48428.pdf

(21)

Gottlieb, Mary H

From: Hurwitz, Evelyn S on behalf of Public Info
Sent: Monday, August 28, 2000 9:19 AM
To: Gottlieb, Mary H
Subject: FW: Comment on Proposed Interagency Guidelines Establishing Standards for Safeguarding Customer Information

-----Original Message-----
From: Shannon Phillips [mailto:Shannon@texasbankers.com]
Sent: Friday, August 25, 2000 5:14 PM
To: 'regs.comments@federalreserve.gov'; 'regs.comments@occ.treas.gov'; 'public.info@ots.treas.gov'
Subject: Comment on Proposed Interagency Guidelines Establishing Standards for Safeguarding Customer Information

August 25, 2000

Communications Division
Office of the Comptroller of the Currency
250 E Street, SW., Third Floor,
Washington, DC 20219
Attention: Docket No. 00-13

Ms. Jennifer J. Johnson
Secretary
Board of Governors
of the Federal Reserve System
20th and C Streets, NW
Washington, DC 20551
Attention: Docket No. R-1073

Mr. Robert E. Feldman
Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429
Attention: Comments/OES

Manager, Dissemination Branch
Information Management & Services Division,
Office of Thrift Supervision,
1700 G Street, NW
Washington, D.C. 20552
Attention: Docket No. 2000-15Dear Sir or Madam:

The Texas Bankers Association ("TBA") submits these comments in response to the Federal Banking Agencies' Proposed Interagency Guidelines Establishing Standards for Safeguarding Customer Information implementing portions of the Gramm-Leach-Bliley Act ("GLB"). TBA represents the interests of approximately 800 financial institutions in the state of Texas - from the smallest community banks to the largest nationwide financial service providers. Founded in 1885, TBA is the oldest and largest Texas banking association. TBA participated actively in the Congressional considerations that yielded the Financial Modernization Act and has received numerous questions and comments from its members about these proposed guidelines.

1. The Agencies have requested comment about whether the standards should be adopted as guidelines or as regulations. We support the adoption of guidelines. As the proposal itself points out, most institutions already have a security policy in place. Security standards are constantly evolving as technology advances. Institutions of all sizes, with varying degrees of complexity and differing security needs, are affected by these security guidelines. Adopting these standards as guidelines maximizes the flexibility necessary to meet changing technology and different size, complexity and budgetary considerations. We believe that the same high standards of protecting customer records can be achieved through guidelines as contemplated by GLB.

As additional support for our request that these standards be adopted as guidelines, we respectfully remind the federal agencies that financial institutions are currently engaged in a massive effort to comply with the Privacy Regulations, just issued in final form in May 2000. The model text for Privacy Policies under those regulations (Model A-7, Appendix A) includes a representation that "We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information." Our financial institutions are working diligently to prepare and disseminate their privacy policies now - well in advance of the July 1, 2001 mandatory compliance date. Many have contacted us with their concern that, although they fully comply now with existing security guidelines and will certainly fully comply with whatever final security guidelines are adopted, they do not want to be caught in a regulatory issue due to the fact that these security guidelines are not final when they are preparing their policies. They and we believe it is appropriate to go ahead with privacy policy preparation, that the representation today that they are in compliance with existing security guidelines is appropriate, and if adjustments in the standards are made under this proposal they will still be making an accurate representation in their privacy policies by coming into compliance with any adjustments in the final security guidelines by July 1, 2001.

2. The Agencies have invited comment about the impact on community banks. We urge the agencies to be mindful of the different level of resources as well as the limited number of personnel available to community banks. Requiring community banks (or any financial institutions for that matter) to implement security programs, when current procedures are adequate, is a waste of precious resources and employee time. The guidelines need to clarify that existing information security programs will comply so long as the stated security objectives are met.

3. The definition of "customer" should be clarified to reflect that business customers are not included. Additionally, the stated scope of the proposed guidelines should affirmatively state that they only apply to an individual, or that individual's legal representative, who obtains a financial product or service from a financial institution that is to be used primarily for personal, family, or household purposes.

4. Section 501 of GLB requires each agency to "establish appropriate standards" to prevent

"unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." GLB did not set this out as a standard for a financial institution's information security program, but for each agency in establishing appropriate standards for financial institutions relating to administrative, technical, and physical safeguards. Inconvenience to the customer is not the true measure of a financial institution's information security program.

5. Although managerial reports to an institution's board regarding its information security program is a necessary element of a complete program, how often a report is needed will vary from bank to bank, and should be left to the discretion of the individual institutions. To dictate board reports at certain intervals will likely prove to only add unnecessary, costly, and unproductive activity to already busy board meetings.

6. Requiring encryption of electronic customer information may be necessary in some instances but an unneeded measure in others. Smaller institutions may encounter significant disruption of business and substantial use of money and time in installing encryption software in systems where encryption software is not needed. Clarification of this guideline would be appropriate.

7. Financial institutions with outsourcing arrangements should not be responsible for auditing their service providers' security programs and use of customer information, and financial institutions should not be responsible for safeguarding the information once it is given to service providers. Appropriate contractual provisions requiring service providers' performance standards in connection with the security of customer information should relieve financial institutions of further responsibility with regard to outsourcing arrangements.

8. Dual control procedures in many cases may be unnecessary and/or impossible. Employees of community banks more often than not perform many functions. Asking these banks to implement possibly unnecessary dual control procedures may make it difficult or impossible for these employees to perform essential functions for their institutions.

9. Financial institutions should be able to use either 1) outside parties or 2) employees not involved in the information security area to test security systems and review the test results. Precedent exists for this in the Bank Secrecy Act where testing requirements for internal review may be performed by financial institution personnel or outside parties.

The banking industry is committed to the security of customer information and has performed the task well for centuries. The proposed guidelines serve as a reminder to our financial institutions to remain diligent in this important task. However, we must insist that the agencies take care that this guidance does not overburden financial institutions, particularly community banks, with guidelines that do not enhance the security of customer information. We believe that the changes suggested in this letter will help the agencies establish appropriate standards for information security while balancing the needs of our financial institutions.

Sincerely,

<<...>>

Rick Smith
President