Office of Thrift Supervision
Department of the Treasury

Richard M. Riccobono
Deputy Director

1700 G Street, N.W., Washington, DC 20552 • (202) 906-6853

June 10, 1999

MEMORANDUM FOR CHIEF EXECUTIVE OFFICERS

FROM: Richard M. Riccobono

SUBJECT: Transactional Web Sites

Many savings associations ("you") are exploring business opportunities presented by electronic services, the Internet, and the World Wide Web to enhance your competitive edge, improve customer service, and reduce operating costs. As a general rule, you do not have to inform the Office of Thrift Supervision ("OTS") before using such electronic means and facilities for activities that you are otherwise authorized to perform or provide. However, you are required to:

- file a written notice with OTS before establishing a transactional web site; and
- follow any procedures imposed in writing by OTS in response to any supervisory or compliance concerns that may affect your use of electronic means or facilities.

The purpose of this memorandum is to provide you with information to help you understand our regulatory requirement and offer guidance to assist you in developing a transactional web site, should you make a decision to establish one.

Notice Requirements

Under the new electronic operations rule (12 C.F.R. Part 555) that became effective January 1, 1999, you must file a written 30-day notice as described in 12 C.F.R. § 555.310 before establishing a transactional web site.[1] The OTS defines a transactional web site as an Internet site that enables your customers to conduct financial transactions such as:

- accessing an account;
- obtaining an account balance;

[1] You must file a written notice if you establish or participate with others to establish a transactional web site. You participate with others to establish a transactional web site when consumers may conduct financial transactions electronically with you through another entity's web site. A formal notice is not required if you simply link an informational web site to another entity's transactional web site. However, you are encouraged to consult with your Regional Office before you implement any type of web site.

- transferring funds;
- processing bill payments;
- opening an account;
- applying for or obtaining a loan; or
- purchasing other authorized products or services.

When you provide your OTS Regional Office a notice that you intend to establish or participate with others to establish a transactional web site, you are required to:

- describe the transactional web site;
- indicate the date the transactional web site will become operational; and
- list a contact familiar with the deployment, operation, and security of the transactional web site.

If you established or participated with others to establish a transactional web site after the date of your last regular on-site safety and soundness examination, but before January 1, 1999, you were to file the notice described above by February 1, 1999.

Upon receipt of your notice, the OTS Regional Office will schedule a telephone interview with your designated contact to discuss your submission. Attachment A lists sample topics that the OTS interviewer will discuss.

In addition, as described in 12 C.F.R. § 555.300(c), if the OTS Regional Office informs you of any supervisory or compliance concerns that may affect your use of electronic means or facilities, you must follow any procedures it imposes in writing.

Developing a Transactional Web Site

Before establishing a transactional or nontransactional web site, you should be fully informed of the significant investment, opportunities, and risks posed by this service delivery method. Your hardware, software, and infrastructure must be safe, sound, and secure. The following reference materials provide useful information to consider when you plan, develop, and deploy a transactional web site:

- *Federal Financial Institutions Examination Council (FFIEC) Information Systems (IS) Handbook.* This handbook contains an overview of IS concepts, practices, examples of sound IS controls, and FFIEC workprograms.

- *Thrift Activities Regulatory Handbook, Information Technology, Section 341.* This handbook section describes a safety and soundness examination program to evaluate technology risk. It can be used to determine if your planning, deployment and operation, and audit processes are adequate to ensure a safe, sound, and secure infrastructure for use of information technology.

- *Interagency Guidance on Electronic Financial Services and Consumer Compliance, CEO Memorandum 90.* This guidance assesses the implications of some of the emerging electronic technologies for the consumer regulatory environment, provides an overview of pertinent regulatory issues, and offers suggestions on how to apply existing consumer laws and regulations to new electronic financial services.

- *Policy Statement on Privacy and Accuracy of Personal Customer Information, CEO Memorandum 97.* In this policy statement, OTS recommends that you notify customers how you will use their personal information and permit them to limit the use of information. Customers expect privacy policies to be available on web sites. You should post your privacy policy on your web site in a clear manner. You should also establish adequate controls to protect and maintain the confidentiality and accuracy of all customer information.

Addressing Security Issues

The security program for a transactional web site should include independent testing performed by computer-security specialists. Independent tests should cover general and environmental controls as well as audit, monitoring, and balancing controls. In a web environment, these controls can be very technical and are not yet standardized. As a result, the controls that are often built into the system are those that "technical" personnel determined were necessary. Operational, audit, compliance, and management personnel may not have been consulted when controls were established. Independent testing of technical controls will give management an objective opinion on the adequacy of these controls. These tests should be reasonable in scope, duration, and expense. You should:

- obtain a copy of the written test results and confirm with reasonable certainty that the computer system prohibits unauthorized or undetected access to customer accounts; and,
- consider all recommendations of the independent computer-security specialists, and any additional standards, requirements or written opinions provided from your most recent computer-security audit.

In some cases, your service provider may already have contracted with a third party to review their controls. If so, request the most recent third party report and review it to determine if it appears to be an independent review and that acceptable controls are in place.

You should also ensure that your Internet home page address (for transactional or nontransactional web sites) is entered correctly (e.g., http://www.yourthrift.com) when filing your Thrift Financial Report with the OTS.

From the telephone interviews, OTS examiners will determine if you appear to have taken reasonable steps to establish a safe, sound, and secure web site. Examiners will also continue to evaluate the adequacy of the internal controls you have in place to protect

your institution from internal and external security threats and 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 this information, please contact your regional OTS office or Paul Reymann, Senior Project Manager, (202) 906-5645.

Attachment

Attachment A
Transactional Web Site
Interview Topics

These topics are samples of those OTS staff may discuss in responding to your transactional web site notice. Your management or designated contact should be prepared to discuss these topics in your telephone interview with OTS staff.

1. Are the purpose and objectives of your transactional web site consistent with your overall strategic plan for the institution?

2. What type of cost/benefit analysis was performed as part of your institution's decision to develop a transactional web site?

3. What is the start-up budget for this operation and expected annual operating and maintenance costs (including telecommunications, hardware, software, and personnel)?

4. Will this service be covered under your fidelity insurance policy?

5. What steps have you taken to identify, review, and make changes in policies and procedures for each of the program areas that will be affected by the deployment and operation of the transactional web site?

6. Will you support the transactional web site with internal staff or will you rely on outside assistance? How will you maintain effective controls once the site is implemented?

7. What type of test did you conduct to ensure that your system controls will be effective?

8. How will you protect the confidentiality of customer data?

9. Do you have formal written contracts with any vendors that are helping you develop, deploy, or maintain your web site? Are these vendors Year 2000 compliant?

10. Have your disaster recovery and contingency plans been updated to include the transactional web site activities and services?

11. What procedures have you established to confirm the identity of new customers who open accounts through the web site?

12. Have you established a customer information privacy policy? Is it posted on your web site in a clear manner?

13. How will you monitor your web site to ensure that you comply with all applicable regulations?