48427.pdf

(20)

Gottlieb, Mary H

From: Hurwitz, Evelyn S on behalf of Public Info
Sent: Friday, August 25, 2000 4:55 PM
To: Gottlieb, Mary H
Subject: FW: Standards for Safeguarding Customer Information

safeguarding customer info, le...

-----Original Message-----
From: Robert Rowe [mailto:Robert_Rowe@icba.org]
Sent: Friday, August 25, 2000 2:27 PM
To: comments@fdic.gov; regs.comments@federalreserve.gov; regs.comments@occ.treas.gov; public.info@ots.treas.gov
Subject: Standards for Safeguarding Customer Information

Attached is a comment letter from the Independent Community Bankers of America (ICBA) addressing the agency proposal on Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness.

Please call the undersigned if you have any questions or need any additional information.

Robert G. Rowe, III
Regulatory Counsel
Independent Community Bankers of America
One Thomas Circle, NW -- Suite 400
Washington, DC 20009
voice: 202-659-8111
fax: 202-659-3604
e-mail: robert_rowe@icba.org

(20)

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 & C Streets, NW
Washington, DC 20551

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

Manager, Dissemination Branch
Information Management Services Division
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552

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

Dear Sir or Madam:

The Independent Community Bankers of America (ICBA)[1] has carefully reviewed and considered the agency proposal on safeguarding customer information, as announced in the *Federal Register* of June 26, and is pleased to offer the following comments.

---

[1] ICBA is the primary voice for the nation's community banks, representing nearly 5,300 institutions at nearly 16,200 locations nationwide. Community banks are independently owned and operated and are characterized by attention to customer service, lower fees and small business, agricultural and consumer lending. ICBA's members hold nearly $439 billion in insured deposits, $526 billion in assets and more than $314 billion in loans for consumers, small businesses and farms in the communities they serve.

The privacy provisions of the Gramm-Leach-Bliley Act (GLB) require the federal bank regulatory agencies to establish appropriate standards relating to administrative, technical, and physical safeguards for customer records and information. The agencies have issued a proposal to implement these requirements.

The ICBA finds the agencies have developed a thorough proposal. We generally support the use of guidelines that offer a great deal of flexibility and allow banks to adapt the requirements to their own particular needs and circumstances. However, the key is to allow as much flexibility as possible and avoid mandating a particular process for establishing a security information plan, or mandating required elements for the plan or testing procedures. We have made a number of additional recommendations, such as eliminating the need for a designated Corporate Information Security Officer and requiring regular board reports, that we believe will help maintain the flexibility needed to reduce the potential burden and costs of this proposal for community banks. We also recommend that a set of examples be issued by the agencies to help community banks comply with these guidelines. Finally, we believe revisions should be made to the proposed oversight for outside service providers to make the guidelines more manageable for community banks.

Rescission of Y2K Guidelines. As part of this proposal, the agencies are considering rescission of their Y2K guidelines, since the Y2K date has now passed. The ICBA agrees this would be appropriate. Through the hard work and diligent effort of banks and their employees and the exemplary cooperation between regulators and banks, the century date change passed with no major problems. Since the event has now passed, the guidelines are no longer needed.

Background and Overview

The primary purpose of this proposal is to address the issue of safeguarding customer information. GLB section 501 requires the federal banking agencies, the Securities and Exchange Commission and the National Credit Union Administration to "establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical and physical safeguards –

a) to insure the security and confidentiality of customer records and information;
b) to protect against any anticipated threats or hazards to the security or integrity of such records; and
c) to protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer."[2]

The agencies have now proposed guidelines – as opposed to regulations - to carry out this requirement. Generally, the guidelines describe the agencies' expectations for the creation, implementation and maintenance of a comprehensive customer information

---

[2] GLB section 501(b)

security program. Such a program would have to include administrative, technical and physical safeguards appropriate to the size and complexity of the bank and the scope of its activities. The oversight role of the bank's board of directors and management's continuing duties are also outlined. The agencies state that many of the requirements incorporated into this proposal already exist in guidelines previously provided on information security and technology by the agencies and the Federal Financial Institutions Examination Council (FFIEC).

