Federal Financial Institutions Examination Council

2000 K Street, NW, Suite 310. Washington, DC 20006. (202) 872-7500. FAX (202) 872-7501

PRESS RELEASE

August 8, 2001

For Immediate Release

FFIEC Releases Guidance on Authentication in Electronic Banking

The Federal Financial Institutions Examination Council (FFIEC) today released guidance on the risks and risk management controls necessary to authenticate the identity of customers accessing electronic financial services.

The guidance, *Authentication in an Electronic Banking Environment,* addresses the verification of new customers and the authentication of existing customers. It applies to both retail and commercial customers.

The FFIEC is the umbrella agency for the federal banking agencies: the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision.

Customer interaction with financial institutions is migrating from person-to-person and 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

-over-

can help financial institutions reduce fraud and promote the legal enforceability of their electronic agreements and transactions.

The FFIEC believes that an effective authentication program should be implemented across a financial institution's operations and that the level of authentication used 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 guidance is divided into two parts. The main portion of the guidance provides financial institutions with some background on authentication and discusses appropriate risk assessments, authentication of new customers, authentication of established customers, and monitoring and reporting. An appendix provides more detail about various authentication technologies.

Authentication methods discussed in the guidance include:

- Passwords and personal identification numbers (PINs)
- Digital certificates – These are used to verify that users sending a message are who they claim to be.
- Public key infrastructure -- A system of digital certificates, certificate authorities, and other registration processes used to verify and authenticate the validity of each party involved in an electronic transaction.
- Tokens – Small physical devices that are usually used in conjunction with a password to gain entry to a computer system.
- Biometrics – Authentication techniques that rely on measurable physical characteristics that can be automatically checked. Examples include computer analysis of fingerprints or speech.

In the guidance, the FFIEC agencies do not endorse any particular technology or method of authentication.

# # #