48435 pdf

(28)

Compass Bank
LEGAL DIVISION
15 South 20th Street
Birmingham, Alabama 35233
Phone: 205-933-3263
Fax: 205-933-3043

August 25, 2000

Via E-mail

Ms. Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551
Attention: Docket No. R-1073
regs.comments@federalreserve.gov

Mr. Robert E. Feldman
Executive Secretary
Attention: Comments/OES (RIN 3064-AC39)
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, D.C. 20429
comments@fdic.gov

Communications Division
Office of the Comptroller of the Currency
250 E Street, SW
Washington, D.C. 20219
Attention: Docket No. 00-13
regs.comments@occ.treas.gov

Manager, Dissemination Branch
Information Management and Services Division
Office of Thrift Supervision
1700 G Street, NW
Washington, D.C. 20552
Attention: Docket No. 2000-15
public.info@ots.treas.gov

Re: Comments on the Proposed Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness

Dear Sirs and Madams:

This letter is submitted to the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation and the Office of Thrift Supervision (collectively, the "Agencies") on behalf of Compass Bancshares, Inc., a financial holding company ("Compass"), in response to the Agencies' request for comment on their Proposed Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness (the "Guidelines") issued pursuant to Title V of the Gramm-Leach-Bliley Financial Modernization Act (the "GLB Act").

Compass conducts a regional general commercial banking and trust business at 325 bank offices located in Alabama, Arizona, Florida, Colorado, New Mexico, and Texas. As of year-end 1999, Compass had assets of $18.2 billion. Compass provides correspondent banking services, including operational and investment services and financial transaction processing assistance, to approximately 1,000 financial institutions located throughout the United States.

Compass appreciates the Agencies' time and effort in preparing the Guidelines and hopes that these comments will be helpful to the Agencies in their effort to promulgate reasonable and workable standards for customer information safety and security.

GENERAL COMMENTS

Form of Issuance

The Agencies questioned whether the proposed guidance should be issued in the form of "Interagency Guidelines" or regulations. The practical effect of the decision will be limited as we intend to comply fully with the final standards regardless of the form in which they are issued. However, we believe that issuing the guidance in the form of "Interagency Guidelines" will allow a greater degree of flexibility and thereby promote innovation that ultimately will lead to better protection of customer information.

Applicability to Non-Consumer Records

The Agencies solicited comment on whether the Guidelines should apply to the institution's records concerning consumer customers only, consumer and business customers, or all records of any type. In many cases, security procedures may not differ based upon the type of customer. For example, demand deposit records of both consumer and business customers often are secured identically because maintaining separate systems would be cost prohibitive. However, in other cases, differences between consumer and business accounts result in the maintenance of separate systems, e.g., commercial account analysis systems, that may be subject to different types of security measures and controls. Further, applying the Guidelines to *all* records would involve systems that do not process any customer data (e.g., accounts payable, general ledger, etc.).

We believe that it would be inappropriate to expand the scope of the Guidelines to apply to any information other than consumer information. To do otherwise would be beyond the scope of the GLB Act and may cause a diversion of resources away from the protection of consumer information. We urge the Agencies to restrict the scope of the Guidelines to consumer

information and allow each institution the flexibility to determine the security procedures appropriate for non-consumer information.

Implementation Deadline

We are concerned that the July 1st, 2001, deadline may not allow adequate time to implement all requirements of the Guidelines. Despite their brevity, the Guidelines contain broad direction on the safety and security of consumer information. Each institution will have to understand and carefully consider the impact of the Guidelines on the organization. Also, even with reasonable and adequate protections already in place, conforming an institution's policies and procedures to those outlined in the Guidelines may involve the expenditure of substantial human and monetary resources. We ask the Agencies to consider extending the implementation deadline to one year from the issuance of the final Guidelines.

Year 2000 Standards Rescission

The Agencies questioned whether the rescission of the Year 2000 Standards for Safety and Soundness is appropriate at this time. We believe that it is appropriate and encourage the Agencies to rescind those standards.

SECTION-BY-SECTION COMMENTS

Standards for Safeguarding Customer Information (Section II.)

Section II outlines proposed objectives for an institution's information security program. We are concerned that the objectives proposed by the Agencies would create unrealistic and unattainable standards for financial institutions. The Guidelines require that a "security program shall: 1. Ensure the security and confidentiality of customer information; 2. Protect against any anticipated threats or hazards to the security or integrity of such information and; 3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer or risk to the safety and soundness of the bank." (Emphasis added.)

