Summary of Presentation by the
National Association of Insurance Commissioners (NAIC)
GLB Interagency Meeting on the ANPR on Privacy Notices
January 26, 2004
Office of the Comptroller of the Currency

Participants:
Audrey M. Samers, Deputy Superintendent and General Counsel, State of New York Insurance Department
Blair W. Cappuccio, Financial Services Policy Analyst, NAIC

Comments:

Forty-nine states have enacted privacy regulations pertaining to the insurance industry. The 50th state, Alaska, is working on privacy regulations now. Currently, 26 states have safeguarding regulations for insurance companies. The New York Insurance Department examines for compliance with New York State privacy regulations. Most insurance companies do comply. There has not been much public outcry about privacy notices. Ms. Samers reported that they hear anecdotally most customers do not read them.

NAIC has had a Privacy Working Group for the past three and a half years. About a year and a half ago, this working group formed a NAIC Privacy Notice Subgroup comprised of consumers, industry, and NAIC members on how to improve the privacy notices. This was a nine-month project that culminated in the "Report on Improving Privacy Notices," with recommendations but no requirements. Ms. Samers provided a copy of this March 2003 Report.

In response to the ANPR questions, 11 Subgroup members met by conference call to discuss these questions prior to this meeting and provide preliminary answers to the Agencies. NAIC intends to submit a formal response after their meeting in March.

In NAIC's view, the most important goals of the GLB privacy notice for consumers is to inform consumers about their rights, enable them to make an informed decision to opt-in or opt-out, provide for the exercise of their rights, and enable consumers to easily compare companies' policies. NAIC believes that a short form, if effective, would inform consumers on each business's privacy policy and would permit easy comparisons among businesses. However, they added a caveat that the federal short form could open up the privacy debate in each state. Also, it would be more difficult to make amendments in those states where legislation, not just regulatory changes, are required.

The Notice Subgroup participants liked Appendix A best, particularly the Yes/No responses to standard questions. In particular, participants liked the large type, good title ("Important Privacy Information"), and explanations of the exceptions. The participants suggested that Appendix A could be improved by shrinking the type to get the last box onto page 1, leaving page 2 with the opt-out. They suggested that the Agencies add the language from Appendix B to explain "companies in our corporate family, such as our securities broker-dealer and our credit card bank" since few people understand the concept. The reference to

"safeguards" should allow consumers an opportunity to request additional information on specific safeguarding policies. They said that the use of the phrase "other sources" to describe where companies get customer information is too open-ended. For the description about joint offerings, participants thought it would be useful to note whether the joint partner has agreed not to share information for other purposes.

Participants liked Appendix B second best, but found the print too small. Participants did not like Appendix C as its headings and flexibility are basically what we see today. While Appendix C might provide some improvement over current privacy notices that are even longer, this approach is not as good as one that contains Yes/No check-off boxes. The flexibility in Appendix C would inhibit easy comparisons by consumers of the businesses' privacy notices. Finally, participants did not think that Appendix D offered consumers enough information.

When asked whether there was any empirical data, research, surveys, testing, or anecdotal experiences they could provide to help shape the GLB notice content or format, Ms. Samers said the NAIC regulators do not have empirical data. She stated that funding precluded such research. Ms. Samers said that the one area of complaints in New York relates to the use of Social Security numbers, and suggested there may be a need for legislation in this area.

In general, the NAIC regulators think it is a good idea to have a layered privacy notice. They believe a short notice alone would not be sufficient, and that the long notice should be available by request, such as through an 800 number.

NAIC Privacy Notice Subgroup

Report on Improving Privacy Notices

As Adopted by the NAIC Privacy Issues Working Group
March 10, 2003

NAIC Privacy Notice Subgroup
Report on Improving Privacy Notices

Title V of the Gramm-Leach-Bliley Act (GLBA) calls on state insurance regulators to promulgate rules enforcing the privacy protections embedded in the Act. All states have taken action to comply with that mandate.[1]

A key element of GLBA's privacy protections – and by far the most visible to consumers - is the privacy notice. The purpose of the privacy notice is to explain the licensee's privacy policies to its customers, and to other consumers whose nonpublic personal information may be subject to disclosure to third parties. The notices are intended to assist consumers in making informed decisions about how to exercise their legal and contractual rights with regard to their personal information, and in comparing licensees' information practices when shopping for insurance and other financial services.

