12 state insurance departments have published versions of the NAIC model regulation. Half of them have either deleted the health information privacy component or have decided to run the issue on a separate track. Three have taken-out workers compensation.

Four other legislatures, including Missouri, are following your lead from last year and are moving legislation to give their own departments similar focused authority. The wisdom of the approach has gained momentum.

Senate Financial Inst. & Insurance
Date: 3-15-01
Attachment No. 2

What Should You Do About HB 2480?

Obviously, the Alliance and its member companies prefer that the bill be withdrawn. We continue in our willingness to work with the Department on regulations that comply with both the letter and spirit of GLB.

If the will of the committee is to approve the bill, we recommend two simple amendments to make the measure more cost-effective and workable:

- GLB provides no authority to regulate health information privacy. Further, the U.S. Department of Health and Human Services (HHS) medical records privacy rules will not take effect until mid-April of 2003. Any Kansas-specific health information regulations should be delayed for *at least* two years, until the HHS rules take effect. To do otherwise is to invite conflicts and the extra expense of premature compliance. Two years will allow plenty of time for insurers, healthcare providers, the department and legislators to craft reasonable and consistent approaches.
- GLB was never intended to apply to commercial insurance. Nevertheless, if the *Insurance* Department wishes the regulations to cover the handling of workers compensation, it is only reasonable to require that such regulations be issued jointly with the Division of *Workers Compensation,* since, *by statute,* that is the agency that administers the workers compensation system.

Before allowing the Insurance Department to impose costly mandates upon insurers and their customers, both individuals and employers, we ask the committee to consider these reasonable suggested amendments. The Alliance and its members look forward to the opportunity to work with you on this effort.

G:\PERSLINE\REB\REB2001\KSPRIVACYTESTIMONY.DOC

Adopted by the NAIC on September 26, 2000

PRIVACY OF CONSUMER FINANCIAL AND HEALTH INFORMATION REGULATION

Table of Contents

Senate Financial Inst. & Insurance
Date: 3-15-01
Attachment No. 3

ARTICLE V. RULES FOR HEALTH INFORMATION

ARTICLE VI. ADDITIONAL PROVISIONS

ARTICLE I. GENERAL PROVISIONS

Section 1. Authority

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

Section 2. Purpose and Scope

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

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

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

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

B. Scope. This regulation applies to:

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

(2) All nonpublic personal health information.

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

Drafting Note: Subsection 2C is intended to give licensees some guidance for complying with Title V of the Gramm-Leach-Bliley Act in those states that do not have laws or regulations that meet GLBA's privacy requirements.

Section 3. Rule of Construction

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

Section 4. Definitions

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

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

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

(2) Examples.

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

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

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

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

(iv) Avoids multiple negatives;

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

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

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

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

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

(iii) Provides wide margins and ample line spacing;

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

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

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

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

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

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

D. "Commissioner" means the insurance commissioner of the state.

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

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

F. (1) "Consumer" 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 that individual's legal representative.

(2) Examples.

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

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

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

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

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

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

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

(IV) the individual is a mortgagor of a mortgage covered under a mortgage insurance policy;

and

(ii) the licensee discloses nonpublic personal financial information about the individual to a nonaffiliated third party other than as permitted under Sections 14, 15 and 16 of this regulation.

(e) Provided that the licensee provides the initial, annual and revised notices under Sections 5, 6 and 9 of this regulation to the plan

sponsor, group or blanket insurance policyholder or group annuity contractholder, workers' compensation plan participant, and further provided that the licensee does not disclose to a nonaffiliated third party nonpublic personal financial information about such an individual other than as permitted under Sections 14, 15 and 16 of this regulation, an individual is not the consumer of the licensee solely because he or she is:

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

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

(iii) A beneficiary in a workers' compensation plan.

Drafting Note: Regulators may wish to urge their workers' compensation state insurance fund (or other applicable agency) to promulgate a regulation similar to this regulation in order to ensure parity in treatment of workers' compensation plans and to ensure that all workers covered by such plans have privacy protections.

(f) (i) The individuals described in Subparagraph (e)(i) through (iii) of this Paragraph are consumers of a licensee if the licensee does not meet all the conditions of Subparagraph (e).

