0

OCC ADVISORY LETTER

Comptroller of the Currency
Administrator of National Banks

Subject: Privacy Preparedness

TO: Chief Executive Officers and Compliance Officers of All National Banks, Department and Division Heads, and All Examining Personnel

PURPOSE

This advisory is to help prepare you for the implementation of the new Privacy of Consumer Financial Information regulation, 12 CFR 40. The regulation becomes fully effective on July 1, 2001, and it affects all national banks, large and small, including most of their subsidiaries. A questionnaire is attached to assist you in your preparations and in performing a self-assessment. During the 2001 quarterly reviews conducted with your bank, your examiner-in-charge or bank portfolio manager will include a discussion of this advisory, the results of your self-assessment, and your progress toward full compliance with the provisions of 12 CFR 40. The extent of that discussion will be determined by the size of the institution involved, the nature of its information collection and sharing practices, and any concerns the examiner may have regarding the state of the bank's preparedness.

BACKGROUND

Title V of the Gramm–Leach–Bliley Act (GLBA) of 1999 sets forth provisions addressing the obligations of a financial institution with respect to the privacy of consumers' nonpublic personal information. The Office of the Comptroller of the Currency's (OCC's) implementing regulation, 12 CFR 40, Privacy of Consumer Financial Information, provides for disclosures to consumers of a financial institution's privacy policy and the rights of consumers to direct their financial institution not to share their nonpublic personal information with third parties (opt out). A copy of the regulation is included in OCC Bulletin 2000-21 ("Privacy of Consumer Financial Information"), issued June 20, 2000. In addition, OCC Bulletin 2000-25 ("Privacy Laws and Regulations"), issued September 8, 2000, provides information and guidance regarding the various federal laws and regulations relating to the disclosure of consumer financial information.

Many who commented on the proposed rule stated that they needed more time than was provided in the statute to comply with the regulation. Commenters noted that they needed extra time to assess existing information practices, prepare new disclosures, develop software to track opt outs, train employees, and create management oversight, internal review, and auditing systems to ensure compliance. As a result of the comments, the agencies exercised their authority under section 510(1) of the GLBA and extended the mandatory compliance date. Financial institutions

are expected to be in full compliance with the regulation by July 1, 2001. Full compliance means that an institution has delivered a privacy notice to its customers and, where applicable, has afforded its customers a reasonable opportunity to opt out of information sharing before July 1, 2001. These institutions may continue to share nonpublic personal information after that date for customers who do not opt out.

PRIVACY PREPAREDNESS MEASURES

Senior management and the boards of directors of national banks and their subsidiaries are strongly encouraged to ensure that their institutions take all appropriate steps before the mandatory compliance date so that their institutions will comply fully with the privacy regulation by the July 1, 2001, deadline. The term "bank" in this advisory includes national banks, federal branches and agencies of foreign banks, and subsidiaries of a national bank or federal branch or agency, except subsidiaries that are brokers, dealers, persons providing insurance, investment companies, investment advisers, and entities subject to regulation by the Commodity Futures Trading Commission.[1] These steps should include

- Assessing existing information practices by conducting an inventory of information collection, disclosure, and security practices;
- Evaluating agreements with nonaffiliated third parties that involve the disclosure of consumer information;
- Where necessary, establishing mechanisms to permit and process opt-out elections by consumers;
- Developing or revising existing privacy policies to reflect the new regulatory requirements;
- Determining how to deliver privacy notices to consumers;
- Establishing employee training and compliance programs; and
- Developing an implementation plan.

Assessing Existing Information Practices. Banks are encouraged to assess their existing practices with respect to nonpublic personal information in order to (1) accurately represent them in their privacy policies; (2) determine the extent to which disclosures to third parties fall within the statutory exceptions; (3) evaluate which information disclosures, if any, would trigger opt-out rights for consumers; and (4) determine whether any practices are prohibited, *e.g.*, impermissible sharing of account numbers with third parties. This exercise should also assist banks in evaluating the desirability of continuing or altering existing practices.

[1] Certain functionally regulated subsidiaries, such as brokers, dealers, and investment advisers will be subject to privacy regulations issued by the Securities and Exchange Commission. Insurance entities may be subject to privacy regulations issued by their respective state insurance authorities.