Privacy notices must contain specific information about a licensee's privacy policies, such as the types of protected information the insurer collects, the types of protected information the insurer discloses, and the categories of entities to which the insurer discloses such information.

Financial institutions, including licensees, were first required to send privacy notices to customers by July 1, 2001. After that date, financial institutions are required to provide notices annually to customers, and to certain other consumers as well. Since the first privacy notices were sent in mid-2001, there has been a great deal of discussion and debate over the effectiveness of the notices. Did the notices really do what Congress and the regulators intended? Did they explain the financial institution's privacy policy in a way that clearly informs customers as to what information is protected and when/where/how such protected information is disclosed?

Many notices have been described as confusing, complicated and overly legalistic. That is not to say that financial institutions are not in compliance with GLBA and applicable regulations, or that they did not make great efforts to draft notices to be clear and understandable. The problem is that it is a very difficult task.

Throughout its discussions, the NAIC Privacy Notice Subgroup (the Subgroup) focused on finding ways to help licensees craft GLBA privacy notices that are simpler, shorter, and more understandable to insurance consumers. Avenues for improving privacy notices are described in this Report. The Report focuses on general themes – such as formatting text, and the placement and merging of the various required elements of the notice – and offers specific suggestions for improving the terminology used in privacy notices. This report focuses on GLBA's privacy

[1] As of February 2003, 36 states and the District of Columbia have enacted laws and/or regulations based on the NAIC Privacy of Consumer Financial and Health Information Model Regulation. Thirteen states have retained the Insurance Information and Privacy Protection Model Act, which was adopted by the NAIC in the early 1980s, and one state has regulations pending.

requirements. It does not address HIPAA, FCRA or any other state or federal requirements, which are beyond the scope of this report.

The Subgroup believes that notices drafted using the ideas outlined below can comply with GLBA's original intent – educating consumers about the disclosure of their information in a manner that they can understand – and still comply with the letter of the law. These suggestions are not mandatory or "best practices." Rather, they are recommendations, drafted by regulators, industry and consumer representatives, that the Subgroup believes licensees could use as a guide for improving their notices.

1. Placement and Ordering of Items in the Notice

Anecdotal evidence suggests that the itemization of the required topics in most licensees' privacy notices is similar and generally follows the same order, which is the order found in Appendix A of the NAIC Privacy of Consumer Financial and Health Information Model Regulation (the Model Regulation) and tracks the order in which those topics are addressed in Section 7 of the Model Regulation, which prescribes the required minimum content of privacy notices.[2]

The Privacy Notice Subgroup believes that the order in which the sample clauses are presented in Appendix A is not necessarily the optimal placement of information in a licensee's privacy notice. Indeed, any strict requirement as to the placement of information in a nonstandardized notice could impede the notice's effectiveness. Mandating a "one size fits all" order of presentation could cause the notice to be "front loaded" with a great deal of information that may not be the most important information for that licensee's customers. The Subgroup encourages licensees to determine the most effective order for the material in their privacy notices, based on the importance of the information to their customers. Licensees should consider placing the more meaningful information and information about any action items (such as opt out instructions) up front.

2. Combining Items in the Notice

The Subgroup discussed the possibility of combining the various required sections of the notice. The Subgroup agreed that combining sections would have the potential to reduce redundancy and length, and improve clarity. The general consensus of the Subgroup was that when many customers received the initial notice, they did not bother to read the notice because it was long and difficult to read. Therefore, the notice was not serving the purpose for which it was intended: to notify the customers of the licensee's privacy policy. For that reason, the Subgroup suggests that companies consider combining sections where possible and taking other steps to create a shorter notice without sacrificing the content of the notice.

---

[2] Appendix A, based on its counterpart in the federal interagency rules, lists sample clauses that can be used in privacy notices. The model regulation does not require that notices disclose information in a particular order. The samples are there merely to illustrate acceptable language. This report in no way alters the validity of the sample clauses in Appendix A.

