

AL 99-6

Subject: : Guidance to National Banks on Web Site Privacy  
Statements

Date: May 4, 1999

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

#### PURPOSE

This guidance provides national banks with examples of effective practices for informing consumers who access bank Internet sites about bank privacy policies for the collection and use of personal information. The guidance also discusses examples of effective practices for the development of bank privacy policies and for ensuring adherence to those policies.

#### BACKGROUND

Banks increasingly are using the Internet as a medium for communicating with their customers, and, to a lesser extent, as a vehicle for enabling their customers to conduct financial transactions. The success of banks in expanding the amount and type of business they and their customers conduct on line will depend largely on customer acceptance of this medium for making financial transactions. Survey data indicate that consumers are sensitive to how businesses, including banks, maintain, use, and analyze information about them. These consumer concerns about the accumulation and use of their personal information are likely to increase with the growing use of the Internet and electronic commerce.

Because a fundamental component of the bank/customer relationship is a customer's trust in the institution to respect the privacy and confidentiality of that relationship, it becomes even more important for banks to reassure customers about the safeguarding of their personal information when it is communicated in a remote, on-line environment. Indeed, informing customers about bank policies for handling of personal information may well increase consumer confidence in transacting business electronically. [Note: A recent Harris-Westin survey found that the majority of Internet users who purchased goods or services on line said that it was very important for businesses to post notices on their Web sites explaining how they will use the personal information customers provide when making purchases over the Internet. Further, the survey found that of consumers not likely to access the Internet in the next year, greater privacy protection was the factor that would most likely convince them to use the Internet. E-Commerce and Privacy: What Net Users Want, a survey conducted by Louis Harris and Associates, Inc. and Dr. Alan F. Westin, June 1998. ] The Internet, thus, presents banks with both new business

opportunities and new challenges for addressing legitimate expectations of customers about the privacy and security of their personal information.

A number of institutions have recognized the growing importance of privacy to their customers and have developed, implemented, and communicated privacy policies. [Note: A number of the banking trade associations -- the American Bankers Association, the Consumer Bankers Association, the Banking Industry Technology Secretariat of the Banker's Roundtable, American's Community Bankers, and the Independent Community Bankers of America -- have adopted a core set of banking industry privacy policies. These industry-wide policies have been used by many banks as a starting point for developing privacy policies tailored to their individual corporate practices. ] Generally, these policies encompass one or more of the following five areas: (1) notice to consumers about the institution's information practices; (2) consumer choice about the disposition of personal information; (3) accuracy of personal information maintained by the institution; (4) security measures to protect consumers' personal information; and (5) mechanisms to handle consumer questions or complaints about the handling of personal information.[Note: For a discussion of widely accepted principles concerning fair information practices see Privacy Online: A Report to Congress, Federal Trade Commission, June 1998 (posted at [www.ftc.gov/reports/privacy3](http://www.ftc.gov/reports/privacy3)). ] This guidance provides examples from a sampling of these existing bank practices that represent effective approaches for the development and implementation of privacy policies and their posting on bank World Wide Web (Web) sites.

Although this guidance is targeted at banks that operate Web sites, the examples of practices and procedures for developing and implementing privacy policies are pertinent to any national bank considering establishing or revising a privacy policy and related procedures. Thus, national banks may find these examples helpful as they develop their own privacy policies and implementation procedures. These examples are not examination standards, do not impose new regulatory requirements on banks, and are not intended to be an exclusive description of the various ways banks can devise and communicate effective privacy policies.

#### EXISTING LEGAL REQUIREMENTS

Financial institutions, historically, have taken special care to protect the privacy and security of confidential customer information and have long been subject to a number of federal and state laws that govern the handling of such customer information. These laws and regulations may apply to aspects of the operation of bank Web sites. [Note: Banks offering PC banking were reminded to be familiar with applicable privacy rules that could restrict their ability to share information with third parties that they obtain from

their customers. See Technology Risk Management: PC Banking, OCC Bulletin 98-38, August 24, 1998. The OCC also recently issued an Advisory Letter alerting bankers to the practice of "pretext phone calling," which is a means of gaining access to customers' confidential account information by organizations and individuals who call themselves "account information brokers." This letter was also intended to enhance institutions' awareness regarding the confidentiality and sensitivity of customer information generally, and identify some appropriate measures for the safeguarding of such information. See OCC Advisory Letter 98-11.