(ii) In no event shall the individuals, solely by virtue of the status described in Subparagraph (e)(i) through (iii) above, be deemed to be customers for purposes of this regulation.

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

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

G. "Consumer reporting agency" has the same meaning as in Section 603(f) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(f)).

H. "Control" means:

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

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

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

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

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

(2) Examples.

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

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

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

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

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

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

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

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

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

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

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

(viii) For the purposes of this regulation, the individual's last known address according to the licensee's records is deemed invalid. An address of record is deemed invalid if mail sent to that address by the licensee has been returned by the postal authorities as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.

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

(2) Financial institution does not include:

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

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

(iii) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as the institutions do not

sell or transfer nonpublic personal information to a nonaffiliated third party.

L. (1) "Financial product or service" means any product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under Section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

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

M. "Health care" means:

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

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

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

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

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

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

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

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

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

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

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

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

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

(2) A licensee is not subject to the notice and opt out requirements for nonpublic personal financial information set forth in Articles I, II, III and IV of this regulation if the licensee is an employee, agent or other representative of another licensee ("the principal") and:

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

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

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

(b) An excess lines broker or excess lines insurer shall be deemed to be in compliance with the notice and opt out requirements for nonpublic personal financial information set forth in Articles I, II, III and IV of this regulation provided:

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

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

PRIVACY NOTICE

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

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

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

(a) A licensee's affiliate; or

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

(2) Nonaffiliated third party includes any company that is an affiliate solely by virtue of the direct or indirect ownership or control of the company by the licensee or its affiliate in conducting merchant banking or investment banking activities of the type described in Section 4(k)(4)(H) or insurance company investment activities of the type described in Section 4(k)(4)(I) of the federal Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).

S. "Nonpublic personal information" means nonpublic personal financial information and nonpublic personal health information.

T. (1) "Nonpublic personal financial information" means:

(a) Personally identifiable financial information; and

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

(2) Nonpublic personal financial information does not include:

(a) Health information;

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

(c) Any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available.

(3) Examples of lists.

(a) Nonpublic personal financial information includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information that is not publicly available, such as account numbers.

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

U. "Nonpublic personal health information" means health information:

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

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

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

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

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

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

(2) Examples.

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

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

(ii) Account balance information and payment history;

(iii) The fact that an individual is or has been one of the licensee's customers or has obtained an insurance product or service from the licensee;

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

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

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

(vii) Information from a consumer report.

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

(i) Health information;

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

(iii) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names or addresses.

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

(a) Federal, state or local government records;

(b) Widely distributed media; or

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

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

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

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

(3) Examples.

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

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

(c) Reasonable basis.

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

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

ARTICLE II. PRIVACY AND OPT OUT NOTICES FOR FINANCIAL INFORMATION

Section 5. Initial Privacy Notice to Consumers Required

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

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

(2) 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.

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

(1) The licensee does not disclose any nonpublic personal financial information about the consumer to any nonaffiliated third party, other than as authorized by Sections 15 and 16, and the licensee does not have a customer relationship with the consumer; or

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

C. When the licensee establishes a customer relationship.

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

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

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

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

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

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

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

E. Exceptions to allow subsequent delivery of notice.

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

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

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

(2) Examples of exceptions.

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

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

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

F. Delivery. When a licensee is required to deliver an initial privacy notice by this section, the licensee shall deliver it according to Section 10. If the licensee uses a short-form initial notice for non-customers according to Section 7D, the licensee may deliver its privacy notice according to Section 7D(3).

Section 6. Annual Privacy Notice to Customers Required

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

(2) Example. A licensee provides a notice annually if it defines the twelve-consecutive-month period as a calendar year and provides the annual notice to the customer once in each calendar year following the calendar year in which the licensee provided the initial notice. For example, if a customer opens an account on any day of year 1, the licensee shall provide an annual notice to that customer by December 31 of year 2.

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

(2) Examples.

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

(b) A licensee no longer has a continuing relationship with an individual if the individual's policy is lapsed, expired or otherwise inactive or dormant under the licensee's business practices, and the licensee has not communicated with the customer about the relationship for a period of twelve (12) consecutive months, other

than to provide annual privacy notices, material required by law or regulation, or promotional materials.

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

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

D. Delivery. When a licensee is required by this section to deliver an annual privacy notice, the licensee shall deliver it according to Section 10.