One combination of sections could be the blending of the "Categories of information the licensee collects" with the "Categories of information a licensee discloses." If a former customer's information is handled in the same way that information about current customers is handled, the "Categories of nonpublic personal financial information about the licensee's former customers that the licensee discloses" can be combined, as well. An example of such a combination is:

> *We collect and may share information about you, some of which is not publicly available. We may share this information now or in the future. We do this to enable us to serve you and to help us to identify you as our customer or our former customer, to process your policy and requests quickly, to pay your claim or tell you about products or services we believe you may want and use.*
>
> - ***Information from you*** *– When submitting your application or requesting an insurance quote, you may give us information such as your name, address, and Social Security number.*
> - ***Information about your transactions*** *– We may keep information about your transactions with us or our family of companies, for example, the products you purchase from us, the amount you paid for the insurance, your account balances, or payment history.*
> - ***Information from outside our family of companies*** *– We also may collect other information. This may include information from consumer reporting agencies such as your credit history, credit scores, driving record or employment.*

If applicable, companies can also consider listing the categories of nonaffiliated third parties to which they disclose information outside the exceptions in the same section of their notice. An example of this combination could be:

> *We may share your name, address, telephone number and demographics, now or in the future, with companies outside of our family of companies such as banks, motor vehicle manufacturers or dealers, parts suppliers, health clubs, travel agencies, car rental agencies, hotels, airlines, or publishers. These companies may offer other financial or non-financial products and services, such as travel programs, magazine subscriptions, dental or legal services, exercise programs, diet programs, credit cards, or mortgages. You will have the opportunity to request that we do not share this information.*[3]

If the licensee does not disclose outside of the exceptions, that licensee could combine the "Categories of nonpublic personal financial information that the licensee discloses" with the "Disclosure that the licensee makes under the exceptions" (as opposed to exercising the

[3] As discussed in section 1, placement of items can be a useful tool to make notices simpler and more effective. A licensee that discloses information to non-affiliated third parties outside the exceptions (or offers the right to opt out of disclosures to affiliates) may wish to follow this item with a discussion of opt out rights.

licensee's prerogative "to state only that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.") An example of the combination could be:

> *We may occasionally convey the information we collect – such as your name, address, e-mail, product information or transaction information – to companies outside of our family of companies in order to:*
>
> - *Perform services for us, such as printing payment coupons, preparing or mailing account statements, processing customer transactions or software programming, or helping us market our own products.*
> - *Offer you financial products that we currently don't offer, like credit cards or specialized programs.*

By combining sections, the licensee may be able to provide a shorter notice in length, while not sacrificing the content of the notice. The Subgroup believes this will result in clearer, more concise notices that are fully read by customers.

3. Use of "Terms of Art"

The Subgroup recognized that the use of "terms of art" in notices could be confusing to customers who are not familiar with insurance and privacy terminology. In order to help consumers better understand the terms in the notices, licensees may wish to define the terms or use common words with the same meanings. A non-exhaustive list of words and phrases synonymous with selected privacy notice terms are listed below. Note that the many words synonymous with "share" illustrate the vast array of meanings this term can possess. As they draft their notices, licensees should be mindful of the requirement in the Model Regulation (and in the various laws and regulations tracking the Model Regulation) that notices be clear and conspicuous, and may refer for guidance to the examples in the definition of "clear and conspicuous" in the model regulation. Licensees should be as precise as possible when using synonyms to avoid further confusing or inadvertently misleading consumers.

Opt-out:

- Stop
- Exercising the right to confidentiality/privacy
- As a customer you have the right, with limited exceptions, to choose whether your information remains confidential or is given out to other companies/ firms/ enterprises/ businesses.
- Prohibit
- With certain exceptions, you may choose not to let companies:
  - Reveal information
  - Give away...
  - Disclose...
  - Exchange...