] For example, banks operating Web sites that permit customers to transfer funds electronically into and out of their accounts [Note: An "account" for the purposes of the Electronic Funds Transfer Act (EFTA) is defined as a demand deposit, savings deposit or other consumer asset account held directly or indirectly by a financial institution, established primarily for personal, family or household purposes. 15 U.S.C. .1693a(2); 12 C.F.R. 205.2(b)(1).] must inform these customers, among other things, about the situations in which the bank, in the "ordinary course of business," will disclose information about the customers' accounts to third parties. [Note: Id. .1693c(a)(9); 12 C.F.R. 205.7(b)(9). This disclosure must describe the circumstances in which any information concerning the account may be provided to third parties, including affiliates. See FRB Official Staff Commentary 205.7(b)(9)-1.]

Additionally, if a bank permits customers to apply for credit over its Web site, the Fair Credit Reporting Act's conditions for sharing certain customer information outside of the bank may apply. [Note: The Fair Credit Reporting Act (FCRA) provides that certain consumer information that is shared among affiliates is not a "consumer report" if there is clear and conspicuous notice to the consumer that the information may be shared and the consumer is given an opportunity to direct that the information not be shared ("opt out" notice). 12 U.S.C. .1681a(d)(2)(A)(iii). For a further discussion about the FCRA, the different types of consumer information that it covers, and examples of effective practices for satisfying the notice and opt out requirements related to sharing of information among affiliates, see OCC Advisory Letter 99-3.]

#### EFFECTIVE PRACTICES

This section discusses examples of existing bank practices that the OCC considers effective means for communicating a bank's

privacy policies, developing a bank's policies for handling customer information, and ensuring adherence to stated policies.

#### Communication of Privacy Principles

The most effective disclosures of privacy principles are clear, prominent, and easy to understand. In general, effective disclosures avoid communicating complicated information in a complex and technical way. Many banks that post privacy notices on their Web sites acknowledge their customers' privacy expectations and indicate how the bank will safeguard and handle personal information. In many instances, banks inform their customers that the bank takes measures to limit employee access to confidential information and to maintain accurate and up-to-date consumer records. Some banks also describe the general circumstances under which the bank will share information with third parties. Some banks explain that customers have a choice about how their information is shared and provide a convenient way to "opt out" of mail or telephone solicitations. Additionally, some Web site privacy policies explain the bank's collection and usage of customer information that is unique to the online environment, such as "cookies." [Note: A "cookie" is a piece of information that a Web site stores on a visitor's Web browser that is retrieved when the visitor logs onto the site again. ]

To ensure that these stated principles are readily understood, some banks have supplemented their privacy principles with a series of questions and answers about the handling of customer information. [Note: Many banks use their Web sites as the only medium for communicating their privacy policies to customers. Some banks, however, provide customers with written copies of their privacy policies as a stand alone document or in conjunction with other written materials. ]

Banks have used a number of different devices to feature their privacy statements prominently. Banks with effective communication practices have posted privacy policies at specific locations on their Web sites where they may be most meaningful to the consumer. For instance, a bank that permits customers to submit on-line credit applications displays its privacy policy at the point at which the customer is asked to submit personal information. Many banks place "hypertext" links or "hotlinks" to privacy statements on their Internet home pages and/or on Web site transactional pages (e.g., on-line banking or small business pages) that automatically present disclosures to customers when the option is selected. Several banks place links to their privacy policies in the footer of each of their Web site pages.

#### Developing an Effective Privacy Policy

Banks with effective privacy policies also take steps to ensure that their internal policies and procedures are consistent with and support stated privacy promises.

Senior Management Involvement

Effective policies and procedures often involve senior management's knowledge of, and involvement in, the planning process. Senior management can provide a broad perspective on the issues, dedicate appropriate resources to accomplish the task, and create the necessary culture to ensure that privacy matters are addressed comprehensively and consistently across the organization. In a number of banks, the teams or personnel responsible for developing privacy policies and procedures report directly to senior officials.

#### Interdisciplinary Working Groups

A number of banks, particularly large banks, have formed privacy working groups, teams, or task forces consisting of members from various departments in the bank (e.g., legal, marketing, compliance, retail, systems, security, and human resources) to either update or develop their privacy policies and procedures for handling customer information. The multi-disciplinary team approach has enabled banks to centralize efforts, while ensuring that diverse interests and perspectives in the company are represented. One institution that used the team approach to develop an institution-wide privacy policy is relying on individual business units to develop appropriate implementation plans to support the policy. Some smaller institutions, however, with different business considerations and personnel resources have found that an interdisciplinary team was not needed to develop privacy policies. In these cases, senior management appointed a particular division or employee to develop policies and procedures.