Section 7. Information to be Included in Privacy Notices

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

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

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

(3) The categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal financial information, other than those parties to whom the licensee discloses information under Sections 15 and 16;

(4) The categories of nonpublic personal financial information about the licensee's former customers that the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal financial information about the licensee's former

customers, other than those parties to whom the licensee discloses information under Sections 15 and 16;

(5) If a licensee discloses nonpublic personal financial information to a nonaffiliated third party under Section 14 (and no other exception in Sections 15 and 16 applies to that disclosure), a separate description of the categories of information the licensee discloses and the categories of third parties with whom the licensee has contracted;

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

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

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

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

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

C. Examples.

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

(a) Information from the consumer;

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

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

(d) Information from a consumer reporting agency.

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

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

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

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

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

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

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

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

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

(b) Types of businesses may be described by general terms only if the licensee uses a few illustrative examples of significant lines of business. For example, a licensee may use the term financial

products or services if it includes appropriate examples of significant lines of businesses, such as life insurer, automobile insurer, consumer banking or securities brokerage.

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

(4) Disclosures under exception for service providers and joint marketers. If a licensee discloses nonpublic personal financial information under the exception in Section 14 to a nonaffiliated third party to market products or services that it offers alone or jointly with another financial institution, the licensee satisfies the disclosure requirement of Subsection A(5) of this section if it:

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

(b) States whether the third party is:

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

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

(5) Simplified notices. If a licensee does not disclose, and does not wish to reserve the right to disclose, nonpublic personal financial information about customers or former customers to affiliates or nonaffiliated third parties except as authorized under Sections 15 and 16, the licensee may simply state that fact, in addition to the information it shall provide under Subsections A(1), A(8), A(9), and Subsection B of this section.

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

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

(b) States whether the licensee has security practices and procedures in place to ensure the confidentiality of the information in accordance

with the licensee's policy. The licensee is not required to describe technical information about the safeguards it uses.

D. Short-form initial notice with opt out notice for non-customers.

(1) A licensee may satisfy the initial notice requirements in Sections 5A(2) and 8C 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.

(2) A short-form initial notice shall:

(a) Be clear and conspicuous;

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

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

(3) The licensee shall deliver its short-form initial notice according to Section 10. The licensee is not required to deliver its privacy notice with its short-form initial notice. The licensee instead may simply provide the consumer a reasonable means to obtain its privacy notice. If a consumer who receives the licensee's short-form notice requests the licensee's privacy notice, the licensee shall deliver its privacy notice according to Section 10.

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

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

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

E. Future disclosures. The licensee's notice may include:

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

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

F. Sample clauses. Sample clauses illustrating some of the notice content required by this section are included in Appendix A of this regulation.

Section 8. Form of Opt Out Notice to Consumers and Opt Out Methods

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

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

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

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

(2) Examples.

(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:

(i) Identifies all of the categories of nonpublic personal financial information that it discloses or reserves the right to disclose, and all of the categories of nonaffiliated third parties to which the licensee discloses the information, as described in Section 7A(2) and (3), and states that the consumer can opt out of the disclosure of that information; and

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

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

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

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

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

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

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

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

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

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

B. Same form as initial notice permitted. A licensee may provide the opt out notice together with or on the same written or electronic form as the initial notice the licensee provides in accordance with Section 5.

C. Initial notice required when opt out notice delivered subsequent to initial notice. If a licensee provides the opt out notice later than required for the initial notice in accordance with Section 5, the licensee shall also include a copy of the initial notice with the opt out notice in writing or, if the consumer agrees, electronically.

D. Joint relationships.

(1) If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may provide a single opt out notice. The licensee's opt out notice shall explain how the licensee will treat an opt out direction by a joint consumer (as explained in Paragraph (5) of this subsection).

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

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

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

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

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

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

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

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

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

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

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

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

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

F. Continuing right to opt out. A consumer may exercise the right to opt out at any time.

G. Duration of consumer's opt out direction.

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

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

H. Delivery. When a licensee is required to deliver an opt out notice by this section, the licensee shall deliver it according to Section 10.

Section 9. Revised Privacy Notices

A. General rule. Except as otherwise authorized in this 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, unless:

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

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

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

(4) The consumer does not opt out.

