OFFICE OF THRIFT SUPERVISION

Policy Statement on Privacy and Accuracy of Personal Customer Information

November 1998

INTRODUCTION

Savings associations regulated by the Office of Thrift Supervision ("OTS") have an obligation to protect and maintain confidential and accurate customer information. Institutions have already established internal controls to protect paper-based personal information. Institutions are now, however, faced with new challenges presented by the electronic storage and retrieval of information. As financial institutions increasingly use new technology to access, compile, and relay information to the customer, other institution staff, and third parties, new concerns arise about the privacy, security, and accuracy of such data. New technology also increases the potential for misuse or alteration of information.

This policy statement recommends that savings associations ("you") notify customers how you will use certain customer information and permit them to limit your use of it. It also reminds you to establish adequate controls to protect and maintain the confidentiality and accuracy of all customer information. Your written procedures should:

- Inform customers how you will use certain customer information and permit customers to limit the use of such information; and

- Safeguard the security and accuracy of all information about customers.

RECOMMENDED PRACTICES TO INFORM CUSTOMERS AND OBTAIN CONSENT FOR THE USE OF PERSONAL INFORMATION[1]

Before you collect any information from a customer, you should describe to that customer how you will use his or her personal information. For example, you may initially need specific information to open an account or authorize a loan for the customer. However, you may also want to share that personal information with your affiliates to cross-market other products or services to the customer.

There are many ways for you to provide adequate notice to your customers about use of their personal information. For example, when you open an account with a customer, you should consider providing the customer a notice that explains:

[1] The term "personal information," as used in this policy statement, does not include "information solely as to transactions or experiences between the customer and the [institution]" as provided in the Fair Credit Reporting Act, 15 U.S.C. § 1681a(d)(2)(A)(i).

- all intended uses of the personal information you are collecting;
- whether you intend to give or sell the personal information to an affiliated or non-affiliated party;
- what happens if the customer declines to provide the required information;
- a general description of the methods you use to assure the confidentiality and accuracy of information; and
- a phone number, e-mail address, or other point of contact at your institution that the customer can use to:
  - — review information that you have about the customer;
  - — correct inaccurate or outdated information; or
  - — notify you of possible unauthorized access to, or use of, his or her account information.

Existing customers and the general public may also want to read your customer notice. You may want to make this notice available upon request.

Before sharing personal information with affiliates, the Fair Credit Reporting Act requires that you disclose to the customer that you may share the information with affiliates and give the customer the opportunity to "opt out" of having this information shared with affiliates. We also recommend you offer your customers the choice to opt out of having this information shared with non-affiliated parties. Furthermore, certain federal and state privacy laws prohibit the release of a customer's financial records without the customer's permission.[2] If the customer has chosen to limit your sharing of their personal information, you may not exchange or sell personal information about the customer to third parties, unless you:

- receive a customer request or permission to release the information; or
- are required or allowed by law (e.g., subpoena or investigation of fraud) to disclose the information.

If you provide personal customer information to a service provider or other reporting agency under an outsourcing arrangement you should assure that they continue to protect the security and accuracy of such information.

[2] The federal Right to Financial Privacy Act ("RFPA"),, prohibits the release of the financial records of any custmer to any "Government authority" except in accordance with the requirements of the RFPA. 12 U.S.C. § 3403. For a listing of other privacy laws, *see* Federal Trade Commission, Privacy Online: A Report to Congress 40, n.160 (June 1988) and "The Report of the Consumer Electronic Payments Task Force" 24-29 (April 1998).

SAFETY AND SOUNDNESS STANDARD TO KEEP INFORMATION SECURE AND ACCURATE

Institutions already have internal controls in place that address the security of paper-based information. Specifically, you should have procedures for access, storage, and disposal of documents that contain confidential customer information.

In addition to handling paper documents within traditional brick and mortar facilities, financial institutions may use delivery channels (e.g., public telephone networks and the Internet) that are partially or totally outside the control of the institution. Operational risks increase with the reach of systems and the number of uncontrolled access points to the information.[3] Access to your electronic records through a local network, telephone or the Internet could potentially open your computer system to unauthorized users.[4] Therefore, adequate security of your institution's systems and customer information is paramount. Your internal controls must be updated to reflect the use of developing technologies and continue to adequately safeguard customer information. You should ensure that all employees are aware of their responsibilities to safeguard customer information. A comprehensive security program:

- Establishes controls to guard against unauthorized access to your networks, systems, and databases;
- Provides for employee training;
- Protects customers during transmissions over public networks to ensure the intended person receives accurate information and to prevent eavesdropping by others;
- Creates proof that both the sender and the receiver participated in a transaction: it is important that you ensure neither party in a transaction can deny his or her obligation;[5]
- Ensures the integrity and accuracy of your customer account information;
- Provides for correcting or updating information that you still use in account data files; and,
- Permits customers to review and correct any erroneous or outdated information.

[3] Operational risks arise from the potential that breaches of internal controls, operating problems, fraud, inadequate information systems, or unforeseen events may result in unexpected losses.

[4] For instance, "information brokers," operating generally over the telephone and the Internet, can obtain detailed information about a customer's financial history from financial institutions. You need to ensure that confidential customer account information is not inappropriately provided to information brokers. (For additional guidance on "information brokers," you can refer to the "Interagency Pretext Phone Calling Memorandum.") Also, outside hackers, disgruntled employees, unauthorized internal users and others may create havoc with your customer information if you fail to establish adequate operating controls.

[5] The *Examination Handbook*, Section 341, Information Technology and Risk Controls offers specific guidance on the type of controls that management should implement to ensure adequate security of information and authentication of users.

If you collect, process, or maintain customer financial information, you should perform certain functions (e.g., account balance reconciling, funds transfer, or bill payments) under dual control. You should segregate the input of information from the review of processed information. These controls should also require the reviewer to reconcile the processed information. Your operating policies and procedures should describe the appropriate controls in detail.

SUMMARY

You should have written policies and procedures, approved by your board of directors, that describe how you will ensure that information is properly protected, confidential, and used as agreed with the customer. This policy statement and applicable laws and regulations will be considered by OTS examiners as they evaluate the adequacy of your internal controls.

OTHER SOURCES OF INFORMATION

Other federal agencies and bank industry trade groups also have issued privacy guidance that you may find useful. This includes:

- *"Privacy Online: A Report to Congress,"* Federal Trade Commission June 1998. (A description of core principles of fair information practices.) This report can be found on the Federal Trade Commission's web site at www.ftc.gov.

- *"Online Privacy of Consumer Personal Information,"* Federal Deposit Insurance Corporation August 1998. (A financial institutions letter that addresses online privacy to raise awareness among financial institutions.) This report can be found on the Federal Deposit Insurance Corporation's web site at www.fdic.gov.

- *"Emerging Privacy Issues in Electronic Banking,"* America's Community Bankers August 1998. (A description of specific operating privacy principles for community banks.) This report can be found on the trade association's web site at www.acbankers.org.

- *Banking Industry Privacy Principles," American* Bankers Association, Consumer Bankers Association, and the Bankers Roundtable. (Joint industry privacy principles for the benefit of bankers and consumers.) This report can be found on several trade associations' web sites such as www.aba.com or www.aba.comg.