The use of the word shall suggests that institutions must assure absolute security protection. This standard is likely impossible for any institution to meet, notwithstanding imposition of reasonable controls and measures to establish a secure environment. Additionally, use of the word any as a modifier to the phrases "anticipated threats" and "customers or risk" in subsections 2 and 3 creates an overly broad standard. Finally, we are confused by the use of the word inconvenience in this context. While we believe that minimizing customer inconvenience

is a hallmark of good customer service, the concept of inconvenience is not an appropriate standard for these Guidelines.

Title V of the GLB Act requires the Agencies to "establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards..." (emphasis added). To address these concerns, we suggest the Agencies adopt the following language:

> "Objectives. A bank's information security program shall be designed to reasonably: 1. Promote the security and confidentiality of customer information; 2. Protect against anticipated threats or hazards to the security or integrity of such information and; 3. Protect against unauthorized access to or use of such information that could result in substantial harm to customers or risks to the safety and soundness of the bank."

The Agencies indicate in the preamble to the Guidelines that "[f]or purposes of the guidelines, unauthorized access to or use of customer information does not include access to or use of customer information with the customer's consent." We agree with this standard. For example, the practice of "screen scraping,"—where a customer provides a third party with authorization to access the customer's financial information—often occurs without the knowledge of the financial institution. In such situations, financial institutions should not be held responsible because the customer has authorized access to their account and account information. Consistent with this view, we strongly encourage the Agencies to include language within the text of the Guidelines that reflects the language from the preamble that is quoted above.

Information Security Program (Section II.A.)

Section II.A. calls for a "comprehensive information security program." The word comprehensive is undefined and is possibly suggestive of an information security program that is beyond the qualifying language at the end of the sentence: "appropriate to the size and complexity of the bank and the nature and scope of its activities." We suggest striking the word comprehensive and rewriting the entire sentence as:

> "Each bank shall implement an information security program that includes administrative, technical, and physical safeguards to reasonably assure the confidentiality of customer information."

Board of Directors Involvement (Section III.A.1.)

Board Approvals

While we believe it is proper for the board of directors to approve the information security policies of the organization, we disagree that it is necessary or appropriate for the board to approve the information security "program" which implements the security policies. We suggest that the phrase "and program" be dropped from Section III.A.1.a.

We also believe that, depending on the structure and complexity of a financial institution, the approval of policies may properly and effectively be performed by a committee of the board or a management committee that reports to the board or to a board committee. Therefore, we ask the Agencies to revise the Guidelines to allow approval of the information security policies by "the board, a committee of the board, management committee, or other appropriate level of management within the financial institution."

Board Oversight

Section III. A.1.b. provides that the board will oversee efforts to develop, implement, and maintain an effective information security program. The word oversee appears to impose a duty on the board to actively manage the security program. This type of "active" management is properly the function of the financial institution's officers. We request the Agencies to reconsider the imposition of this duty on the board and provide flexibility for the board "or other appropriate level of management" to carry out this function.

Reporting to Board of Directors (Section III.A.2.c.)

The Agencies invite comment regarding the appropriate frequency of reports to the board of directors. We do not believe there should be a requirement for defined periodic reporting to the board. Often, reporting certain non-material information to a management level below the board, such as a committee of the board or a representative(s) of senior management, is a more efficient and appropriate reporting mechanism than reporting to the board or directors. For example, attempted security breaches are an everyday occurrence for financial institutions that have an Internet presence. Indeed, unsuccessful attempts to breach security are a demonstration that the institution's security practices are effective. As discussed in the above comment to III.A.1.b., the security "program" is properly the responsibility of management. Management should be empowered to make changes to the security program without a need to make "recommendations" to the board.

Each financial institution should determine the appropriate scope and frequency of information reporting and the appropriate level of senior management to which that information should be reported. Accordingly, we believe that periodic reporting, no less than annually, should be performed "at the level of senior management responsible for administration of the institution's security program."

In the event the Agencies do not support this proposal and decide to impose a requirement for periodic reporting, we believe that annual reports to the board or a committee of the board would be more than adequate.

Access Rights to Customer Information (Section III.C.1.a.)

The Agencies list proposed factors that an institution should consider when evaluating their security policies. One of these, listed as factor III.C.1.a., applies to "access rights to customer information." We believe that this element is intended to ensure that financial institutions have appropriate security measures in place to prevent unauthorized access to customer information. However, this statement could be misinterpreted to apply to a customer's right to access financial information maintained by a financial institution under laws such as the Fair Credit Reporting Act. If the Agencies intend to use this factor to promote appropriate standards against unauthorized access to customer's information, we believe that the other factors listed, including III.C.1.b. and c., appropriately address this area. Accordingly, we encourage the Agencies to delete this factor. At a minimum, the Agencies should clarify that factor III.C.1.a. is not intended to create a new customer right to access financial information.

Access Controls on Customer Information Systems (Section III.C.1.b.)