While there are no explicit enforcement provisions in the guidelines, the agencies make it clear that they would be enforced under their general powers to address unsafe or unsound practices.

Guidelines vs. Regulations. The ICBA fully supports the use of guidelines as opposed to regulations in this instance. As suggested in the proposal, guidelines will provide a much more flexible system for banks than would regulations. Moreover, since these guidelines address an area that is rapidly changing, guidelines will be more adaptable than regulatory requirements to changes as they take place. However, it is critical that examiners understand that the guidelines offer banks room to adapt the requirements to their own individual situation, and are not rigid requirements. Otherwise, we fear the guidelines will become unnecessarily overly burdensome for community banks. Therefore, for the guidelines to work properly, thorough examiner training and understanding of the application of the guidelines will be critical.

Scope of Guidelines; Customer Information

The guidelines would apply to "nonpublic personal information" of "customers" as those terms are defined in the final privacy rules. The ICBA believes that it is appropriate to have a definition that is consistent with the existing privacy rule. It is simpler, less costly and certainly less confusing for banks, especially community banks, to manage regulatory compliance when definitions are the same. Consistency between regulations also helps avoid misunderstandings.

Under the proposal, *customer information* would be defined as "any records, data, files, or other information containing nonpublic person information . . . about a customer, whether in paper, electronic or other form, that are maintained by or on behalf of the bank." The agencies anticipate that, "for the sake of simplicity," banks are likely to apply these safeguards to *all* customer records, although technically they would not cover business customers nor consumers who have not established an ongoing relationship with the bank (e.g., someone who merely uses a bank's ATM without having an account relationship).

The ICBA agrees that the practical difficulty of distinguishing subcategories of individuals who use bank services will mean that banks will apply these guidelines to all. For many community banks with sole proprietors and similar small business customers, inability to easily distinguish between business and non-business customers – combined with the fact that customer data files often overlap -- makes it unlikely that community banks will apply different security standards for business and non-business customers. More important, irrespective of federal guidelines, community banks regard the sanctity of

customer information for *all* their customers as equally important. However, to keep the requirements of these guidelines consistent with those of the final privacy rules, the ICBA believes the definitions should be the same between these guidelines and the privacy rules.

Development and Implementation of an Information Security Program

The agencies have identified four essential steps to the development of an information security program:

1. identify and assess the risks that may threaten customer information;
2. develop a written plan with policies and procedures to manage and control these risks;
3. implement and test the plan; and
4. continually adjust the plan to account for changes in technology, the sensitivity of customer information, and threats (internal and external) to information security.

While to a certain extent, most banks already have some type of information security policy in place, the proposed guidelines anticipate a greater involvement by the board and senior management by assigning specific certain duties to the board and management.

Board and Management Responsibilities

Board Responsibilities. Under the proposed guidelines, the bank's board would be required to:

- approve the bank's written information security policy and program
- oversee efforts to develop, implement, and maintain an effective information security program

We agree that the information security program is a compliance matter over which the board should reasonably be expected to exercise oversight. And, the board should be expected to oversee the initial implementation of the program. However, once the policy has been properly implemented, it should become one more aspect of the general oversight responsibilities of the board. Day-to-day supervision of the program is a management responsibility, not the board's, and the final guidelines should make this clear.

Board Reports. Under the proposal, the board also would have to regularly review reports from management on the information security program. The ICBA does not agree that regular reports to the board of directors should be mandated. Such a requirement imposes a degree of formality and burden on the board process that is unnecessary for most community banks. Management should be expected to alert the board only to the need for changes or to special occurrences (e.g., computer intrusion) that require board attention. Routine reports take up the time of the board, leaving them less time to focus on

other matters of importance (e.g., the bank's strategic plan). Therefore, the ICBA does not believe it is necessary that the final guidelines mandate routine management reports to the board concerning the security information program, beyond a statement that management should keep the board apprised of extraordinary developments or updates/revisions to the policies and procedures.