B. Examples.

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

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

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

G. Joint relationships. If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may satisfy the initial, annual and revised notice requirements of Sections 5A, 6A and 9A, respectively, by providing one notice to those consumers jointly.

ARTICLE III. LIMITS ON DISCLOSURES OF FINANCIAL INFORMATION

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

A. (1) Conditions for disclosure. Except as otherwise authorized in this 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:

(a) The licensee has provided to the consumer an initial notice as required under Section 5;

(b) The licensee has provided to the consumer an opt out notice as required in Section 8;

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

(d) The consumer does not opt out.

(2) Opt out definition. Opt out means a direction by the consumer that the licensee not disclose nonpublic personal financial information about that consumer to a nonaffiliated third party, other than as permitted by Sections 14, 15 and 16.

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

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

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

days after the date that the customer acknowledges receipt of the notices in conjunction with opening the account.

(c) Isolated transaction with consumer. For an isolated transaction such as providing the consumer with an insurance quote, a licensee provides the consumer with a reasonable opportunity to opt out if the licensee provides the notices required in Paragraph (1) of this subsection at the time of the transaction and requests that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction.

B. Application of opt out to all consumers and all nonpublic personal financial information.

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

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

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

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

A. (1) Information the licensee receives under an exception. If a licensee receives nonpublic personal financial information from a nonaffiliated financial institution under an exception in Sections 15 or 16 of this regulation, the licensee's disclosure and use of that information is limited as follows:

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

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

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

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

B. (1) Information a licensee receives outside of an exception. If a licensee receives nonpublic personal financial information from a nonaffiliated financial institution other than under an exception in Sections 15 or 16 of this regulation, the licensee may disclose the information only:

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

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

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

(2) Example. If a licensee obtains a customer list from a nonaffiliated financial institution outside of the exceptions in Sections 15 or 16:

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

(b) The licensee may disclose that list to another nonaffiliated third party only if the financial institution from which the licensee purchased the list could have lawfully disclosed the list to that third party. That is, the licensee may disclose the list in accordance with the privacy policy of the financial institution from which the licensee received the list, as limited by the opt out direction of each consumer whose nonpublic personal financial information the licensee intends to disclose, and the licensee may disclose the list in accordance with an exception in Sections 15 or 16, such as to the licensee's attorneys or accountants.

C. Information a licensee discloses under an exception. If a licensee discloses nonpublic personal financial information to a nonaffiliated third party under an

exception in Sections 15 or 16 of this regulation, the third party may disclose and use that information only as follows:

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

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

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

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

(1) To the licensee's affiliates;

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

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

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

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

B. Exceptions. Subsection A of this section does not apply if a licensee discloses a policy number or similar form of access number or access code:

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

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

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

C. Examples.

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

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

ARTICLE IV. EXCEPTIONS TO LIMITS ON DISCLOSURES OF FINANCIAL INFORMATION

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

A. General rule.

(1) The opt out requirements in Sections 8 and 11 do not apply when a licensee provides nonpublic personal financial information to a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf, if the licensee:

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

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

(2) Example. If a licensee discloses nonpublic personal financial information under this section to a financial institution with which the licensee performs joint marketing, the licensee's contractual agreement with that institution meets the requirements of Paragraph (1)(b) of this subsection if it prohibits the institution from disclosing or using the nonpublic personal financial information except as necessary to carry out the joint marketing

or under an exception in Sections 15 or 16 in the ordinary course of business to carry out that joint marketing.

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

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

Section 15. Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Financial Information for Processing and Servicing Transactions

A. Exceptions for processing transactions at consumer's request. The requirements for initial notice in Section 5A(2), the opt out in Sections 8 and 11, and service providers and joint marketing in Section 14 do not apply if the licensee discloses nonpublic personal financial information as necessary to effect, administer or enforce a transaction that a consumer requests or authorizes, or in connection with:

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

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

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

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

B. "Necessary to effect, administer or enforce a transaction" means that the disclosure is:

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

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

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

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

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

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

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

(f) In connection with:

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

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

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

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

A. Exceptions to opt out requirements. The requirements for initial notice to consumers in Section 5A(2), the opt out in Sections 8 and 11, and service providers and joint marketing in Section 14 do not apply when a licensee discloses nonpublic personal financial information:

(1) With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;