We believe the reference to "companies" in factor III.C.1.b. should be struck. As stated previously in this letter, we believe that these standards should apply only to consumers and customers as those terms are defined by the GLB Act. Accordingly, imposing standards for protection of "company" information should be outside the scope of the Guidelines.

Encryption (Section III.C.1.d.)

In III.C.1.d., the Agencies propose instructing institutions to "consider appropriate encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access." This language seems to require encryption in many cases where encryption would not be appropriate. Encryption can be a complex and sophisticated approach to protecting confidential data. Requiring institutions to use encryption when it is not necessary could impair two-way electronic communication

between financial institutions and their customers, as well as communications within the institution which are already subject to the institution's other security protections. Moreover, in some cases, use of encryption can be potentially harmful. For example, if magnetic media (e.g., tapes and disks) were encrypted for transit and storage offsite, the data would be irretrievable if the encryption key is lost.

We recommend that the Agencies change this provision to focus on protection of customer data rather than a particular methodology for doing so. For example, we suggest the following language to replace the proposed language:

> "Procedures to protect the confidentiality of electronic customer information, which may in appropriate circumstances include encryption of electronic customer information, while in transit or in storage on networks or systems that are not controlled or monitored by the bank or its agents and that are accessible to unauthorized persons."

Employee Background Checks (Section III.C.1.f.)

In the banking industry, nearly all employees have some responsibility for or access to customer information as part of their job responsibilities. We are troubled by the suggestion of "employee background checks" for all employees with access to customer information because such checks are not warranted for each teller, data entry clerk, etc. and would be prohibitively expensive. We ask that the Agencies delete the reference to "employee background checks."

Testing (Section III.C.3.)

Specific Types of Testing

The Agencies seek comment on the need for specific types of tests, such as penetration or intrusion detection tests. We oppose a requirement of specific tests because the necessity and suitability of a specific type of test must be determined in the context of the controls being relied upon and the systems being tested. Therefore, consistent with the principle of measured supervision according to the perceived risk, each institution should be allowed the flexibility to develop and implement testing programs that are appropriate under the circumstances.

In the event the Agencies decide to incorporate examples of tests into the Guidelines, the nature of the tests should be clear. For example, the specific tests mentioned by the Agencies--penetration and intrusion detection tests—are not adequately descriptive. If the Agencies mean automated tools that scan networks for weaknesses, these are not "penetration and intrusion

detection tests," they are vulnerability assessment tools. "Penetration and intrusion" testing refers to what is commonly known as "hacking," which takes a piecemeal approach to testing and depends greatly on the "hacking skills" of the those conducting the tests.

Conduct and Review of Tests by Independent Parties

Section III.C.3. requires tests to "be conducted, where appropriate, by independent third parties or staff independent of those that develop or maintain the security programs" and test results to be "reviewed by independent third parties or staff independent of those that conducted the test." These requirements appear to mandate both independent testing *and* independent review of the independent testing. While independent review of non-independent testing *or* independent testing is appropriate in many circumstances, requiring both activities to be both activities would be redundant and unnecessary.

Also, the requirement that testing be performed by someone "independent of those that develop or maintain the security programs" fails to recognize that those who develop or maintain the security program may already be independent of those that implement or administer the security program. For example, a data security department might develop a program that is independently reviewed by the audit department and administered by the user department responsible for the particular application. While this situation provides adequate independent review of both the program and its implementation, it would not meet the requirements set forth in the proposed Section III.C.3.

We suggest replacing the final two sentences of proposed Section III.C.3. with the following: "Appropriate independence between parties involved in monitoring, testing, and reviewing testing of security programs will be maintained."

Outsourcing Arrangements (Section III.D.)

We believe that the proposed section governing oversight of outsourcing arrangements would create a standard that financial institutions will be unable to meet, particularly as it refers to "monitoring" of outsourcing agreements. For example, it would be nearly impossible for financial institutions to "monitor" compliance by mail houses and other third-party vendors. Rather, we support a standard that requires initial due diligence that reflects each institution's business structure and complexity and involves commitment by third parties to appropriate protection standards. The Guidelines also should acknowledge that the degree of sensitivity of the information to which the third party provider has access should be considered during the due diligence process. Each institution could be expected to include provisions in contracts to promote the protection of customer information.

CONCLUSION

We thank the Agencies for considering our comments and appreciate the Agencies challenge in developing guidelines in this area that are beneficial to consumers, yet are reasonable and do not place an undue burden on financial institutions. If you have any questions concerning this letter or if you would like us to provide any additional information, please do not hesitate to contact me at 205/933-4268.

Very truly yours,

/s/ Joseph B. Cartee

Joseph B. Cartee
Senior Corporate Counsel
Compass Bank