However, if the agencies determine that regular reporting is needed, the ICBA believes that the guidelines should mandate routine reports no more frequently than annually (absent any special occurrences that need to be brought to the board's attention sooner). Without guidance on the minimum frequency for board reports, overzealous examiners might criticize a bank for what the examiner concludes are insufficiently regular reports. The ICBA believes that an annual report on the program should be more than adequate.

Management Responsibilities. Under the guidelines, bank management would be required to:

- evaluate the impact of changing business arrangements on the bank's security program (including mergers, joint ventures and outsourcing)
- document compliance with the guidelines
- keep the board informed of the current status of the information security program through regular reports on overall status, including *material* matters relating to risk assessment, testing, attempted or actual security breaches, management's response to those breaches, and recommendations for improvement

Overall, the ICBA agrees with the proposed outline for management responsibilities. The ICBA believes it is important, though, that the final guidelines stress that the detail and extent of a bank's information security program should correlate with the bank's size and complexity of operations. The agencies have done that in other regulations, and it would be especially appropriate for these guidelines.

The ICBA is also concerned about the requirements for documentation to demonstrate that each step outlined has been considered. The important element is that a bank develop an information security program appropriate to its size and risk profile. While the steps and elements outlined in the proposal should be considered, it is not necessary that a bank document all actions involved in deciding to adopt or not implement a particular step or element. The information security program should be evaluated as a final product, and not the process that produced the program.

Management and Control. The proposed guidelines would establish the elements of a comprehensive risk management plan that each bank should take into consideration when establishing its own written policies and procedures commensurate with the sensitivity of information as well as the complexity and scope of the bank and its activities. Under the proposal, each bank should consider appropriate:

- access rights to customer information

- access controls for customer information (including controls to ensure that only authorized individuals or companies have access)
- restrictions on physical access to places where customer information is housed
- encryption of electronic customer information in storage or transit
- procedures to confirm that modifications to the bank's customer information system are consistent with the bank's customer information security policies
- dual control procedures, segregation of duties and background checks for employees with access to customer information
- contract provisions and oversight mechanisms for customer information handled by service providers
- mechanisms to detect actual or attempted attacks on customer information systems – and appropriate responses
- protections against threats to customer information from physical hazards such as fire and flood
- protections against threats from technological problems (and possible backups to reconstruct customer information)

The guidelines also would mandate a training program for all employees that teaches them to recognize fraudulent attempts to access customer information and, where appropriate, report such attempts to the appropriate authorities.

Generally, the ICBA believes that the listed elements are appropriate for banks to consider. However, in order to avoid undue burden, the final guidelines should specifically clarify that these are not requisites but recommendations for consideration. In addition, the ICBA notes that dual control procedures are part of the normal operations of a bank and do not need to be restated here. If they are repeated, the agencies might consider emphasizing that the requirement is part of normal audit procedures and is merely being restated here for assistance.

Best Practices. The ICBA believes that examples of information security practices that banks have used and found successful would be useful to include in the guidelines. So-called "best practices" offer a bank a set of models or methods that can be reviewed and adapted to fit its own particular needs and circumstances. And, since this is an area that is changing rapidly with new developments in technology, "best practices" can regularly be supplemented and updated by the agencies.

Need for Detailed Guidance. The agencies ask for comment on the amount of detail that should be provided in the final guidelines. While detailed guidance can aid compliance, it also raises concerns. On the one hand, regulatory expectations would be clearly delineated. If the specific requirements are reasonable and workable and do not create significant administrative or regulatory burden, they would be useful. However, the more specific the guidelines, the greater the danger they can become rigid and burdensome, and detract from the flexibility needed to account for differing circumstances among banks.

There is also a concern that examiner exuberance can mean that any item mentioned in a guideline is a *de facto* requirement, whether or not it is logical for the risks

and needs of a particular bank. As a result, small, community banks may find themselves in the position of having to take steps to "safeguard" customer information that are unnecessary, burdensome and overkill.

