



Division of Supervision and Consumer Protection, 500 West Monroe, Suite 3500, Chicago, IL 60661 312-382-7500

Bulletin Number: CHIRO-11-2006

INTERAGENCY GUIDANCE ON AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT

This bulletin is being issued to remind you of Financial Institution Letter (FIL) 103-2005 dated October 12, 2005, which addresses the need for stronger authentication for internet banking customers. Here is a link to the FIL: [FIL-103-2005](#). The guidance is effective as of December 31, 2006. This bulletin provides banks with an update regarding the guidance.

- At this time, banks should have completed their internet banking risk assessments that identify high risk internet banking applications covered by the guidance. Your bank should have identified an authentication solution and coordinated implementation to meet the year-end deadline.
- Banks that have outsourced electronic banking should have contacted the service provider to determine its solutions for complying with the guidance. Vendor solutions should meet your customers' needs and concur with your risk assessment.
- Banks that have outsourced electronic banking may require coordinating a conversion date with their internet banking providers.
- Implementing enhanced authentication will affect a significant portion of your bank's customer base. Many banks are implementing a phased approach and providing online customers a period of time to enroll.
- Banks should consider adequate resources for employee training and customer support during and after the conversion process. Areas to consider include training costs for employees, marketing costs to prepare customers for the change, and additional customer service calls during the enrollment period.

The Federal Financial Institutions Examination Council (FFIEC) has published frequently asked questions (FAQs) to assist banks and their technology service providers in conforming to the FFIEC authentication guidance. Here is a link to the FAQs: [FAQs](#).

The FFIEC agencies consider single-factor authentication, when used as the only control mechanism, to be inadequate for high-risk internet transactions involving access to customer information or the movement of funds to other parties. Risk assessments should provide the basis for determining an effective authentication strategy according to the risks associated with the various internet products and services available to customers. Customer awareness and education should be emphasized as they are effective deterrents to the on-line theft of assets and sensitive information.

If you have any questions concerning this information, please contact us by e-mail at SCANS@fdic.gov or call us at the Chicago Regional Office Banker Hotline 312-382-6926.