Gottlieb, Mary H 48425.pdf (18)

From: Hurwitz, Evelyn S on behalf of Public Info
Sent: Friday, August 25, 2000 4:53 PM
To: Gottlieb, Mary H
Subject: FW: Proposed Interagency Guidelines - Comment Letter

Word 6.0 Windows/
Mac

-----Original Message-----
From: Patricia.Alberto@chase.com [mailto:Patricia.Alberto@chase.com]
Sent: Friday, August 25, 2000 3:54 PM
To: regs.comments@occ.treas.gov; regs.comments@federalreserve.gov; comments@fdic.gov; public.info@ots.treas.gov
Cc: Barbara.DAmico@chase.com; Alan.Weinberg@chase.com
Subject: Proposed Interagency Guidelines - Comment Letter

(See attached file: GLBSTAN4LTR.doc)

18

The Chase Manhattan Bank
One Chase Manhattan Plaza-22
Compliance & Operational Risk
Mgmt.
New York, NY 10081 USA
Tel 212/552-2014

Patricia L. Alberto
Senior Vice President
National Consumer
Services

August 24, 2000

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

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

Communications Division
Office of the Comptroller of the Currency
250 E Street, SW
Washington, D.C. 20219
Docket No. 00-13

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

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

Dear Sirs and Madams:

On behalf of The Chase Manhattan Bank and its affiliates, including Chase Manhattan Bank USA, N.A, Chase Manhattan Mortgage Corporation, Chase Investment Services Corp., Chase Manhattan Automotive Finance Corporation, and Chase Insurance Agency, Inc. (collectively, "Chase"), we welcome the opportunity to provide comments to the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision and the Office of the Comptroller of the Currency (collectively the "Agencies") in connection with the proposed Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness.

We commend the Agencies for their efforts in developing a uniform proposal and recognize the difficulties that were faced by the Agencies. The proposal generally receives our support. Some aspects of the proposal, however, require further clarification, and we would urge the Agencies to provide institutions with somewhat greater flexibility. For example, we are concerned that the Agencies are proposing to mandate unnecessary involvement by the bank's board of directors where responsibilities might more properly be delegated to management. With regard to flexibility, we request

that the Agencies affirmatively state that nothing in the guidelines is intended to preclude an institution from having the discretion to adopt appropriate policies and procedures based upon considerations that may be unique to that institution. In addition, we request that the Agencies affirmatively state that nothing in the guidelines is intended create a private right of action in favor of any party.

Chase is eager to work with the Agencies towards creating a balanced approach that will enable the Agencies to adequately perform their supervisory roles and statutory obligations while both minimizing burdens on financial institutions and helping to ensure that information about customers continues to be adequately protected. It is in that spirit that we offer these comments on the proposal and the ways in which it ought to be improved.

SPECIFIC COMMENTS

Guidelines

The proposal relating to standards for safeguarding customer information was issued in the form of guidelines by the Agencies. We support issuing the final version in the form of "Interagency Guidelines" rather than regulations. The final guidelines should be issued as appendices to the Agencies' applicable regulations for safety and soundness. Promulgating guidelines rather than regulations will provide a greater degree of flexibility for financial institutions and will, thus, allow for greater innovation in the protection of customer related information.

Year 2000 Standards

Chase supports the Agencies' proposal to rescind the Year 2000 Standards for Safety and Soundness. The standards address events that no longer give rise to significant safety and soundness concerns.

Customer Information

Chase urges the Agencies to clarify that the guidelines only apply to individuals who are "consumer customers." The GLB Act requires "standards ...to insure the security and confidentiality of customer records and information" (emphasis added) and in the final rules governing Privacy of Consumer Financial Information, 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). Since the privacy regulations under the GLB Act apply only to individual consumer customers, we believe that the guidelines should have the same coverage, too. Although some banks might opt to apply the same standards to all or certain other records, that should not be required by the guidelines.

Security Program Objectives

Chase is concerned about several aspects of the objectives proposed by the Agencies that would create unrealistic and potentially unattainable standards for financial institutions. The proposed

guidelines provide 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).

First, requiring that a security program shall "ensure" the security and confidentiality of customer information suggests that institutions must assure (or guarantee) absolute security protection. We currently go to great lengths to protect sensitive data and continually refine our practices. An "ensure" standard may, however, be impossible for Chase or any institution to meet and gives rise to unreasonable expectations among our customers. Therefore, we suggest that the term be changed to "protect," which is used in subsections 2 and 3. In addition, the lead in language should be changed from "shall" to "shall be designed to" in order make clear that an absolute protection standard is not intended. Incorporating these changes, element one in the security program objectives would be stated as follows: "A bank's information security program shall be designed to: 1. protect the security and confidentiality of customer information."