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

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

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

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

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

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

(4) To the extent specifically permitted or required under other provisions of law and in accordance with the federal Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), to law enforcement agencies (including the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, the Securities and Exchange Commission, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping), a state insurance authority, and the Federal Trade Commission), self-regulatory organizations or for an investigation on a matter related to public safety;

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

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

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

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

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

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

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

B. Example of revocation of consent. A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under Section 8F.

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

ARTICLE V. RULES FOR HEALTH INFORMATION

Section 17. When Authorization Required for Disclosure of Nonpublic Personal Health Information

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

B. Nothing in this section shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a licensee for the performance of the following insurance functions by or on behalf of the licensee: claims administration; claims adjustment and management; detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity; underwriting; policy placement or issuance; loss control; ratemaking and guaranty fund functions; reinsurance and excess loss insurance; risk management; case management; disease management; quality assurance; quality improvement; performance evaluation; provider credentialing verification; utilization review; peer review activities; actuarial, scientific, medical or public policy research; grievance procedures; internal administration of compliance, managerial, and information systems; policyholder service functions; auditing; reporting; database security; administration of consumer disputes and inquiries;

external accreditation standards; the replacement of a group benefit plan or workers compensation policy or program; activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit; any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services; disclosure that is required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes; and any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with legal process. Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable to the interest of consumers.

Section 18. Authorizations

A. A valid authorization to disclose nonpublic personal health information pursuant to this Article V shall be in written or electronic form and shall contain all of the following:

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

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

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

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

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

B. An authorization for the purposes of this Article V shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than twenty-four (24) months.

C. A consumer or customer who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to this Article V at

any time, subject to the rights of an individual who acted in reliance on the authorization prior to notice of the revocation.

D. A licensee shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information.

Section 19. Authorization Request Delivery

A request for authorization and an authorization form may be delivered to a consumer or a customer as part of an opt-out notice pursuant to Section 10, 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 17A.

Section 20. Relationship to Federal Rules

Irrespective of whether a licensee is subject to the federal Health Insurance Portability and Accountability Act privacy rule as promulgated by the U.S. Department of Health and Human Services [insert cite] (the "federal rule"), if a licensee complies with all requirements of the federal rule except for its effective date provision, the licensee shall not be subject to the provisions of this Article V.

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

Section 21. Relationship to State Laws

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

ARTICLE VI. ADDITIONAL PROVISIONS

Section 22. Protection of Fair Credit Reporting Act

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

Section 23. Nondiscrimination

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

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

Section 24. Violation

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

Section 25. Severability

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

Section 26. Effective Date

A. Effective date. This regulation is effective November 13, 2000. In order to provide sufficient time for licensees to establish policies and systems to comply with the requirements of this regulation, the commissioner has extended the time for compliance with this regulation until July 1, 2001.

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

(2) Example. A licensee provides an initial notice to consumers who are its customers on July 1, 2001, if, by that date, the licensee has established a system for providing an initial notice to all new customers and has mailed the initial notice to all the licensee's existing customers.

C. Two-year grandfathering of service agreements. Until July 1, 2002, a contract that a licensee has entered into with a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf satisfies the provisions of Section 14A(1)(b) of this regulation, even if the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information, as long as the licensee entered into the agreement on or before July 1, 2000.

information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right. The licensee may use this clause if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections 14, 15 and 16.

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 Section 7A(8) 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.

National Association of Independent Insurers

2600 River Road, Des Plaines, IL 60018-3286

ANN M. WEBER
COUNSEL

March 15, 2001

Chairperson Sandy Praeger
Senate Insurance Committee
State House
Topeka, KS 66612

RE: HB 2480

Dear Madam Chair and Members of the Insurance Committee:

The NAII represents hundreds of property/casualty insurers doing business in Kansas. These companies provide approximately 38% of the state's property/casualty insurance coverage. NAII respectfully submits to you and the members of the House Insurance Committee NAII's position on HB 2480 which includes the NAIC Model Regulation.

As you may know, the NAII joined the Alliance of American Insurers, the American Association of Health Plans and the Health Insurance Association of America in opposing adoption of the NAIC Model. We believe the Model is not the route to follow in Kansas and the reasons for our opposition are outlined below.

