Rationalizing Government Oversight

Thursday, November 17, 2011

Michael B. Benardo
Cyber Fraud & Financial Crimes Section
Division of Risk Management Supervision
Federal Deposit Insurance Corporation
U.S. Regulatory Structure

- Banking Regulator Perspective
- Financial Institutions
- Technology Service Providers
- Payment System Networks
- Payment Processors falling outside the regime
Established in 1979, pursuant to title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978

A formal interagency body empowered to prescribe uniform principles, standards, and report forms for examinations of financial institutions by:

- Board of Governors of the Federal Reserve System (FRB)
- Federal Deposit Insurance Corporation (FDIC)
- National Credit Union Administration (NCUA)
- Office of the Comptroller of the Currency (OCC)
- Consumer Financial Protection Bureau (CFPB)
Example of Interagency Cooperation
Supplement to 2005 Authentication Guidance
Factors that lead to the Supplement
Discussion of the 2011 Supplement
Supplement: Key Points

- Annual, and as needed, risk assessment updates
  - Upgrade controls in response to changing threats
- Retail versus commercial accounts
  - Multifactor recommended for commercial accounts
- Layered security for all “high-risk” accounts
- Enhanced layered security for commercial accounts
  - Detect & respond to anomalous/suspicious activity
  - Enhanced layered security for commercial accounts
- Simple device ID and challenge questions no longer effective as primary control, expect additional controls
- Customer awareness and education efforts
Risk Assessments

- **Supervisory expectation for at least annual risk assessments (RA)**
- **RAs should consider**
  - Changes in internal and external threat environment
  - Changes in customer base
  - Changes in system or application functionality
  - FI fraud trends
- **Controls should be upgraded in response to changing risk**
For first time, agencies distinguish between retail and commercial accounts

Reemphasizes and clarifies expectation for minimum controls for all accounts
Layered Security

- Agencies now expect “layered security” for all accounts
- Defined as different controls at different points in a process so that weakness in one is compensated for by strengths in another
- At a minimum, layered security should include anomaly detection and response
  - At initial customer login, and
  - At initiation of funds transfers to other parties
Controls Considered Ineffective
(as a primary control)

- **Simple device identification**
  - One-dimensional approach that usually relies on a cookie loaded on customer PC
  - Cookie can be copied or moved allowing fraudsters to impersonate legitimate customer

- **Simple challenge questions**
  - Usually a single question (sometimes chosen from a short list) that can be easily answered by anyone who has done an Internet search of the customer or visited their social media page
More Effective Controls

- **Complex device identification**
  - One-time cookie, in conjunction with other factors, used to create digital “fingerprint” of customer PC
  - PC configuration, IP address, geo-location, etc.

- **Complex challenge questions**
  - AKA “out of wallet” questions
  - Do not rely on publically available information
  - Answer more than one question
  - Include a red herring
Customer Awareness

- Customers have an important role to play in online banking security.
- FIs should advise customers on how to practice good online banking security.
- FIs should address Regulation E:
  - Explain protections provided and not provided to account holders relative to electronic funds transfers.