48,414

8

Gottlieb, Mary H

From: Hurwitz, Evelyn S on behalf of Public Info
Sent: Friday, August 25, 2000 11:37 AM
To: Gottlieb, Mary H
Subject: FW: Security Standards Comment Request

-----Original Message-----
From: kkrieger@SummitBank.com [mailto:kkrieger@SummitBank.com]
Sent: Friday, August 25, 2000 9:57 AM
To: public.info@ots.treas.gov
Subject: Security Standards Comment Request

Manager, Dissemination Branch
Information Management & Services Division
Office of Thrift Supervision
1700 G Street, NW
Washington, D.C. 20552

Dear Sir or Madam:

This comment letter is sent by Summit Bancorp, a bank holding company, on
behalf of itself and its subsidiaries, which include two state-chartered banks which are members of the Federal Reserve System, Summit Bank (Hackensack, NJ) and Summit Bank (Bethlehem, PA), a state-chartered bank not a member of the Federal Reserve System, Summit Bank (Norwalk, CT), a registered broker-dealer, Summit Financial Services Group, Inc., and an insurance agency, Summit Insurance Associates.

In general, we appreciate the efforts the regulators have made to propose
consistent and coordinated security guidelines. Summit supports issuing the proposed guidance in the form of "Interagency Guidelines" rather than
regulations. Promulgating guidelines rather than regulations will provide
a greater degree of flexibility for financial institutions. This needed flexibility will promote greater innovation and advances in security procedures and practices that will, in turn, lead to greater protection of
customer information.

SPECIFIC COMMENTS

Rescission of Year 2000 Standards

We agree that rescission of the Year 2000 Standards for Safety and Soundness is appropriate at this time.

Scope of Guidelines

The agencies invite comment on the scope of the guidelines. We urge the agencies to clarify that the guidelines only apply to consumers and customers as those terms are defined by The Gramm-Leach-Bliley Act (GLBA).
Subsection 501(b) of the GLB Act requires that "each agency or authority?
shall establish appropriate standards for the financial institutions

subject to their jurisdiction relating to administrative, technical, and physical safeguards?(1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer" (emphasis added).

In the final rules governing Privacy of Consumer Financial Information, published in the Federal Register on June 1st, the agencies defined "customer" to mean a "consumer who has a customer relationship with a bank." Further, a consumer is defined by those regulations as "an individual who obtains or has obtained a financial product or service from a bank that is to be used primarily for personal, family, or household purposes?" (emphasis added). Given that the agencies have correctly applied the privacy regulation required under Title V solely to "individual" customers, we believe that this guidance should similarly apply only to the records of such customers.

Board of Directors

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 reporting mechanism than reporting to the full board.

Accordingly, at Summit, we believe that the board or a committee of the board should be responsible for providing initial approval of the institution's security policies. Following the initial approval, we believe that management discretion should govern the frequency of reporting. Under this standard, management would be expected to report material exceptions to its board or a committee of the board on an as needed basis.

In the event the agencies do not support this proposal and decide to impose a requirement for periodic reporting, we recommend that annual reports to the board or a committee of the board are more than sufficient.

Standards for Safeguarding Customer Information

Section II outlines proposed objectives for an institution's information security program. Summit supports goal oriented definitions but we are concerned that the objectives proposed by the agencies would create unrealistic and unattainable standards for financial institutions. The proposed 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).

We are concerned that use of the word "shall" suggests that institutions must assure absolute security protection. This standard is likely impossible for any institution to meet. Additionally, use of the word "any" as a modifier to the words "anticipated threats," and "customers or risk" in subsections 2 and 3 is overly broad. Finally, the concept of inconvenience is not an appropriate standard for these security guidelines.

Title V of the GLB Act requires the regulators 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." We believe that use of the term "appropriate" in the GLB statute supports inclusion the phrase "?be designed to reasonably?" in the final regulations.

The agencies indicate in the preamble to the proposed regulation 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." Summit agrees 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 since the customer has clearly authorized access to their account and associated information. Consistent with this view, we would strongly encourage the agencies to include language within the text of the guidelines themselves that reflects the language referenced above that is already included within the preamble.

