Office of Thrift Supervision
Department of the Treasury
Deputy Director
1700 G Street, N.W., Washington, DC 20552 • (202) 906-6853

November 3, 1998

MEMORANDUM FOR CHIEF EXECUTIVE OFFICERS

FROM: Richard M. Riccobono

SUBJECT: Policy Statement on Privacy and Accuracy of Personal Customer Information

The tremendous growth in new technology and its use to facilitate the exchange of personal customer information raises new and unique issues. Some of the more important issues focus on the controls that organizations have in place to protect the privacy and accuracy of customer information. Efforts are under way, both domestically and internationally, to establish standards governing information use. Though this area continues to evolve, savings associations nonetheless have an obligation to protect and maintain confidential and accurate personal information. Your institution should establish adequate controls to ensure that customer information is properly protected, confidential, and used as agreed with the customer.

The Office of Thrift Supervision (OTS) is issuing the attached two policy statements to enhance your awareness of customer privacy. These policy statements reflect our current understanding of some "best practices" that may help you to adequately protect personal information. OTS will continue to monitor this area, continue to keep you informed, and update our recommendations, as needed.

In the *Privacy and Accuracy of Personal Customer Information* policy statement, OTS recommends that you notify customers how you will use their personal information and permit them to limit the use of information. As described in the policy statement, the federal Fair Credit Reporting Act requires customer disclosure and an opportunity to opt out for certain types of information sharing. You are also reminded to establish adequate controls to protect and maintain the confidentiality and accuracy of all customer information.

The *Interagency Pretext Phone Calling Memorandum* policy statement addresses a particularly troubling issue: 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." It also enhances your awareness about the confidentiality and sensitivity of customer information generally, and identifies appropriate measures to protect your institution and customers from unauthorized disclosure of customer information.

Examiners will continue to evaluate the adequacy of the internal controls you have in place to protect your institution's and your customers' information and will discuss findings with management, as needed. I encourage you to share this guidance with your board of directors and staff.

If you have questions concerning these policy statements, you should contact your regional OTS office or Paul Reymann, Senior Policy Analyst, (202) 906-5645, Paul Glenn, Special Counsel, (202) 906-6203, or Paul Robin, Program Analyst, (202) 906-6648.

Attachments

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 customer 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 STANDARDS 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.

If you collect, process, or maintain customer financial information, you should perform certain

---

[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 *OTS Thrift Activities Handbook*, Section 341, Information Technology offers specific guidance on the type of controls that management should implement to ensure adequate security of information and authentication of users.

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.

- "*U.S. 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.cbanet.org.

Office of Thrift Supervision

Interagency Pretext Phone Calling Memorandum
November 1998

PURPOSE

This memorandum alerts insured financial institutions 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." It is 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.

This guidance was jointly prepared by the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the Federal Reserve Board, the FBI, the Secret Service, the Internal Revenue Service, and the Postal Inspection Service.

BACKGROUND

There is a tremendous demand for information about individuals' and businesses' bank accounts. In recent years, this rising demand for account information has led to an increase in the number of organizations known as "account information brokers." These "brokers" gather confidential financial information, including specific account numbers and balances, from various public and nonpublic sources. The brokers then sell this information to anyone who is willing to pay for it. Their clients include lawyers, debt collection services, and private investigators, who may use account information in civil lawsuits and other court proceedings, or identity thieves who may use account information to engage in check and credit card fraud, and other criminal acts.

Unscrupulous account information brokers are obtaining customers' account information from insured financial institutions through a practice known as "pretext phone calling" or "social engineering." Brokers who engage in this practice call institutions and use surreptitious or fraudulent means to try to induce employees into providing a customer's account information. For example, a broker may pose as a customer who has misplaced his or her account number, and may repeatedly call the institution until the broker finds an employee who is willing to divulge confidential account information. The broker may use information about the customer, such as the customer's social security number, that has been obtained from other sources, to convince the employee that the caller is legitimate. While there are no reliable estimates as to the extent of this practice, there is concern among the federal banking and law enforcement agencies that it is becoming increasingly prevalent.

The use of surreptitious or fraudulent means to obtain a customer's account information may violate state and federal laws prohibiting unfair and/or deceptive practices. It also may violate federal wire fraud laws. In addition, institutions that disclose customers' account information may be violating state privacy laws, such as those that prohibit the release of a customer's financial records without having first obtained the customer's permission.

RECOMMENDED ACTIONS

Institutions have an obligation to their customers to ensure that their customers' account information is not improperly disclosed. Authorizing employees to use their own discretion to determine whether to disclose confidential information over the telephone can result in inconsistent practice and expose the institution and its customers to the risk of an inappropriate or unauthorized release of information. To avoid this risk, institutions are encouraged to develop policies and procedures for addressing customers' financial privacy, and should, at a minimum, establish clear guidelines for dissemination of customer account information. These guidelines should set forth precisely the types of information and the circumstances under which an employee is allowed to disseminate such information over the telephone. Employee training should ensure that all employees are aware of their responsibility to safeguard customer financial information, and also should educate employees of the tactics used by information brokers to surreptitiously or fraudulently obtain confidential customer information.

Institutions should have strong controls in place to ensure against the unauthorized disclosure of customer information. For example, they should consider adopting a policy that prohibits the release of information over the telephone unless the proper authorization code is provided. The authorization code should be used in the same manner as a personal identification number (PIN) for transacting business by automatic teller machines, or credit, debit, or stored-value cards. The authorization code should not be associated with other commonly used numbers or identifiers, such as social security numbers, savings, checking, loan or other financial account numbers, PINs, or the customer's mother's maiden name. In addition, the authorization code should be unique to, and readily changed by, the authorized account holder. Finally, to increase effectiveness, the authorization code should be used in conjunction with other customer and account identifiers.

Another means of preventing unauthorized disclosures is to use a caller identification service or require employees who receive calls requesting account information to ask the caller for the number from which he or she is calling. If the number differs from that in the customer's account records, it may be an indication that the request is not a legitimate one, and the employee should not disclose the requested account information without taking further steps to verify that the customer made the request.

The institution's security or internal audit department should consider conducting (or using third parties to conduct) unscheduled pretext phone calls to various departments to evaluate the institution's susceptibility to unauthorized disclosures of customer information. Any weaknesses detected should be addressed through the adoption of enhanced training, procedures, and controls.

While this memorandum primarily concerns the unauthorized access to customer account information through pretext phone calling, unauthorized access to sensitive account information may occur through other means as well, including burglary, illegal or unauthorized access to the institution's computer systems, and bribing employees with access to personal account information. Institutions should have effective procedures and controls in place to limit access to confidential information on a need to know basis, and to prevent unauthorized access to customer information through these and other means, including ensuring that all sensitive documents are properly disposed of and that the institution's physical premises and computer systems are secure. Institutions also must properly train employees to understand the importance of protecting personal account information against improper disclosure. The federal banking agencies will continue to monitor institutions' efforts to safeguard sensitive account information.

Institutions that suspect an illicit attempt to obtain a customer's confidential information should immediately report the matter to the proper authorities. In such circumstances, institutions are encouraged to file a Suspicious Activity Report, and to contact their primary federal banking regulator, the Federal Trade Commission, and the appropriate state agencies charged with enforcing laws against unfair or deceptive practices. In addition, institutions should directly contact appropriate law enforcement agencies if a fraud requiring immediate attention is suspected.