- Offer…
- You may choose to limit information given to others
- You have the choice of allowing our company to offer your information to other companies for their use/ viewing
- You can choose to keep information:
  - Confidential
  - Private
  - Protected

Disclose:

- Share
- Give
- Distribute
- Make known
- Release
- Display
- Make public

Affiliates:

- Companies within our "family" of companies
- Partners / copartners
- Sister companies
- Companies related to our company
- Companies under common ownership

Non-affiliated Third Parties:

- Companies outside our "family" of companies
- Not associated with our company
- Not related to our company
- Not legally linked with/to our company

Non-Public Personal Financial Information:

- Information that is not publicly available
- Protected information
- Private information

Companies should consider whether the simple phrase "customer information" could substitute for the more technical "non-public personal information" or any of the synonyms above. This would likely depend in large part on how they handle disclosures of information.

Publicly Available Information:

- Information that is unprotected
- Open records information
- Commonly available information
- Information freely available through the media
- Information available through public records
- Information in the public domain

Share:

- Sell
- Provide
- Trade
- Furnish
- Exchange
- Give
- Offer
- Make available to
- Deliver
- Market
- Supply

4. Explaining Disclosures "Permitted by Law"

The Model Regulation permits licensees to simply state, "we disclose information as permitted by law" to explain all disclosures made pursuant to sections 15 and 16. These exceptions are generally for legal and "doing business" purposes.

Anecdotal evidence suggests that some consumers are suspicious when they see "permitted by law," thinking their information will be widely distributed no matter what the rest of the privacy notice says. The Subgroup believes a better approach for consumers and licensees alike is to more fully explain these disclosures with examples or a more complete description. A fuller explanation gives consumers – who are not likely to know what is "permitted by law" – a better understanding of how their information is disclosed, and may promote better customer relations.

In addition to explaining the legal and business exceptions that are "permitted by law," the Subgroup believes that it would be helpful to consumers for licensees to explain that they are also permitted to share information freely with their affiliates. Although neither GLBA nor the model regulation mandates any disclosure by a licensee regarding the licensee's right to share information with its affiliates, the Subgroup believes it would be consumer-friendly to include a clear discussion of this point. This would also offer licensees the opportunity to inform their consumers if they voluntarily limit their power to share information with some or all affiliates.

The following provisions are examples of language that could be incorporated into notices to improve the description of disclosures "permitted by law."

- *We may also share personal information about you with companies or other organizations outside of the [INSURER] family as required by or permitted by law. For example, we may share personal information to:*
  - *Protect against fraud;*
  - *Respond to a subpoena; or*
  - *Service your account.*

- *We Share Information for Legal and Routine Business Reasons. We may disclose information we have about you as permitted by law. For example, we may share information with government regulators and law enforcement agencies. We may provide information to protect against fraud. We may report account activity to credit bureaus. We may share information with your consent. We may give account information such as [list examples] to service providers who work for us.*

- *Other Circumstances Where We May Share Your Information: We may share customer information in other circumstances. Some examples are:*
  - *When you specifically request it or give us permission to do so;*
  - *When we are required by law. For example, we may be required to share information with insurance regulators;*
  - *When we share information with consumer reporting agencies;*
  - *When we suspect fraud or criminal activity;*
  - *When we receive a subpoena;*
  - *When we are ordered by a court to do so; and*
  - *When we sell a particular line of business or function.*

- *In certain circumstances, [INSURER] may share your customer information with trusted service providers that need access to your information to provide operational or other support services. To ensure the confidentiality and security of your information, service providers must agree to safeguard your information in strict compliance with our policy. Additionally, when you apply for a [INSURER] policy, [INSURER] may share information about your application with credit bureaus. We also may provide information to regulatory authorities and law enforcement officials in accordance with applicable law or when we otherwise believe in good faith that the law requires it. In the event of a sale of all or part of one of our businesses, we may share customer information related to that business as part of the transaction.*

- *We may share information as permitted by law. For example, providing information to industry regulators, to law enforcement agencies, for fraud prevention, to credit bureaus and to third parties that assist us in processing the transactions you authorize and in mailing statements to you.*

- *Sometimes we may share your information with other companies affiliated with us or our parent company [NAME], particularly if they support our efforts to provide you with services and product information.*

  Sometimes we may also share your information with a company or business not officially connected to us but who may do work on our behalf.

  And sometimes we may disclose information about you to an insurance regulatory authority, a government agency or a law enforcement official.

