Electronic Commerce and Consumer Privacy

FIL-86-98
August 17, 1998

TO:
CHIEF EXECUTIVE OFFICER
SUBJECT:
Online Privacy of Consumer Personal Information

Consumers have become increasingly concerned about the privacy of their personal information. With the rapid growth of electronic commerce, and the increased collection of diverse pieces of consumer personal information over the Internet, the potential for this information to be used in ways unwanted by consumers is a growing risk to financial institutions. In the attached "Online Privacy of Consumer Personal Information," the FDIC addresses online privacy to raise awareness about this issue among financial institutions.

The FDIC considers the privacy of consumers' personal information an important element of public trust and confidence in depository financial institutions. Financial institutions' compliance with existing laws on consumer privacy matters and their demonstrated ability to protect sensitive information have given customers confidence. However, new consumer privacy concerns are emerging due to changes in the industry and technology. The FDIC supports industry self-regulation to address consumer privacy issues, and encourages financial institutions to maintain an awareness of emerging consumer online privacy concerns while taking voluntary, specific actions to address those concerns. Institutions should provide meaningful disclosures of their privacy policies and information practices, and effectively enforce them.

During the course of regular examinations, examiners will continue to review information collection practices and discuss them with bank management. For further information, please contact your FDIC regional office.

Carmen J. Sullivan
Nicholas J. Ketcha Jr.
Director, Division of Compliance and Consumer Affairs
Director, Division of Supervision

Attachment: Online Privacy of Consumer Personal Information

Distribution: FDIC-Supervised Institutions (Commercial and Savings)

NOTE: Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 801 17th Street, NW, Room 100, Washington, DC 20434 (800-276-6003 or 202-416-6940).

ONLINE PRIVACY OF CONSUMER PERSONAL INFORMATION

The privacy of consumer personal information has become an increasing concern with the rapid growth in electronic commerce conducted over the Internet, emerging electronic payment systems, financial services industry consolidation, new business affiliations, and bundling of financial services. Financial institutions are increasingly deploying online systems to facilitate the convenient delivery of services. Some financial institutions use Internet Web sites designed to collect information from consumers via online forms, surveys or e-mail links. Information about consumers is also collected through inconspicuous means such as hidden, undisclosed electronic information collection methods (e.g., "cookies"[1]). The FDIC understands the importance of information exchange on the Internet and the benefits for banks and consumers. However, because the dramatic pace of technological change has enhanced the collection of diverse pieces of consumer personal information and increased the velocity of data transfer, the potential for personal information to be used in ways unwanted by consumers is a growing risk to financial institutions.

The FDIC considers the privacy of consumer personal information to be an important element of public trust and confidence in depository financial institutions. The Corporation acknowledges that existing laws pertaining to specific consumer privacy matters impact financial institutions. Their compliance with these laws and demonstrated ability to protect sensitive information have given their customers confidence. Consumer privacy concerns, however, are being influenced by changes in the industry and technology. Therefore, the FDIC encourages financial institutions to maintain an awareness of emerging consumer online privacy concerns, and to take voluntary, specific actions to address them. In particular, financial institutions should provide meaningful disclosures of privacy policies and information practices, and effectively enforce those policies and practices.

Consumer Privacy Concerns and the Online Environment

The collection of consumer data by financial institutions is not new. However, recent public hearings, consumer surveys, studies and reports by federal government entities and private organizations clearly indicate that consumers are increasingly concerned about the collection, use and dissemination of personal information, particularly in the online environment. While consumer concerns about privacy are not uniform, studies have shown that the vast majority of consumers want the ability to control their personal information and to feel comfortable with how it is used.

Generally, consumers have three primary concerns about the privacy of personal information in the online environment:

- How personal information is being collected;
- How the information is used by the entity collecting the information, particularly for purposes other than the original transaction; and
- Whether personal information is transferred to third parties, and how they will use it.

Financial institutions should recognize that electronic commerce is facilitated by a network environment often including third parties that may come into contact with sensitive information. Institutions should acknowledge and respond to consumer concerns about emerging online technology and the potential access and use of personal information by third parties.

Privacy Policies and Information Practices

The Federal Trade Commission (FTC) and the Consumer Electronic Payments Task Force[2] , with representatives from the federal financial institution regulatory agencies, recently issued reports highlighting consumer privacy interests. Both reports supported voluntary industry action and self-regulation to address consumer privacy concerns.

In the FTC's report, *Privacy Online: A Report to Congress*[3] , dated June 4, 1998, the FTC found that self-regulation efforts of businesses to protect the privacy of consumer personal information over the Internet were ineffective. The report concluded that the vast majority of Web sites collect information, but had not yet adopted the most fundamental fair information practice of "notice." The report included a survey of the financial sector, which showed that 97 percent of the Internet Web sites surveyed collect personal information, but only 16 percent provide notice of their information practices. The report also noted that established trade association privacy guidelines have not been widely accepted by their respective industries.