First and foremost of the NAII's concerns in the Model is the inclusion of health information privacy standards (Article V). GLB does not include health information privacy and therefore does not require any action on the states' part on this issue. Nevertheless, the NAIC Model includes health information privacy provisions that are inconsistent with and not required for compliance with GLB. This is of grave concern to the NAII. It could result in dual compliance standards for property/casualty insurers and confusion and frustration for the consumer. The dual compliance issue arises from regulations on health information privacy promulgated by the United States Department of Health and Human Services. While these regulations do not impact property/casualty insurers directly, they probably will do so indirectly. Many people with whom or entities with which property/casualty insurers contract or otherwise do business with clearly fall within the federal regulations.

Phone: (847) 297-7800 FAX: (847) 297-5064
FAX on demand: 1-800-291-0229 Web site: http://www.naii.or

Senate Financial Inst. & Insurance
Date: 3-15-01
Attachment No. 4

Entities directly regulated by the HHS rules will have to insist that the property/casualty insurers comply with the federal health information standards in order to do business with those insurers. This will entail costs for insurers and these costs will be passed along to consumers. It most likely also entails problems for the consumer such as multiple authorization forms for release of the same information, duplicate but inconsistent notices on privacy protection policies, and delay in claims payment because necessary information takes longer to obtain. In addition, the Model is not limited to sharing of health information with nonaffiliated third parties for marketing purposes, as is GLB for financial information.

Second, workers' compensation coverage is included in the Model. The definition of "consumer" expressly references workers' compensation (Section 4 F [2] [e]). GLB excludes workers' compensation coverage in that it is limited to products or services used primarily for personal, family or household purposes. The Model goes beyond GLB and adoption of the Model in Kansas will subject workers' compensation carriers and the businesses they insure to new privacy practices and procedures.

Third, the Model may create new producer liability. Section 4 Q (2)(a) states that a producer is not subject to the notice and opt out requirements of the Model if the principal otherwise complies with, and provides the notices required by, the Model. How is a producer to know if all insurers with which the producer has an appointment are in compliance with the Model?

Fourth, the definition of "consumer" in Section 4 F is broad enough to include third party claimants. A third party claimant is an individual that seeks to obtain, obtains or obtained an insurance service. The examples make quite clear that an individual is a consumer if he or she is a claimant under an insurance policy (Section 4 F [2][d][II]). This will require the insurer to provide a notice of its privacy policies and practices as well as an opportunity to "opt out" to all third party claimants before it discloses nonpublic personal financial information to nonaffiliated third parties.

Fifth, we find the prohibitions in Section 23 dealing with unfair discrimination unclear. In the usual insurance context, "unfair discrimination" involves an action not actuarially justified or not supported by sound business judgment. Is that what is meant by this language? If so, that should be specified or a court interpreting the language could give it a different meaning.

Finally, and with all due respect, Kansas law adopted last year does not allow the regulatory authority to adopt the Model as the NAIC Model Regulation goes far beyond the requirements of GLB (as discussed above).

The above critique of the Model being said, the NAII recognizes that all of us are concerned about the privacy of health information. If the committee concludes that health must be included in the Act we respectfully submit that there is a better approach than the NAIC Model. However, as part of this discussion, it is always important to keep in mind the broader objective of GLB: the lowering and/or removal of artificial barriers between and among banks, insurers and securities firms. The Model fails in this important objective in that it adds additional layers of compliance for state regulated insurers.

The NAII does support a strong, uniform standard for protecting the confidentiality of personally identifiable consumer financial information. We believe consumers and the industry will be best served if there are consistent standards for how information is protected and with respect to the disclosure of that information. Therefore, we generally support and appreciate the fact that the National Conference of Insurance Legislators (NCOIL) recognized the need for uniformity and took an approach consistent with the federal rules in order to implement and enforce GLB. As legislators interested in the economic development and well being of their states, NCOIL felt it was important that whatever they do, they maintain parity between and among the various branches of the financial services industry, so that all have a "level playing field."

NCOIL accomplished this in several ways. For example, we believe that NCOIL appropriately excluded commercial lines from the scope of their model. Title V of GLB applies to personally identifiable financial information derived from transactions where individuals have obtained a financial product, including insurance, for personal, family or household use. When translated into the context of insurance, this was intended by Congress to regulate privacy practices as to personal line applicants or policyholders, not commercial line policies. Thus, the approach taken by NCOIL is consistent with that taken by relevant federal agencies as to banks and securities firms, thereby maintaining parity and promoting a level playing field.

