48,413

7

August 24, 2000

Communications Division
Office of the Comptroller of
the Currency
250 E Street, SW
Washington, D.C. 20219

**Re: Docket No. 00-13**

Robert E. Feldman, Executive
Secretary
Federal Deposit Insurance Corp
550 17th Street, NW
Washington, D.C. 20429

**Attention: Comments**

Ms. Jennifer Johnson, Secretary
Board of Governors of the Federal Reserve System
20th and C Streets, NW
Washington, D. C. 20551

**Re: R-1073**

Manager, Dissemination Branch
Information Management & Services
Division
Office of Thrift Supervision
1700 G Street, NW
Washington, D. C. 20429

**Re: Proposed Standards for Safeguarding Customer Information**

Dear Sirs and Madam:

The Connecticut Bankers Association (the "Association") respectfully submits the following comments on the proposed standards for safeguarding customer information ("Proposal") published pursuant to the Gramm-Leach-Bliley Act (the "Act"). By way of background, the Association is an industry association representing over eighty (80) banks and thrifts conducting financial operations in the State of Connecticut. Those institutions include state chartered non-member banks, national banks, and federal and state chartered thrifts (many of which are in holding company structures).

In recent months, we have been engaged in discussions with many of our members regarding

the Proposal and have solicited comments for possible submission to the applicable federal bank regulatory agencies responsible for the implementation of the new standards (the "Agencies"). Although we cannot suggest that the views set forth below are held by all our member banks and thrifts, we do feel comfortable in suggesting that we have captured the views of the majority of our members, and in some cases, the vast majority of our members.

1. **General Comment on Industry Burden and the Need for Examples.** Many, if not most, of our member banks *already* have extensive policies and procedures in place to protect the confidentiality and security of customer information. In some cases, those policies and procedures were adopted on a voluntary basis out of general concern for risk management objectives. In other cases, the policies and procedures were adopted in response to existing security-related supervisory guidance.

Now, Congress has raised the issue to a new level by mandating the adoption of more comprehensive security standards. These new security standards have the *potential* to increase the compliance burden well above that which was previously imposed. At this stage, it is difficult to assess the precise amount of additional burden. However, we note that the proposed standards are, in many cases, broad and imprecise. This means that many institutions will be forced to guess as to how much effort and detail is required in order to comply with a particular standard. And, with each guess, comes the risk that examiners will disagree with the good faith judgments of bank

management. This is a dangerous situation which could lead to unnecessary and excessive compliance burdens, not to mention uneven and unfair enforcement.

Notwithstanding the forgoing concern, we recognize that the broad language in the Proposal was designed, at least in part, to provide *flexibility*. The banking industry wants and needs this flexibility, particularly for community banks. In order to avoid the potential excessive burdens discussed above without sacrificing flexibility, the Association believes that it is important for the Agencies to provide more detailed *examples* of how an institution might comply in different scenarios.[1] When providing those examples, it should be made clear that they are merely examples and do not constitute the sole means to achieve compliance.

We also urge the Agencies to emphasize that *existing* policies and procedures *may*, in some cases, satisfy some or many of the concerns discussed in the guidelines and that additional compliance efforts may not be necessary to address those concerns. Similarly, we urge the Agencies to emphasize that if security risks are *already* being properly managed through several *separate* policies, then the consolidation of those policies into a single "information security policy" is not necessary.

Finally, we urge the Agencies to be judicious in their expectations as to how much detail and effort is required in order to comply with the new standards. In this case, our concern for regulatory burden is a matter of competitive parity. We note that many *non-bank* financial institutions will *not* be subject to a similar set of *detailed* security standards.[2] The banking industry should not be subjected to a disproportionate amount of regulatory burden. Otherwise, the banking industry may find it increasingly difficult to compete against non-bank competitors.

2. **Whether The Standards Should Be Issued In The Form of Guidelines.** The Agencies have requested comment on whether the final standards should be issued in the form of "guidelines" or in the form of "regulations". The Association urges the Agencies to adopt guidelines, rather than regulations. Guidelines, by their very nature, connote a degree of flexibility, whereas regulations impose an element of rigidity. In this case, flexibility is of paramount importance and a guideline format is the best vehicle for the creation of a flexible compliance framework.[3]

3. **Community Bank Burdens.** The Agencies have requested comment on the impact of the Proposal on community banks. Consistent with our comment from Section 1 above, we are concerned that community banks will be left to guess as to how much effort and detail is required to achieve compliance.

---

[1] Wherever possible, we urge the Agencies to provide examples which help to illustrate how compliance requirements might differ among banks of different size, banks with different activities, etc.

2 For example, at present, the SEC has indicated that it does not expect to adopt a similar set of detailed guidelines for broker-dealers and other securities firms subject to SEC jurisdiction.

[3] We also note that Congress did not require the adoption of *regulations* under Section 501. In other parts of the Act, Congress explicitly required regulations. We believe this evidences Congressional intent that the standards be something other than regulations.

For that reason, we urge the Agencies to provide specific *examples* of how a community bank (or other small institution) might achieve compliance. In this regard, we support the development of a separate "compliance guide" for community banks (as is mentioned by the Agencies in the preamble).

**4. Customer Information.** The Agencies have solicited comment on whether the guidelines should apply to *all* of the institution's customer records (both business and consumer). The Association strongly urges the Agencies to adopt the more narrow definition of "customer" found in the privacy regulations. Compliance with the privacy regulations and the new security standards will be a monumental and expensive undertaking. Please do not expand that undertaking to include commercial records. Those records do not necessarily warrant the same degree of protection that should be afforded to "consumer" records.[4] Congress did not mandate such protections and the potential additional burdens far outweigh the benefits.