As a result of the FTC study, the FDIC conducted its own informal survey of Web sites of FDIC-supervised banks. The FDIC's survey findings were comparable to the FTC's. The FDIC found that information collection is conducted by many sites using many different methods, such as online applications, transaction capabilities, and forms and questionnaires. However, the survey showed that statements addressing privacy are frequently absent from bank Web pages.

Bank trade associations developed the "U.S. Banking Industry Privacy Principles" to encourage voluntary adoption of privacy policies and information practices by financial institutions. These principles can be found in the appendix of Financial Privacy in America, published in June 1998 by several financial service industry trade associations and service providers. The Banking Industry Technology Secretariat created a "Privacy Principles Implementation Plan" that provides further guidance to the industry. These guidelines were issued to foster industry self-regulation on the privacy matter. Financial institutions may want to consider these guidelines when customizing their own privacy policies and practices.[4]

Financial institutions may also want to consider observing examples of Web site privacy policies displayed by other financial service providers. A list of some Web sites can be found in the appendices of Financial Privacy in America. When preparing policies and practices, financial institutions may also benefit from exploring the solutions offered by private sector organizations that work with businesses to help implement effective privacy policies and practices.

While a number of resources on the privacy issue are available to banks, the "fair information practice principles" advocated by the FTC are considered to be the foremost articulation of what a privacy policy should contain. The five principles are:

- Notice to consumers about information practices before any personal information is collected;
- Choice for consumers about the collection and use of information from them or about them, and choice to restrict the use of information;
- Security and accuracy of consumer information collected, protecting against loss and unauthorized access and disclosure of information;
- Access for consumers to information collected and the ability to identify and correct errors in a timely and inexpensive manner; and
- Enforcement and consumer redress to ensure compliance with the privacy policy and information practices and a means of recourse for an injured party.

While each principle plays an important role in protecting consumer privacy, the "notice to consumers" may be the most important action taken by a financial institution. The notice should include information about the remaining four principles, which will benefit consumers by permitting them to make an informed choice about the level of protection they want before divulging personal information. The notice should also include the identity of the information collector, how the information is collected, why the information is collected, how the information will be used (particularly for secondary purposes), and how a consumer may limit disclosure of information. Privacy policy statements should be conspicuous and easy to find on a financial institution's Web site, and should be clearly stated and readily understandable by consumers.

Industry self-regulation of privacy policies and information practices can only be effective when accompanied by employee education, adequate internal controls, and meaningful enforcement and redress. Financial institutions should train staff about their responsibilities under the institution's privacy policies and information practices. Financial institutions should ensure that

online privacy policies and information practices are consistent with the bank's offline, or physical environment, information-collection activities.

Financial institutions should review their internal controls to ensure that these controls prevent the improper disclosure of personal information to third parties. Banks with outsourcing arrangements may need to be especially cognizant of privacy concerns as outsourcing arrangements present a greater potential for banks to lose control over consumer information. Banks that lose control of consumers' information are subject to liability and reputation risk. Internal controls should incorporate a monitoring and review mechanism that will test compliance with established privacy policies and information practices.

Finally, financial institutions should confirm that procedures are established to address internal breaches of online policies and practices. Banks should also consider disclosing a procedure by which consumers may inquire about their personal information or inform the institution about the potential misuse of personal information in the online environment.

Conclusion

The FDIC supports industry self-regulation that is specific, meaningful and effective. The agency believes it is a good business practice for financial institutions to adopt responsible privacy policies and information practices, disclose those policies and practices to increase consumer knowledge and understanding, and take other prompt, effective actions necessary to provide consumers with privacy protections in the online environment.

The FDIC recognizes that information collection practices will vary among financial institutions. Therefore, it encourages banks to develop and implement information practices that best serve the needs of the bank and its customers. Such actions are good risk management and will enhance consumer confidence in online banking.

Footnotes

[1] Information placed on a consumer's computer hard drive by a Web site's server that allows the Web site to monitor the user's visit to the site. The cookie can contain such information as login and registration information, and a consumer's interests as indicated by the pages visited at the Web site.

[2] The Report of the Consumer Electronic Payments Task Force, dated April 1998, can be found on the Internet at www.occ.treas.gov/emoney/ceptfrpt.pdf.

[3] The report can be found on the Internet at www.ftc.gov/reports/privacy3/toc.htm.

[4] Information about consumer privacy, including the banking industry privacy principles, implementation plan, and/or the report can be obtained from the financial institution trade associations, or on their respective Web sites at: (1) www.ibaa.org/privacy.html, (2) www.aba.com/, (3) www.cbanet.org/, (4) www.acbankers.org/.