Another example is the way NCOIL will treat health information privacy. Although we do not believe that health information privacy should be included, we do believe that the approach taken in the NCOIL model better conforms to the general underlying objectives of GLB's Title V. The NCOIL approach addresses specific concerns about the disclosure of health information, absent affirmative consent by the consumer (i.e. opt-in), to non-affiliated third parties for use in marketing of products or services. We believe that to go beyond this standard would create significant challenges for insurers faced with complying with GLB.

Thank you again for this opportunity to comment.

Sincerely,

Ann M. Weber

Ann M. Weber

AMW/rp

cc: NAII members doing business in Kansas
Robert Zeman
Michael Duncan
Bill Bradford

h:\Legal\Weber\Kansas\ks Praeger NAII Privacy ltr.doc

Amerisure® Companies

Michigan Mutual Insurance Company

Amerisure, Inc.
Amerisure Insurance Company
Amerisure Re (Bermuda) Ltd.

D. JOSEPH OLSON
Senior Vice President and General Counsel

March 8, 2001

Kathleen Sebelius
Commissioner of Insurance
Kansas Insurance Department
420 SW 9th St.
Topeka, KS 66612-1678

RE: NAIC Model Privacy of Consumer Financial and Health Information Regulation

Dear Kathleen:

I understand that Terri Vaughan spoke with you at the NCOIL meeting in Hilton Head last week about my concerns about the manner in which the NAIC Model Privacy Regulation impacts the operations of commercial lines insurers. I am sorry I did not have the opportunity to speak to you at the meeting, but after the privacy hearing was delayed, I switched to an earlier flight and returned to my office in Michigan. (Otherwise, I would have had to wait until the next day to leave.)

The problems that Amerisure has encountered in its study of compliance with the NAIC Model appear to arise from the fact that workers' compensation beneficiaries and third party claimants were added to the definition of "consumer" appearing in the Gramm-Leach-Bliley Act (GLB), but the model does not make adjustments in the GLB "disclosure exceptions," appearing in GLB Section 502(e) and in the definition of "necessary to effect, administer, or enforce" in GLB Section 509(7), that would be appropriate in light of the different ways in which commercial lines insurers interact with their customers, in contrast to insurers issuing policies for "personal, family, or household purposes." Perhaps this would become more clear if I briefly described some of the ways in which the Amerisure Insurance Companies do business.

With the possible exception of an automobile policy issued to a bank in Michigan covering its employees' automobiles, Amerisure is exclusively a commercial lines insurer. We specialize in mid-market risks (approximately $50,000 - $500,000 annual premium) in the manufacturing and contracting areas, although we do occasionally write outside of those areas and for smaller or larger customers. Approximately ½ of our business is workers' compensation, much of it written on a large deductible or loss sensitive basis. In addition, much of our commercial auto and general liability business (whether written separately or as part of a package) is also experience-rated. Thus, with

Senate Financial Inst. & Insurance
Date: 3-15-01
Attachment No. 5

respect to many of our claims (high deductible and retroactively rated workers' compensation policies, for example), we're using what is ultimately the insured's money when we pay a claim. Even when the policy is simply experience-rated, the number and amount of losses will obviously impact our insureds' premiums.

For this reason, our insureds are intensely, and justifiably, interested in our decisions with respect to contesting, settling or paying claims. Many of our larger customers insist upon periodic meetings to discuss the status and handling of all pending claims. And, of course, after we have paid a claim under the deductible in a workers' compensation policy and ask to be reimbursed by the insured, that customer obviously needs to be comfortable that our payment was appropriate. In short, we need to be able to disclose claims information to our customers and to their and our agents.

Unfortunately, under the definitions in the NAIC Model, these agents and insureds are nonaffiliated third parties. If we are going to disclose information that meets the definition of "nonpublic personal financial information," and there is not much information collected in the loss adjustment process that does not meet that definition (except for health information), we may need to notify workers' compensation beneficiaries and third party claimants that we are releasing such information to these nonaffiliated third parties, giving them the opportunity to opt-out of such disclosure. Because of the adversarial position in which we find ourselves with respect to these beneficiaries and claimants, and the fact that they are usually represented by counsel, opt-outs can be expected, making it difficult for us to provide proper service to our insureds.