The ICBA believes that broad guidelines supplemented by models and best practices examples provided by the agencies, coupled with thorough examiner training on the flexibility of the guidelines, would be the most appropriate approach.

Corporate Information Security Officer. The ICBA does not believe it is necessary to require a bank to designate a specific individual with the title of Corporate Information Security Officer. While specifying a single individual has the benefit of placing all responsibilities for safeguarding customer information in one place, it also detracts from the flexibility of the guidelines. Especially for small, community banks, it may be more appropriate to spread the responsibilities among a number of different individuals within the bank. For many banks, it is likely that these responsibilities will be assigned entirely to the compliance officer, but for other banks, responsibility may rest with the chief technology officer, the internal auditor or operations. Or, a bank may assign different parts of the program to different areas. The important element is that the bank have an information security program, not an individual designated as the Corporate Information Security Officer.

Testing. The proposal would require regular testing to ensure that customer information security policies and procedures are being followed and that risks are being properly identified and addressed; that tests "be verified by an independent third party or staff independent of those who conducted the tests;" that test frequency be established relative to the risk presented by the bank's overall; and that testing be properly documented.

Testing requirements can be cumbersome, costly, and time consuming for community banks. Accordingly, it would be helpful if the agencies provided guidance on the types of testing a bank should consider conducting in analyzing its own information security program. Testing is an area where best practices would be especially useful, by outlining the types of tests that are available and the situations under which different types of tests are better suited. Then, based on its own assessment of its risk file, each bank would be able to institute such tests as it deems necessary.

Since the review being mandated is essentially an audit of bank policies and procedures, the ICBA recommends that the bank's own staff be allowed to conduct these tests. If the bank has an internal auditor, that person may be the most appropriate individual to conduct the review. Or, the bank compliance officer may be the one most suited to the task. As long as an individual with sufficient independence under standard auditing procedures does the review, that should be acceptable. Requiring a bank to hire an outside firm to conduct such tests would be an expensive proposition for many community banks. And, many community banks operate in small, rural areas, where finding an outside auditor to conduct testing can be difficult.

Outside Review. The proposal would require independent review of test results. While the ICBA believes that it is appropriate to require some kind of review of test results,

the ICBA urges the agencies to specify that bank staff may conduct the reviews of test results as well. The ICBA also recommends that the guidelines not specify how much independence a reviewer should have. Normal audit procedures should provide ample guidance. However, the individual conducting the review, as well as the individual conducting the original tests of the information security program, should have the authority to report any findings directly to the board of directors to ensure that any potential problems or concerns are brought to the board's attention.

Outsourcing

Under the proposal, banks would be responsible for the security practices of outside vendors or service providers that handle customer information for the bank. According to the proposal, "an institution should 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 proposal does not explicitly establish the extent of that due diligence.

While many community banks process information in-house, many also rely on outside vendors for some or all of their data processing needs. Community banks take great care in selecting these outside vendors, since the performance of the vendor reflects directly on the performance of the bank in the eyes of its customers. The ICBA believes that careful selection of a service provider by the bank should be sufficient. A regulatory requirement that banks conduct reviews, audits, and/or some form of examination of the information security programs of third parties is unduly burdensome and beyond the scope of the statutory requirements. Moreover, the costs and responsibilities associated with such reviews could make it cost prohibitive to use the services of outside vendors which in turn would limit the products and services that the bank—especially a community bank—might be able to offer customers. Banks cannot control nor be held responsible for the actions of unaffiliated third parties. The bank takes care in selecting high-quality, trusted vendors, and can enforce any breach of a confidentiality agreement that occurs, but to require it to do more would be unreasonable.

Contract provisions in vendor agreements are the preferred way to address this issue. Any regulatory requirement that specifies certain contract provisions, though, should only apply to contracts that are entered *after* the effective date of the guidelines. Contract provisions could be used to outline the expectations and responsibilities between the parties, and any breach of those provisions could be addressed through normal legal remedies.

