Federal Deposit Insurance Corporation
550 17th Street NW, Washington, DC 20429

Division of Supervision

AUTHENTICATION IN AN ELECTRONIC BANKING ENVIRONMENT

FIL-69-2001
August 24, 2001

TO: CHIEF EXECUTIVE OFFICER AND CHIEF INFORMATION OFFICER

SUBJECT: *FFIEC Guidance on Electronic Authentication*

The Federal Financial Institutions Examination Council (FFIEC) has issued the attached guidance, "Authentication in an Electronic Banking Environment." This guidance focuses on the risk-management controls necessary to authenticate the identity of customers accessing electronic financial services. It also addresses the verification of new customers and the authentication of existing customers. The guidance applies to both retail and commercial customers.

Increased Risk

Customer interaction with financial institutions is migrating from in-person, paper-based transactions to remote electronic access and transaction initiation. This migration increases the risk of doing business with unauthorized or incorrectly identified parties that could result in financial loss or reputation damage to the financial institution. Effective authentication can help financial institutions reduce fraud and promote the legal enforceability of their electronic agreements and transactions.

Effective Authentication to Reduce Risk

The Federal Deposit Insurance Corporation (FDIC) believes that an effective authentication program should be implemented on an enterprise-wide basis and that the level of authentication used by a financial institution in a particular application should be appropriate to the level of risk in that application. The success of a particular authentication method depends on technology as well as effective policies, procedures and controls.

The attached guidance is divided into two parts. The main portion of the guidance provides financial institutions with some background on authentication and then discusses appropriate risk assessments, authentication of new customers, authentication of established customers, and monitoring and reporting. The Appendix discusses in more detail various authentication technologies and specific recommendations to financial institutions on using these authentication methods: passwords, personal identification numbers (PINs), digital certificates, public key infrastructure (PKI), tokens, and biometrics.

In this guidance, the FDIC does not endorse any particular technology or method of authentication.

For more information, please contact Jeffrey M. Kopchik (202-898-3872), Senior Policy Analyst, in the FDIC's Electronic Banking Branch, Division of Supervision.

Michael J. Zamorski
Acting Director

Attachment

Distribution: FDIC-Supervised Banks (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 (703) 562-2200).