Of course, there are exceptions in the model regulation for such disclosures, appearing in sections 14, 15 and 16. Unfortunately, these are the exceptions that have not been modified to reflect the realities of providing proper service to commercial lines insureds. For example, Section 15 permits disclosures to nonaffiliated third parties "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 authorized . . . [emphasis added]"; the only "consumer" involved in our claims is the beneficiary or claimant. Further complicating the matter is the definition of "necessary to effect, administer or enforce," because with respect to claims, subpart B.(2)(e) indicates that the term means the disclosure is required, or is a usual, appropriate or acceptable method "to underwrite insurance at the consumer's request or for any of the following purposes as they relate to a consumer's insurance [emphasis added]: . . . processing insurance claims . . . "

It seems obvious to me that this language does not authorize an "unopt-outable" disclosure (that is, one from which the consumer cannot opt-out), because it would not relate to a consumer's insurance; it is our commercial lines insured's insurance, and that insured does not meet the definition of consumer. (Also, "processing insurance claims" is not quite clear.)

I think the other specific problems with the NAIC Model will become obvious when I suggest some amendments, but before I do so, perhaps I ought to explain why I failed to bring this to your attention earlier. First, the industry in general objected to the inclusion of workers' compensation beneficiaries and third party claimants in the definition of consumer; if the definition of consumer were coextensive with the GLB definition, none of the problems I have outlined with respect to our commercial lines insured would exist. Since it was not clear to me what the NAIC might do with respect to the industry request, I was disinclined to suggest amendments to the model, and I assumed, perhaps incorrectly, that trade association representatives had made clear why they had concerns about the broadened definition of consumer. Apparently, I was wrong, as most regulators with whom I have spoken do not seem to have had these matters brought to their attention.

At this point, it seems appropriate that amendments of the NAIC Model be considered, in those states which have decided to adopt the model, to deal with what I believe to be legitimate concerns. I would suggest the following:

(1) Amend Section 15.A.(1) as follows:

"Servicing or processing an insurance product or service that a consumer requests or authorizes, or adjusting a claim submitted by a consumer;"

(2) Amend Section 15.B.(2)(e) as follows:

"To underwrite insurance at the consumer's request or for any of the following purposes as they relate to a consumer's insurance, or, when the consumer is a workers' compensation beneficiary or third party claimant, to the policyholder's insurance: . . . processing, adjusting, paying and settling insurance claims . . . "

(3) Amend Section 15.B.(2)(c) as follows:

"To provide a confirmation, explanation, 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, or a commercial lines policyholder or the policyholder's agent or broker with respect to a claim asserted by, or paid to, a consumer under the commercial lines policy." (This would permit disclosure of claims information with respect to experience-rated renewal policies.)

(4) Amend Section 15.B.(2)(f)(ii) as follows:

> "The transfer or collection of debts, receivables, accounts or interest therein; or . . . " (This would allow the disclosure of claims information with respect to large deductible workers' compensation policies and retroactively-rated workers' compensation policies.)

Speaking just on behalf of Amerisure, if these amendments were included in the NAIC Model, we would be much less concerned if this model were adopted in any state in which we do business, because it would authorize disclosures that are necessary and appropriate, and we neither make nor intend to make any other sort of disclosure to nonaffiliated third parties. Interestingly enough, the NAIC Model's rules for health information, which have caused much concern to the industry, do not seem particularly onerous as applied to the operations of a commercial lines insurer. It seems to me that the Section 17B list of insurance functions authorizes all of the disclosures I have discussed earlier in this letter (claims administration, claims adjustment and management, underwriting, policy placement or issuance, loss control, risk management, policyholder service functions). However, I would be interested in hearing whether you agree with my optimistic interpretation.

Thank you for taking the time to consider this lengthy exposition of my concerns. I never have had the reputation for brevity, but I have done the best I can. Please do not hesitate to call if you would like to discuss any of my thoughts, and I look forward to seeing you in San Francisco (I am skipping the Nashville meeting).

Sincerely,

D. Joseph Olson

cc: Therese Vaughan

(p\G:\GEN_COUN\MISC\KS-DOI.01)