Evaluating Agreements with Nonaffiliated Third Parties that Involve Disclosure of Consumer Information. Banks should determine whether their agreements with nonaffiliated third parties that involve the disclosure of nonpublic personal information meet the regulatory requirements for maintaining the confidentiality of the bank's consumer information. For instance, if a bank discloses customer lists to a nonaffiliated third-party service provider to market the bank's own products or services, or to a nonaffiliated financial institution pursuant to a joint marketing agreement, section 40.13 of the regulation requires the bank to enter into a contract limiting the third party's use or disclosure of that information. Additionally, banks should consider how best to maintain the confidentiality of the consumer information they disclose pursuant to other nonaffiliated third-party arrangements, such as routine service agreements. Under the regulation, any nonaffiliated third party that receives nonpublic personal information from a bank is limited in its ability to use or disclose the information. Banks are encouraged to inform their service providers to familiarize themselves with these limitations. Moreover, banks that obtain nonpublic personal information from other nonaffiliated financial institutions also face limits on their use or disclosure of this information.

Establishing Mechanisms to Handle Opt-Out Elections. Banks that disclose information to nonaffiliated third parties outside the statutory exceptions must provide their consumers with a mechanism to opt out of that information sharing. Banks must ensure that they meet the regulatory requirements for providing consumers with a clear and conspicuous opt-out notice and a reasonable means to do so (*e.g.*, a convenient mechanism for opting out and a reasonable period of time (*e.g.*, 30 days)). In addition, banks must devise the means to record, maintain, and effectuate opt-out elections by consumers.

Developing a Privacy Policy. The regulation requires that all banks, even those that do not share nonpublic personal information, provide privacy notices to customers. Institutions must develop or revise existing privacy notices to conform them to the new privacy requirements. The notices must meet the clear and conspicuous standards, and they must accurately reflect the bank's privacy practices. In developing their privacy practices and notices, banks may want to evaluate the competitive aspects of their policies and obtain consumer input (*e.g.*, as to whether consumers understand and accept the policy).

Delivering Privacy Notices. Banks must determine the mechanism to deliver initial, annual, and revised privacy notices and opt-out notices to customers, consumers, and joint account holders. Methods of delivery may include hand delivery, mail, and electronic delivery where the consumer is conducting business with the bank electronically and agrees to electronic disclosures. Banks should deliver privacy notices to customers, and where applicable, afford them a reasonable opportunity to opt out of information sharing before July 1, 2001.

Establishing Training Programs. All bank employees should have a general understanding of the bank's privacy policies; however, certain employees require more detailed knowledge. Customer service personnel, personnel who process requests for consumer information or who provide such information to third parties, and other employees in contact with consumers must have a thorough understanding of the bank's privacy policies and practices. They should be prepared to answer questions about the bank's privacy policies and practices, address whether an individual consumer's records are shared, direct consumers through the bank's complaint

process, and if applicable, provide notices to consumers. Bank training programs should be customized for the audience, should be ongoing, and should provide follow-up when problems are noted.

Establishing Compliance Programs. Banks should ensure that their compliance personnel are involved in the privacy preparations. Compliance should evaluate the bank's privacy practices and measures undertaken to ensure regulatory conformance. Internal controls, policies, and audit procedures should be developed, and audits/compliance reviews scheduled, in time for the July 1, 2001, implementation date. Implementation problems and compliance deficiencies identified by the compliance staff should receive immediate attention by senior management.

Developing an Implementation Plan. To ensure timely and adequate compliance with the new privacy requirements, banks should develop a privacy action plan that takes into consideration the above measures, as appropriate. The plan should be approved by senior management and the board, and should include target dates, goals, and responsible parties. Also, it should call for testing and progress reports.

Attached to this advisory is a privacy preparedness questionnaire that may be used to perform a privacy self-assessment. It sets forth measures for implementation and compliance. The questionnaire is a general guide that addresses a broad scope of application, and as a result, some questions may not be applicable to your financial institution. During the 2001 quarterly reviews of your bank, examiners will inquire about your privacy policies and preparations, and the results of any self-assessment. They will use the attached questionnaire to ask applicable questions about your privacy readiness and may also offer suggestions to improve your compliance efforts. Results of these reviews will allow the OCC to determine which national banks may be at higher risk for noncompliance requiring priority in examination scheduling.