Second, protecting against "any anticipated" threats or hazards to the security or integrity of information is overly broad. A financial institution can not be expected to protect against every conceivable threat. Therefore, we propose that the language in element two in the security program objectives should be revised to read, "protect against reasonably anticipated and preventable threats or hazards to the security or integrity of such information." (Emphasis added).

Third, in the preamble's section-by-section analysis of the proposed guidelines, the Agencies indicate that "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 statement and we believe that financial institutions should not need to develop security procedures with respect to access to or use of customer information with the customer's consent. Furthermore, it should not matter whether the financial institution is aware that the customer granted access to another party. (For example, this can occur in "screen scraping" by account aggregators, where a customer provides a third party with authorization and personal identification code to access the customer's financial information unbeknownst to the financial institution.) We request that the agencies include some form of the above-quoted preamble language within the text of the guidelines. One way the Agencies could achieve that would be to add a definition of "unauthorized access" to the guidelines based on the preamble language.

The definition should make clear that access is unauthorized where there is a lack of customer consent or access was gained contrary to the information security program and procedures of the bank. We propose that "unauthorized access" should be defined as, "access gained without customer consent and not in substantial compliance with the information security program and procedures established by the bank."

Finally, protecting against unauthorized access to or use of information that could result in substantial harm "or inconvenience to any customer" could be read to impose an unwarranted new standard. While the word "inconvenience" is used in the GLB Act, this language should be

deleted or clarified because it is not an appropriate standard for information security guidelines and customers are protected in this regard by the privacy regulations issued under the GLB Act. If, however, the Agencies choose not to delete it, they should explain that such a standard is not intended to add new requirements to the regulatory protections already in place. Our suggestion is that element three in the security program objectives should be revised to read as follows: "3) protect against unauthorized access to or use of such information that could result in substantial harm to a customer or risk to the safety and soundness of the bank."

Board of Directors

The degree to which actual board of directors involvement is required ought to depend on the financial institution's structure, the nature of its business and the materiality of the information. For example, organizations with multiple subsidiaries and affiliates should not necessarily be required to have extensive board involvement for each. The guidelines should not dictate the degree of involvement of the board, but rather each institution should make that determination and the guidelines should be designed to establish only an appropriate baseline.

Chase recommends that the base requirement set forth in the guideline should simply be that the relevant board of directors of the subsidiary or, if appropriate, of the holding company, should review the institution's information security policy and program and should not be required to formally approve it. It is a common corporate practice for a board to review and comment upon policies and programs developed by management. The policy and program will be subject to changes from time to time, and such changes will not be able to be implemented expediently if there is a specific requirement that the institution's policy and program have board approval. To arbitrarily require board approval of each and every minor change would be unduly burdensome and would detract from the board's ability to consider other matters that may be more important or urgent at that time, including matters that have an immediate bearing on overall safety and soundness. The proposed guidelines already provide for board oversight of the program and that is consistent with our above recommendation. An institution should be permitted to involve individuals of appropriate levels and expertise to assume any required responsibilities. Certainly, the board should not be required to be involved in the formulation of the program. In addition, flexibility of this sort will allow a security program to be approved more rapidly and, thus, minimize the burden on an institution of having to have a program in place by July 1, 2001.

In response to the Agencies' request for comment, Chase also believes that management discretion should govern the frequency of any reporting. Under this standard, reports of material exceptions would be made to the board on an as needed basis. If, however, the Agencies choose to specify a requirement, we suggest that it be "periodic reporting." In addition, if the Agencies decide to impose a requirement for the frequency of periodic reporting, we respectfully suggest that annual reports to the board would be sufficient.

The Agencies also ask whether the board should be required to designate an individual to develop and administer the program subject to board approval. For the reasons above, we believe that the board should be permitted to designate such a person, but there ought to be no requirement that it do so.

Manage and Control Risk

We have several comments on the Agencies' list of proposed factors that an institution should consider as potentially appropriate in establishing security policies and procedures. First, in general, we request that the Agencies clarify that the listed factors are simply factors to be considered by the institution, and that the institution have discretion whether to apply the factor in particular circumstances as it deems appropriate. This issue is illustrated in our points on encryption and dual controls below.

Second, factor III(C)(1)(a) states that in banks should consider appropriate "access rights to customer information." We believe that the purpose to be served by this reference is that financial institutions should consider which employees and third parties ought to have access and what security measures are appropriate to prevent unauthorized access to customer information. Because this statement could be misinterpreted to imply that customers are being given rights to access financial information maintained by a financial institution, we suggest that Agencies delete this factor. The other factors listed, including III(C)(1)(b) and (c), ought to be adequate for the Agencies' purpose. Alternatively, the Agencies should revise factor III(C)(1)(a) to indicate that it applies to third party access to information about customers and to clarify that it is not intended to create a new customer right to access financial information. We suggest that this factor should be restated as follows: "each bank should consider appropriate access rights of employees and third parties to customer information."