#### Review of Existing Procedures and Systems

Often the individuals or groups responsible for establishing policies and procedures reviewed existing systems, operations, and other internal policies to better understand current information practices, to assess risks associated with information handling, and to avoid promulgating privacy promises that could not be met. Additionally, reviews have involved an assessment of which, and the extent to which, existing systems and practices needed to be modified to accommodate a bank's new or revised privacy policy. [Note: Because of changes in bank systems, operations, and technology, banks expect these reviews will need to be ongoing or periodic.]

#### Review of Relationships with Third Parties

In addition to reviewing internal procedures and practices, many banks have reviewed their relationships with unaffiliated third parties to assess their adherence to the bank's privacy policies. Several banks that provide customer information to unaffiliated third parties for joint marketing purposes or operational support, such as data processing, have required the third party to execute a confidentiality agreement and agree to limit the use of information. Some banks also monitor these third parties for compliance with their agreements and/or give their customers prior opportunity to opt out of the information sharing where

feasible (e.g., joint marketing).

#### Enhancing the Effectiveness of the Bank's Privacy Policy

Banks with effective privacy policies take measures to enhance their employees' understanding of compliance with such policies. These banks have supported their policies with employee training and compliance mechanisms.

#### Internal Communication and Training

Banks with effective privacy policies take steps to ensure that their policies are understood by bank personnel involved in the handling of confidential customer information. These banks widely communicate the policies among appropriate bank employees and support them with employee training. For example, banks have informed their employees about their privacy policies through employee handbooks, codes of ethics, articles in company newspapers, Intranet postings, individual mailings from senior management, or the distribution of policy guidance. Some banks have supplemented communications with various forms of training -- live sessions, handbooks or videos. Many banks require employee acknowledgment of training, i.e., the staff must formally acknowledge their understanding of privacy/confidentiality policies, by signing a form. Where the bank's privacy policies have been incorporated into the bank's code of ethics, officers and employees have been required to certify their own compliance (annually or periodically) with the ethics code.

#### Compliance

A number of banks have established programs or procedures to enhance compliance with their privacy policies. Some banks require individual business unit compliance officers to establish appropriate compliance plans and/or require periodic self assessments by business lines to determine the adequacy of their adherence to procedures and internal controls. Others determine the adequacy of compliance through internal audits (the frequency of which is determined by the risk associated with the individual lines of business), or use audits to supplement the activities of business line managers or compliance officers. Depending on the size of the institution or the nature of the activity at issue, some institutions rely on periodic reviews rather than formal audits to monitor compliance with privacy policies.

Most banks have procedures designed to deter employee violations of their policies. An employee's failure to comply with a bank's privacy policy is often subject to the same disciplinary actions as any other breach of bank policy -- including termination where appropriate. These personnel procedures have been provided for in banks' ethics codes, codes of conduct, or human resource policies.

Additionally many banks have established mechanisms for handling consumer privacy complaints and inquiries. Some banks provide for a central point of contact within the bank to handle customer

privacy issues. For instance, some banks provide an e-mail link on their Web sites for privacy related questions or complaints. Another bank has appointed an ombudsman to handle customer privacy complaints. Still, another bank catalogues privacy complaints, and depending on their nature, routes them to different centralized locations for handling. Each business line is expected to appoint a privacy officer and track and correct privacy complaints in another bank. Some banks have determined that, because of their size or the nature of the activities they conduct, they can use established mechanisms or procedures within the bank designed to deal with customer complaints, generally, to handle customer privacy related complaints.

#### CONCLUSION

At a time of growing public sensitivity and concern about the treatment of personal information, bank privacy policies may enhance customer confidence and trust in their financial institutions. When posted on bank Web sites, privacy policies may increase customer acceptance of the Internet as a medium for conducting financial transactions. The most effective privacy policies found on bank Web sites are those that are posted prominently, contain clear and readily understandable disclosures about the handling of customer information, and are supported by consistent internal procedures and methods to enhance compliance by bank personnel.

#### FURTHER INFORMATION

For further information or questions relating to this advisory, please contact Amy Friend, assistant chief counsel at (202) 874-5200.

---

Julie L. Williams  
Chief Counsel