Questions concerning this advisory may be directed to your supervisory office or the Community and Consumer Policy Division at (202) 874-4428.

_____

Ralph E. Sharpe,
Deputy Comptroller for Community and
Consumer Policy

Attachment

Privacy Preparedness Questionnaire

Assessing Existing Information Practices

1. What are your information-sharing practices?

- What information is shared with affiliates and nonaffiliates (including sharing within and outside of the regulatory exceptions contained in 12 CFR 40.13, 40.14, 40.15), what is the purpose of the sharing, and is information shared on former customers?
- Are account numbers or access numbers/codes disclosed to nonaffiliated third parties?
- What information do you share on consumers who are not customers?
- Do you route requests for nonpublic personal information to a central point or use other control measures?
- Will any of your current information-sharing practices be prohibited by the regulation?

2. What kinds of information do you collect from consumers and customers for the various financial products and services offered by the bank?

3. Do you obtain information about consumers and customers from other financial institutions? If so, do you use or share the information for other purposes?

4. Are your safeguards for protecting customer information consistent with Section 501(b) of the Gramm–Leach–Bliley Act?

- Has the board approved the written information security program?
- Are your safeguards adequate to: a) ensure security and confidentiality of customer records and information, b) protect against any anticipated threats or hazards to the security or integrity of customer records and information, and c) protect against unauthorized access to, or use of, such records or information that could result in substantial harm or inconvenience to any customer?
- Has your information security program been tested in accordance with the regulatory guidelines?

Evaluating Agreements with Nonaffiliated Third Parties that Involve Disclosure of Consumer Information

5. What arrangements, agreements, or contracts exist with nonaffiliated third parties that involve disclosing consumer information? Do contracts or agreements detail responsibilities regarding the use, disclosure, and protection of consumer information?

6. What changes need to be made to conform the arrangements, agreements, or contracts to the regulation?

Establishing Mechanisms to Handle Opt-Out Elections

7. If applicable, how will you administer the opt-out provisions of the regulation?

- Is the opt-out mechanism reasonably convenient for the consumer to use?
- How will you document those consumers who opt out or later change their opt-out status, and how will you segregate their information?
- How much time will you allow for consumers to opt out and how quickly will you process opt-outs?
- What are your opt-out arrangements for consumers who jointly hold a financial product or service?
- Will you allow partial opt-outs? If so, under what circumstances, and are your record-keeping systems capable of handling that level of complexity?

Developing a Privacy Policy

8. Have you developed a privacy policy? If so, what is it?

- Does the policy contain all relevant disclosures required by the privacy regulation?
- Is the information in the privacy policy stated clearly and in a way that consumers are likely to understand? Is it presented in a way that is likely to call the consumer's attention to the nature and significance of the information in the notice?
- Has the policy been reviewed by the board and senior management, the compliance officer, and legal counsel?
- Does it reflect your actual practices?
- Do you think your customers will accept your privacy policy?
- Does the institution have a process to ensure that privacy policies are kept current?

Delivering Privacy Notices

9. How will you deliver initial, annual, and revised privacy notices, and opt-out notices to customers, consumers, and customers who jointly hold a financial product or service?

- Will you hand deliver notices to individuals conducting transactions in person?
- Will you mail the notices, and if so, will you mail them with other information, such as account statements, or separately?
- Do you intend to deliver any notices electronically? If so, how will you obtain the consumer's/customer's agreement to receive electronic delivery?

Establishing a Training Program

10. Describe your plan to train employees on privacy.

- Who will be trained, when, and what information will be covered?

- Will there be different levels of training depending upon job responsibilities?

Establishing a Compliance Program

11. Describe audit's/compliance review's role in developing and implementing the bank's privacy program.

12. Have internal controls, policies, procedures, and audit programs been established to ensure a satisfactory level of compliance?

Developing an Implementation Plan

13. Describe your implementation plan.

- Has the plan been approved by senior management and the board?
- Does it contain target dates, responsibilities, responsible parties, testing procedures, and progress reports?
- Is the plan on schedule?
- Does the plan ensure delivery of the privacy policy prior to July 1, 2001, and afford customers a reasonable time to exercise any opt-out rights before that date?