Third, factor III(C)(1)(d) instructs 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." We request the Agencies to clarify that this does not require encryption in cases where encryption is not appropriate. Encryption can be an appropriate approach to protecting certain confidential data while it is in transit and perhaps in other circumstances.

We do not believe that the Agencies intended to require use of encryption when it would not be necessary (e.g., the information is not highly sensitive and a determination is made that disclosure of the information will not result in financial damage). Unnecessary encryption would be burdensome to the institution and its customers. We suggest that this factor might be revised to read: "each bank should consider appropriate procedures, such as encryption, to protect the confidentiality 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."

Lastly, we have a similar concern with factor III(C)(1)(f) relating to dual control and segregation of duties. Proper controls may be in place to restrict access to customer information on a need to know basis, but there likely will not be full dual controls or segregation of duties in a paper-based documentation environment, and we do not think that it is necessary. Dual controls or segregation of duties would not be practical and would negatively affect efficiency, work flows and staff resources where there is a need to have access to this information during the work day in order to perform normal duties. We request that the Agencies clarify that this factor does not require dual controls or segregation of duties in cases where dual controls or segregation of duties are not appropriate.

The agencies invite comment on a number of other questions related to this section. They have, for example, posed a question regarding the degree of detail that should be specified in the guidelines regarding a risk management program. We believe that detailed requirements may be counterproductive. We urge the Agencies to provide each institution with sufficient flexibility to adopt appropriate policies and procedures based upon considerations that may be unique to that institution.

The Agencies have also asked whether specific types of security tests, such as penetration tests or intrusion detections, should be required. We do not believe that types of tests should be required. Again, each institution should have the flexibility to design and implement a testing program that is appropriate for its particular systems and procedures. Such flexibility will promote innovation and improvement that will benefit the entire industry.

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. Chase believes that institutions should consider the independence of individuals performing these tasks, but the guidelines should not specify the extent to which independence is required. An institution should have the flexibility to use internal audit, external audit, or other qualified professionals to conduct testing and reviews. There should be no requirement that testing or reviews of testing be conducted by independent third parties. Independence can be assured where there is "segregated reporting" – that is, where tests are conducted by staff independent of those that develop or maintain the security programs and where test results are reviewed by staff independent of those that conduct the test.

Outsourcing Arrangements

Chase has concerns about the proposed section on oversight of outsourcing arrangements. Under the proposed guidelines, financial institutions will be required to exercise due diligence in "managing and monitoring" outsourcing arrangements. The term "monitor" could be interpreted to require ongoing supervision that extends beyond an auditing function. We believe it would be nearly impossible for financial institutions to "monitor" compliance by each of its vendors. We suggest that the due diligence requirement instead apply to "establishing and managing" the outsourcing arrangement. This standard would require and emphasize initial due diligence' but would require a somewhat lesser burden of ongoing oversight of third parties' compliance with appropriate protection standards. One exception to this standard is needed, however, to "grandfather" contractual arrangements that are already established to allow time to bring agreements into compliance at the later of July 1, 2002 or at the end of their current term. Also, we request that the guidelines clarify that the degree of due diligence required would depend on the sensitivity of the information to which the third party provider has access.

The Agencies request comments on a number of related points that affect outsourcing arrangements. They ask whether there are industry best practices to monitor the security precautions of service providers. We believe each institution needs to determine the appropriate treatment of a particular arrangement based on its unique facts and circumstances. Best practices could become minimum requirements that produce inappropriate burdens. Nevertheless,

minimum standards could be helpful. For example, institutions could be expected to include provisions in contracts to promote the protection of customer information. This point is related to the Agencies' inquiry on whether service providers sometimes do not accommodate requests for such contractual provisions. At times, they object to such provisions and, where that occurs, it is unclear whether institutions, in particular smaller institutions, have the negotiating leverage to overcome the objections. Specific contractual provisions in the guidelines could help these institutions, but would be problematic in our view. We believe that a "one-size-fits-all" approach is inappropriate and that contractual provisions need to be tailored to the particular circumstances. Another example of minimum standards that could be helpful is the use of what are commonly known as Type II SAS 70 reports. These reports, under which service providers commission comprehensive, regular audits from third-party organizations, are frequently used as external audit tools.

* * *

Chase appreciates the opportunity to comment and thanks the Agencies for consideration of our comments. We understand that the Agencies are striving to develop guidelines that strike an appropriate balance between specifying requirements for controlling risk and providing flexibility to financial institutions to minimize their burdens. If Chase can be of further assistance in these efforts, please do not hesitate to contact Patricia Alberto at (212) 552–2014.

Very truly yours,

Patricia L. Alberto

Patricia L. Alberto
Senior Vice President