Manage and Control Risk

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 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. The agencies are encouraged to delete this factor. 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. At the least, the agencies should clarify that factor III(C)(1)(a) is not intended to create a new customer right to access financial information.

Additionally, it is noted that the references to "companies" in factor III(C)(1)(b) should be struck. As stated previously in this letter, we believe that these standards should only apply to consumers and customers as those terms are defined by GLBA. Accordingly, imposing standards for protection of "company" information should be outside the scope of this guidance.

In III(C)(1)(d) the agencies also propose instructing institutions to "consider appropriate encryption of electronic customer information, including while in transit or in storage on networks or system to which unauthorized individuals may have access." This language would require encryption in many cases where encryption is not 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. We recommend the agencies change this section to focus on protection of customer data rather than a particular methodology for doing so. For example, we would suggest the following language to replace the proposed language:

III(C)(1)(d) "Procedures to protect the confidentiality of electronic customer information, for example by encryption of electronic customer information, including while in transit or in storage on networks or systems not controlled and monitored by the bank or its agents."

The agencies invite comment on the degree of detail that should be included in the Guidelines regarding a risk management program. We strongly encourage the agencies to adopt guidelines that provide institutions sufficient flexibility to adopt policies and procedures that best reflect appropriate business and risk management practices for each individual institution.

The agencies ask for comment on whether specific types of security tests, such as penetration tests or intrusion detections should be required. We oppose requiring specific types of tests. Rather, each institution should have the flexibility to design and implement a testing program that is appropriate for their particular systems and requirements. This approach will allow institutions to develop and implement testing programs that are appropriate given the sophistication of each system being tested. We believe that this is consistent with supervision-by-risk principles. Additionally, allowing institutions this appropriate flexibility will promote innovation and improvement that will lead to better security.

The agencies also invite comment regarding the appropriate degree of independence that should be specified in the guidelines in connection with the testing for information security systems and the review of test results. We support the standard put forth in OCC Bulletin 98-38 on Technology Risk Management: PC Banking. The section entitled Audit/Quality Assurance includes the following standard:

> "An objective review of PC banking systems should identify and quantify risk, and detect possible weaknesses in the bank's risk management system as it pertains to PC banking. Management may rely on internal audit, external audit, or other qualified professional sources to conduct this review?".

Each institution should have the flexibility to develop an independent standard that reflects the institution's culture, management reporting structure, and business activities, as well as sound business practices. Developing a one-size-fits-all approach for review of each institution's security standards will not properly reflect the needs or demands of each individual system.

Consistent with this view, we encourage the agencies to strike from section III(C)(3) the words "Test shall be conducted, where appropriate, by independent third parties or staff independent of those that develop or maintain the security programs. Test results shall be reviewed by independent third parties or staff independent of those that conduct the test." It would be appropriate to insert in its place similar language to that cited above from OCC Bulletin 98-38.

Outsourcing Arrangements

Summit believes 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 ensures initial compliance by third parties with appropriate protection standards. Further, the guidance should explicitly recognize 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.

Summit Bank is participating with the Financial Services Roundtable and BITS to form a working group to evaluate the control, security, privacy and customer confidentiality issues associated with outsourced relationships. This working group will evaluate the risks, benefits and control requirements from the request for proposal stage through the audit and assessment process. The group will review current risk assessment practices, as well as opportunities to develop new ones, such as the development of outsourcing criteria by the BITS Financial Services Security Laboratory. The work product of this group will help shape industry requirements.

CONCLUSIONS

Summit Bancorp and its subsidiaries thank the agencies for consideration of our comments. If you have any questions or we can provide additional assistance, please do not hesitate to contact me, Susan Bredehoft, Senior Vice President and Director of Compliance at 609-324-6939, or Lari Sue Taylor, Senior Vice President and Director of Information Security at 201-296-3605.

Sincerely,

Susan U. Bredehoft
Senior Vice President, Director of Compliance
Summit Bank
270 Route 130
Bordentown, NJ 08505

Lari Sue Taylor
Senior Vice President, Director of Information Security
Summit Bank
55 Challenger Road
Ridgefield Park, NJ 07660