Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-50-2011
June 29, 2011

FFIEC Supplement to *Authentication in an Internet Banking Environment*

Summary: The FDIC, with the other FFIEC agencies, has issued the attached guidance, which describes updated supervisory expectations regarding customer authentication, layered security, and other controls in an increasingly hostile online environment. Financial institutions will be expected to comply with the guidance no later than January 1, 2012.

Statement of Applicability to Institutions with Total Assets under $1 Billion: This Financial Institution Letter applies to all FDIC-supervised institutions offering online banking services.

Suggested Distribution:
FDIC-Supervised Banks (Commercial and Savings)

Suggested Routing:
Chief Executive Officer
Chief Information Security Officer

Related Topics:

- FIL-103-2005, Authentication in an Internet Banking Environment, October 12, 2005

Attachment:
FFIEC Supplement to Authentication in an Internet Banking Environment

Contact:
Jeffrey Kopchik, Senior Policy Analyst, at jkopchik@fdic.gov or (703) 254-0459

Note:
FDIC Financial Institution Letters (FILs) may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2010/index.html.

To receive FILs electronically, please visit http://www.fdic.gov/about/subscriptions/fil.html.

Paper copies of FDIC Financial Institution Letters may be obtained through the FDIC's Public Information Center, 3501 Fairfax Drive, E-1002, Arlington, VA 22226 (1-877-275-3342 or 703-562-2200).

Highlights:

- In 2005, the FFIEC issued guidance entitled *Authentication in an Internet Banking Environment*.
- This FFIEC guidance supplements the FDIC's supervisory expectations regarding customer authentication, layered security, and other controls in an increasingly hostile online environment.
- The FDIC expects institutions to upgrade their controls for high-risk online transactions through:
  - Yearly risk assessments;
  - For consumer accounts, layered security controls;
  - For business accounts, layered security controls consistent with the increased level of risk posed by business accounts; and
  - More active consumer awareness and education efforts.
- Layered security controls should include processes to detect and respond to suspicious or anomalous activity and, for business accounts, administrative controls.
- Certain types of device identification and challenge questions should no longer be considered effective controls.