4/8408.pdf

3

National Association of Independent Insurers ("NAII")

Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness

Comments to the

FEDERAL DEPOSIT INSURANCE CORPORATION (FDIC)

FEDERAL RESERVE SYSTEM (FRS)

Board of Governors of the Federal Reserve System

DEPARTMENT OF THE TREASURY

Office of Thrift Supervision

DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

12 CFR Part 30

12 CFR Parts 208, 221, 225, and 263

12 CFR Parts 308 and 364

12 CFR Parts 568 and 570

[Docket No. 00-13]

RIN 1557-ab84

[Docket No. R-1073]

RIN 3064-AC39

[Docket No. 2000-51]

RIN 1550-AB36

August 16, 2000

Overview

The National Association of Independent Insurers (NAII) is a trade association of over 675 property and casualty insurers writing all lines of business in all states. For the most recent year data were available, NAII members wrote nearly $100 billion in premium. NAII respectfully submits these comments to the proposed guidelines of the federal regulators. For reasons which follow, NAII urges the federal regulators to promulgate guidelines rather than rules. Thus these comments are in terms of the word "guidelines."

General Comments

NAII appreciates that underlying the Gramm-Leach-Bliley Financial Services Modernization (GLB) Act is the concept of functional regulation. While the GLB Act leaves the regulation of the business of insurance to the states, NAII believes that to a large extent any guidelines safeguarding customer information adopted by the federal regulators will be generally adopted at the state level as to the business of insurance. On this basis, it is appropriate for NAII to comment to the federal guidelines. In addition, it is likely that under financial services modernization, banks, insurers, and securities firms will be dealing extensively with each other, whether on an affiliated basis or not. For the ease of transaction of business, guidelines at the federal level must address the needs of the insurance segment of the financial services industry.

These comments are directed to the federal regulators as a unit to stress the need for uniformity across federal regulatory lines in regard to the guidelines. One purpose of the GLB Act is to permit affiliations among financial entities, streamlining of financial

services. Now that GLB is law, it is imperative that the guidelines for each of the federal regulators be uniform to minimize unnecessary cost of business which would exist should one or more of the federal regulators "break ranks" to have a unique set of guidelines. In effect, NAII urges the federal regulators to streamline the standards. NAII also urges the federal regulators to promote uniformity while balancing the need to protect consumer privacy with the need for a practical business approach toward the protection of that information. In addition, any set of guidelines or rules should be technologically neutral. This theme underlies the comments contained herein.

Guidelines

NAII urges the federal regulators to adopt guidelines rather than rules for a number of reasons. Guidelines will permit the highest level of flexibility in designing cost effective, and for that matter, procedurally effective internal systems to safeguard customer information. Imposition of rules would impose inflexibility. Many organizations would likely, under rules, have to modify or replace systems at a very high cost, while guidelines would set broad parameters on how organizations can effectively safeguard customer information. Further, many organizations may already adequately protect the customer information. Nothing more need be done. Those same organizations, under rules, may have to change how they operate, solely for the purpose of meeting the rules. Guidelines also permit the greatest flexibility to adapt internal procedures to the rapidly changing technological world. Rules would be more static, requiring change by the federal regulators. Under guidelines, an organization can upgrade its system as the opportunity arises, consistent with internal policy.

Finally, guidelines permit the greatest flexibility as the financial services sectors begin to interact. As affiliations occur, it is natural that there will be differing internal systems and procedures to safeguard customer information. Many will be tailored to the particular financial service offered. Guidelines more readily permit the resulting affiliation to move ahead.

Comment was sought as to whether consumer information, business client, or all information be included.

NAII believes that the type of information to be included should be consistent with and not exceed that covered in Title V of the Gramm-Leach-Bliley Act. Thus, NAII is uncertain as to the term "business client." NAII recommends that the guidelines as promulgated should track with the privacy rules and Title V itself.

Comment was sought whether there are additional or alternative objectives to those listed in the joint notice.

NAII believes that the two objectives listed in the Notice: substantial harm to the customer, and safety/soundness risk to the institution should be joined by a third objective: practicality and reasonableness of the internal standards set forth in the guidelines. NAII has stressed in its comments relating to privacy rules that the need to protect the consumer's information should be balanced with the business use of the information. Consistent with that position, NAII also believes that the need to protect the

customer information needs to be balanced with the cost of doing so. There should be no unreasonable requirements to protect the information imposed on financial institutions.

NAII also believes that there needs to be definition, clarification, or examples of what is meant by "substantial harm" to the customer, especially if rules rather than guidelines are adopted. In either case, failure to do so only invites costly litigation.

Comment was sought as to frequency of reports to the Board of the financial institution and how frequently should there be reports on security and should there be a designated Corporate Information Security Officer.

Given the myriad and volume of issues considered by a Board of any financial institution, NAII believes annual reporting to the Board suffices to reasonably safeguard the information. Similarly, annual reporting on security is reasonable. In either case, establishment and monitoring of internal procedures should be the focus. However, a designated "Corporate Information Security Officer" should not be a guideline, but only a suggestion, as the need for making such a distinction must relate to the volume of information. Again, flexibility is the key. For smaller entities, that role will be part of other duties of an individual. Perhaps the guidelines could be crafted to stress the need for someone internally to be monitoring such activity rather than the accompanying title.

Comments regarding testing.

NAII is concerned that the proposed guidelines on testing create a number of issues. Costly testing procedures should be removed from the guidelines. For example, there is

no reason why internal testing, by employees should not suffice, provided the parameters of the testing are appropriate. In fact, testing by employees is more flexible and likely to reveal problems at an earlier date than, for example, annual testing. In the insurance sector, NAII and its members have seen the value of self-audits as to insurance practices. The same should be permitted here. Plus, employee testing will be in the context of the security system unique to that organization. Outside testing will, by its very nature, be based on standards which may not be appropriate or cost effective for a given organization.

It is appropriate to raise another, perhaps more serious concern, with outside testing, namely access by third parties to personal information. The very process of outside testing exposes the information to further release. NAII urges the federal regulators to focus on the guidelines which then by definition constitute an appropriate test rather than who does the test.

Comment was sought regarding "best industry practices."

NAII believes that "best industry practices" create unique problems. First of all, given the variety of entities, banks, thrifts, insurers, securities firms, etc., which are financial institutions, it is likely that there could be a number of "best industry practices." These will differ for each financial services sector. Thus, to impose a "best" practice would be inconsistent with the concept of flexibility and even with the concept behind issuing guidelines rather than rules. Banking information differs from insurance information in that the former tends to be financial information with some personal information while

the later is usually minimally financial with a good deal of personal information. Yet now banks will be holding insurance information, either through insurer or agency affiliates. NAII urges that no "best practice" be adopted. Rather, we encourage regulators to adopt guidelines which permit the entity to adopt the best practice to suit its unique needs.

NAII appreciates the opportunity to comment to the proposed rules. Should there be any questions relating to these comments, please contact Michael Koziol, Senior Director and Counsel, NAII, 2600 S. River Road, Des Plaines, Illinois 60018. Phone: 847 297 7800. Fax: 847 297 5064. Email: mkoziol@naii.org.

Comments or questions may also be sent to: Julie L. Gackenbach, Director of Government Relations, NAII, 444 N. Capitol Street NW, Suite 801, Washington, D.C. 20001. Phone: 202 639 0473. Fax: 202 639 0494. Email: jgackenb@naii.org.