However, it is important the final guidelines also take into account the fact that small, community banks have very little negotiating power in contract arrangements with outside service providers, especially large service companies that have hundreds of community bank customers. These vendors are not likely to be willing to accept variations on their standard contract forms from dozens of community banks, each requesting unique and individual elements in their contracts. While banks might consider asking vendors to

include such provisions, it is imperative for the regulatory agencies to recognize that the vendors can just as easily decline such requests.

The agencies have also suggested that banks review or audit the performance of outside service providers. This is an unnecessary requirement that is impractical and unworkable. Community banks do not have the resources and should not have to incur the expense of conducting such a review. And vendors are unlikely to grant access for such review, particularly from hundreds of individual institutions. Therefore, the ICBA opposes any requirement that a bank be required to audit its outside service providers.

The bank regulatory agencies have the authority to examine third party vendors that provide data processing and software services for banks. During the months leading up to the century date change, the agencies used this authority to examine vendors to ensure they were adequately prepared for Y2K. The assurance that bank customer information is properly secure is another area where the bank agencies could play an active role, inasmuch as the agencies are in a much better position and have greater resources to conduct such reviews. In addition, this would centralize the review process and avoid duplication by each customer of the vendor or service provider.

Community Banks

The ICBA is very concerned that the proposed standards offer the potential to become unreasonable or unrealistic for community banks. Detailed requirements in an information security program are more appropriate for a large institution that requires more structure and formalization of policies and procedures. If the final guidelines are sufficiently flexible – and that flexibility is clearly understood by examiners – and the guidelines do not become mandates, they will be more realistic for community banks. For some small community banks with simple product and service offerings and with low-risk profiles, a simple information security "program" will suffice, and it is important that the final guidelines allow that possibility.

An additional resource that would be helpful for all banks, but especially for community banks, would be a compliance guide on these requirements. Development of a set of model procedures and methods to serve as examples would certainly be useful. Another helpful tool would be a set of questions and answers on meeting the requirements.

Since the agencies recognize the community institutions have less resources at their disposal to address these issues, it also might be appropriate to allow smaller banks, say those under $1 billion, additional time to comply with the guidelines. Since GLB did not mandate or explicitly authorize the agencies to create an exemption for smaller institutions, the reluctance to create one is understandable. However, there is no reason that the agencies could not grant additional time for smaller banks to comply with the requirements. Clearly, complying with the new privacy rules and these guidelines will put a strain on the resources of smaller banks. To alleviate that strain, the ICBA recommends that they be given an additional twelve months, to July 1, 2002, to comply with the final guidelines.

Conclusion

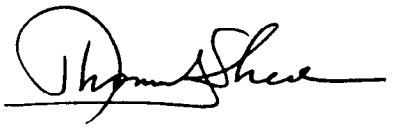
The ICBA commends the banking agencies for proposing guidelines to carry out this requirement, as guidelines will be more flexible and more adaptable to the rapidly changing needs of the banking industry and to the circumstances of individual banks.

We believe that ensuring the guidelines stay flexible is extremely important. Not mandating specifics such as detailed board oversight, regular routine reports to the board, extensive documentation of the process, or designation of specific individuals within the bank to carry out the process will help maintain the flexibility of the guidelines. For all banks, but especially community banks, examples and models that can be adapted to their own particular needs and circumstances will be helpful. And, thorough examiner training in the flexible nature of the guidelines is imperative.

Community banks rely on outside service providers to serve their customers, and because they value the relationship they have with their customers, community banks choose these outside service providers with care. Provided the bank has taken appropriate care in selecting outside vendors, and to the extent it can, included appropriate provisions in its contract with the vendor, that should be sufficient to meet the guidelines. And, for smaller community banks, allowing additional time for them to comply with the guidelines will help alleviate the strain on their resources.

Thank you for the opportunity to comment.

Sincerely,



Thomas J. Sheehan
President