  Various industry and professional organizations may also ask us for customer information in order to conduct research studies. These studies are purely scientific in nature and never identify individuals.

  Finally, if we do provide your information to any party outside our company we require them to abide by the same privacy standards as indicated here.

5. Brief Introduction/Notice Preamble

Anecdotal evidence suggests that many consumers do not know why they are receiving privacy notices. Therefore, the Subgroup believes it may be helpful for a licensee to explain to consumers why it is sending the notice, even though neither GLBA nor the NAIC model requires such an explanation. If the explanation were a brief introduction to the privacy notice, it could also offer licensees the opportunity to highlight key issues in the notice, for example items in the notice that address marketing disclosures, opt out rights, etc.

There are a number of benefits that flow from use of an introductory statement. First, it is necessarily generic, so it can be used uniformly by insurance licensees without regard to their unique information handling practices and without changing individual GLBA privacy notices. Second, it is adaptable, so licensees can incorporate the statement into existing privacy notices relatively easily. Third, and most importantly, it is informative, allowing insurance consumers to see at a glance the privacy protections afforded by GLBA and directing those consumers to the more detailed description of a licensee's information handling practices outlined in the individual privacy notices.

The brief introduction could contain statements about the following basic GLBA provisions (as augmented by the Model Regulation):

- *Privacy policy.* Licensees must have privacy policies describing their personal information collection practices, and the extent to which they share that information with third parties for purposes other than normal business operations.

- *Privacy notice.* Licensees must provide privacy notices to customers, reflecting their privacy policies, when the relationship is established and annually thereafter. A privacy

notice must also be provided to applicants and certain other non-customers when their personal information is shared with a third party for marketing purposes, or other purposes for which disclosure without consent is not expressly permitted or required by law.

- *Marketing "opt-out."* Licensees must provide their customers, applicants, and other consumers with the opportunity to "opt-out" from having their personal financial information shared with third parties for marketing purposes. The only exceptions are for financial information shared with a corporate affiliate, with the licensee's own service providers or under a joint marketing agreement with another financial institution.

- *Medical information authorization.* Licensees may not share personal health information for marketing purposes with anyone, including affiliates, unless the licensee has received affirmative authorization to do so.

- *Business operations and legal disclosures.* Licensees may share personal information for non-marketing business operations and for legal purposes without consent.

- *Affiliates.* Except for health information, the restrictions on sharing personal information with third parties do not apply if the third party is under common ownership with the licensee.

6. Formatting Notices

Dynamic formatting is another way to make notices more inviting and easier to read, while still taking care to include all the required elements in the notice.

Incorporating the themes and suggested language changes outlined in this Report with improved visual appeal may also increase the effectiveness of privacy notices. Again, it may be helpful to refer to the examples in the definition of "clear and conspicuous" in the Model Regulation and in the various laws and regulations tracking the Model Regulation. In addition, a licensee may wish to consider the following to increase readability:

- Use of readable typefaces, including size (10 to 12-point type suggested) and fonts (easy to read fonts like Times and Arial; consider different fonts for text and headings);
- Use of **bold** and *italics* to make words and phrases stand out;
- DON'T OVERUSE ALL CAPITAL LETTERS BECAUSE IT'S DIFFICULT TO READ;
- Use of informative headings ("Our Security Practices Protect Your Information," "We Don't Share Your Information with Companies Outside Our Corporate Family," "We Share Your Information for Legal and Routine Business Reasons");
- Use of bulleted or numbered lists; and
- Use of short sentences and short paragraphs.

7. Conclusion

Drafting GLBA privacy notices is a difficult process, made more difficult by the need to comply with specific legal requirements and the desire to draft a readable, consumer-friendly notice that effectively presents the licensee's privacy policy. The Subgroup recognizes the difficulty of this task. In consultation with industry and consumer representatives, the Subgroup has identified methods that may improve notices so that they are both GLBA-compliant and consumer-friendly

- re-ordering and combining required elements;
- explaining phrases and terms of art;
- adding a short preamble describing why the notice is being sent; and
- dynamic formatting.

Licensees are encouraged to regularly review their notices with these suggestions in mind, remembering that the goal is to make the notices simple, readable and effective.