FFIEC Authentication Guidance Examination in 2012: Are Your Prepared?

Areas of Continuity, Change, and Emphasis

The Knowledge Congress
LIVE Webcast
March 8, 2012

Andrew Lorentz
Partner, Washington, D.C.

Overview

- Critical differences in the 2011 Supplement as compared to the 2005 Guidance
- Other useful sources of regulatory guidance on authentication
- Concluding thoughts on areas of examination emphasis

Why the need for the Supplement?

- Supplement reiterates the need to perform periodic risk assessments and adjust customer authentication controls as appropriate in response to new threats
- However, certain aspects of the 2005 Guidance have become less effective or require enhancement due to significant changes in the threat landscape:
  - More sophisticated, effective and malicious methods to compromise authentication mechanisms and gain access to online accounts

Why the need for the Supplement?

- Criminal groups specializing in financial fraud
- Fraud tools are easily obtainable on Internet
- Malware installed on computers monitor user activity, facilitate theft and misuse of login credentials
- Cybercrime complaints significantly up since 2005, in particular with respect to commercial accounts.

Key Differences: 2005/2011

Expectations	2005 Guidance	2011 Supplement
Risk Assessment	Risk assessment should consider type of customer (retail vs. commercial); sensitivity of transmitted information and ease of transmitting such information; volume of transactions.	Recommends updating risk assessments before implementing new financial services or at least every 12 months and including changes in internal/external threats, customer base, e-banking functionalities, and actual breach/fraud incidents.
Authentication	Expects authentication method that is appropriate and reasonable in light of reasonably foreseeable risks; single-factor inadequate for high-risk transactions. FAQ stated multi-factor authentication not required except in high-risk circumstances.	Distinguishes between retail/ consumer versus commercial transactions, the former posing a comparatively lower level of risk due to lower frequency and dollar amounts. Recommends multifactor authentication for commercial customers.

Key Differences: 2005/2011

Expectations	2005 Guidance	2011 Supplement
Layered Security	Generally recommends layered security (or multifactor authentication or other controls) where single-factor authentication is inadequate.	Specifically recommends a layered approach to securing high-risk Internet-based systems. Expects, at minimum, (1) processes to detect and respond to suspicious activity and (2) controls for system administrators beyond those controls for routine business customer users.
Device Identification	Many financial institutions implemented simple device identification, typically cookies on personal computers.	Discourages use of simple device identification like basic web cookies. Recommends more sophisticated techniques, including one-time cookies coupled with digital fingerprints that look at multiple characteristics of a device.

Key Differences: 2005/2011

Expectations	2005 Guidance	2011 Supplement
Challenge Questions	Many financial institutions use challenge questions as backup to primary logon authentication.	Discourages use of basic challenge questions. Recommends "out of wallet" questions and other sophisticated challenge techniques (*e.g.*, multiple questions, red-herring inquiries).
Customer Awareness	Generally recommends that financial institutions continue efforts to educate customers; evaluate effectiveness of education programs.	Emphasizes need to educate both retail and commercial account holders about federal consumer protections and risk mitigation controls.

Customer Awareness

- Supplement emphasizes need to inform both retail and commercial account holders about:
  - Regulation E protections for electronic fund transfers and what accounts are covered
  - When institution may make unsolicited requests for customer account credentials
  - Need for customers to periodically perform risk assessments and control evaluations
  - Alternative customer risk control mechanisms
  - Contact information to report suspicious account activity or information security-related events

Customer Awareness

- FAQ to the 2005 Guidance indicated that institutions may make such information available:
  - On the institution's website
  - In statement stuffers or other direct mail communication
  - At branch offices
- Institutions may track customer clicks on information security links or volume of written materials disseminated (not expected to force customers to read)

Other Guidance

- Federal Reserve, FDIC, NCUA and OCC have each issued notices that provide (some) additional guidance on the 2011 supplement and examinations
- No authentication guidance from the CFPB
- FFIEC member agencies have other materials on which financial institutions can rely for guidance
  - Much of the material available from regulatory agencies has yet to be updated to reflect the 2011 supplement
  - Although predate the 2011 supplement, these additional materials still have some relevance in particular contexts