[4] We recognize that, in some cases, a breach of security in a *commercial* context can raise safety and soundness and reputational concerns similar to those found in the consumer arena. However, we believe that the security risks associated with commercial records can best be managed (and will likely be managed) on a voluntary basis, without the need for explicit supervisory standards. We note that the exclusion of commercial records from the scope of coverage would not have the effect of limiting the authority of the Agencies to address any unsafe or unsound practice. However, if the Agencies include commercial records within the scope of coverage, the Agencies will simply give plaintiff's lawyers additional ammunition to attack banks in litigation proceedings (which, in turn, could affect safety and soundness).

**5. Unauthorized Access or Use.** In the preamble discussion of Section II.B., the Agencies state that unauthorized access to or use of customer information does not include access or use *with customer consent*. We urge the Agencies to make it clear that "unauthorized" access or use does not include access or use that is otherwise "required or permitted by law". The concept of "authorization" should not be equated with the concept of express customer consent. There are many instances where access or use should be permitted without express customer consent. Those instances should be reflected as exceptions to the broad objectives set forth in Section II.B. of the Proposal.[5] For example, a bank may want or need to use customer information for *debt collection* purposes (which might be "harmful" or "inconvenient" for the customer) and the bank may not have the customer's express consent for such purposes. A bank should not have to adopt a program or policy to prohibit such a use.

**6. Reporting Responsibilities.** The Agencies have solicited comments on the appropriate frequency of reports to the board. The Association believes that a specific time interval should *not* be mandated. Reports to the board should only be required when there are *material* issues for consideration. If there are no material events (e.g., significant breaches of security) or material changes in policies or procedures, the board should not be compelled to engage in a "status" review that might distract the board's attention from other, more important issues.

---

[5] By way of illustration, we also draw your attention to the privacy regulations and the many exceptions permitting disclosure of customer information to nonaffiliated third parties. For example, providing access to customer information pursuant to a lawful subpoena may ultimately prove to be "inconvenient" to a customer.

7. **Information Security Officer.** The Agencies have solicited comments on whether it is appropriate to require the board to designate a "Corporate Information Security Officer". The Association does not believe that a mandatory requirement is appropriate. That decision should be left to each individual institution. Depending upon the size of the institution, its staffing resources, and the scope and nature of its activities, such an appointment may or may not be appropriate. In some cases, the duties might even be segregated and assigned to different individuals.

8. **Risk Assessment.** The Proposal requires an institution to "identify and assess risks". This is a broad and imprecise requirement. We urge the Agencies to clarify, through the use of examples, what kind of risks might be implicated and how those risks might be "assessed". For smaller banks, we particularly urge the Agencies to clarify that this process does not necessarily require an elaborate analysis or extensive documentation.

9. **Outsourcing Arrangements.** Section III.D. of the Proposal states that "[t]he bank continues to be responsible for safeguarding customer information even when it gives a service provider access to that information". The Association believes that this is an overly broad, unfair and dangerous statement. Although some protective measures may be appropriate (e.g., contract provisions), a bank should not be required to act as a policeman or guarantor with respect to third party activities. As a practical matter, a bank often cannot control the activities of the third party. A guideline statement suggesting that a bank is responsible for the activities of a third party may serve to broaden existing law (thereby providing ammunition to plaintiff's lawyers looking to hold a bank

---

Nonetheless, it is required by law and a bank should not have to develop a program that prohibits such access.

responsible for third party activities). This is an industry safety and soundness issue and the Agencies should be careful to avoid such broad statements.

Similarly, the Proposal states that "*[t]he bank must exercise appropriate due diligence in managing and monitoring its outsourcing arrangements to confirm that its service providers have implemented an effective information security program to protect customer information and customer information systems consistent with these Guidelines*". The Association believes that this is an overly broad and unrealistic requirement. As a practical matter, many third parties will not agree to be subjected to the type of due diligence suggested in the Proposal. Moreover, even if such due diligence is permitted, the imposition of "management" and "monitoring" responsibilities upon the bank can, in many cases, constitute an unreasonable and unrealistic standard. Many banks will simply not have the resources, time or money to comply with that standard. The best a bank can do, in most cases, is perform certain limited preliminary due diligence inquiries, "attempt" to impose contractual requirements, and thereafter remain attentive to detect problems that manifest themselves in a material and visible way. The Agencies should explicitly recognize the limited powers and resources that are available to banks with respect to outsourcing arrangements. We recommend that the Agencies focus on the imposition of contractual requirements (recognizing that the third party may not always be cooperative) and explicitly note that it is the third party (not the bank) that is ultimately responsible for information security.

We thank you for the opportunity to present these comments. Please do not hesitate to contact me directly at (860) 677-5060 (or our counsel on this matter, David J. Wiese of Tyler Cooper & Alcorn, LLP at (860) 725-6213) if you have any questions about any of the matters discussed in this letter.

Respectfully submitted,

Lindsey R. Pinkham
Senior Vice President and Secretary

cc: David J. Wiese
Tyler Cooper & Alcorn, LLP
CityPlace/35th Floor
185 Asylum Street
Hartford, Connecticut 06103-3488

H:\WIESE\Connecticut Bankers Association\Privacy Policies\Letters\CommentLtrOFFICE OF COMPTROLLER.doc