Other Guidance

- FFIEC E-Banking Handbook (Aug. 2003)
  - Focus is on authentication of customers in an e-banking environment
  - Discusses new customer and existing customer authentication techniques, password administration, and what should be in a financial institution's Customer Identification Program
  - Includes examination procedures to help examiners reach conclusions regarding the effectiveness of a financial institution's risk management of e-banking activities

Other Guidance

- FFIEC Information Security Handbook (Jul. 2006)
  - Discusses authentication in the context of internal controls and the products and services offered by financial institutions
  - Provides a more in-depth description of various authentication methods and describes common authentication weaknesses, attacks, and controls that can be used to offset such weaknesses and attacks
  - Includes examination procedures to help examiners reach conclusions regarding the effectiveness of the financial institution's risk management processes as they relate to the security measures instituted to ensure confidentiality, integrity, and availability of information systems

Other Guidance

- FFIEC Retail Payment Systems Handbook (Feb. 2010)
  - Focus is on authentication to ensure integrity of transaction data and customer information in the retail payments environment (this includes P2P and A2A systems)
  - Substantially similar conclusions as in the 2011 supplement
  - Includes examination procedures to evaluate the policies and procedures, business processes, and internal controls of financial institutions and their technology service providers

Other Guidance

- FFIEC InfoBase
  - Includes presentations and other reference material relating to the Handbooks
- FFIEC Authentication FAQ
  - Answers questions based on the 2011 supplement
  - Provides more insight into what is expected of financial institutions

Other Guidance

- Putting an End to Account-Hijacking Identity Theft, FDIC (Jun. 2005)
  - Discusses trends in identity theft
  - Provides information on various authentications methods and controls that can be used to curb identity theft and consumer acceptance of such methods
- ACH corporate account takeover resources
- FinCEN Advisory on identifying account takeover activity

Thoughts on Emphasis

- No specific guidance yet on mobile – perhaps later in 2012 with other updates?
- Potential areas of emphasis for examiners
  - Controls commensurate with risk: how has your business changed?
  - Plan and path to compliance based on risk assessment
  - Enhanced expectations for anomaly detection and cross-channel (enterprise-wide) fraud prevention

Links

- FFIEC 2001 Authentication Guidance
  http://www.ffiec.gov/pdf/pr080801.pdf
- FFIEC 2005 Authentication Guidance
  http://www.ffiec.gov/pdf/authentication_guidance.pdf
- FFIEC 2011 Authentication Supplement
  http://www.ffiec.gov/pdf/Auth-ITS-Final 206-22-11 (FFIEC Formated).pdf
- FFIEC eBanking Handbook
  http://ithandbook.ffiec.gov/it-booklets/e-banking.aspx

Links

- FFIEC Information Security Handbook
  http://ithandbook.ffiec.gov/it-booklets/information-security.aspx
- FFIEC Retail Payment Systems Handbook
  http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems.aspx
- FFIEC InfoBase
  http://ithandbook.ffiec.gov/
- FFIEC Authentication FAQ
  http://www.ffiec.gov/pdf/authentication_faq.pdf

Links

- Putting an End to Account-Hijacking Identity Theft, FDIC
  http://www.fdic.gov/consumers/consumer/idtheftstudy/
- NACHA Corporate Account Takeover Resource Center
  https://www.nacha.org/CorporateAccountTakeoverResourceCenter
- FinCEN Account Takeover Advisory
  http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2011-A016.pdf

Questions?

Andrew Lorentz
Davis Wright Tremaine LLP
1919 Pennsylvania Ave NW, Suite 800
Washington, DC 20006
(202) 973–4232
AndrewLorentz@dwt.com

Disclaimer

This presentation is a publication of Davis Wright Tremaine LLP. Our purpose in making this presentation is to inform our clients and friends of recent legal developments. It is not intended, nor should it be used, as a substitute for specific legal advice as legal counsel may only be given in response to inquiries regarding particular situations.

Attorney advertising. Prior results do not guarantee a similar outcome.