


## Brace Yourself: Updated FFIEC Internet Banking Authentication Guidance is Out

October 13, 2011

Paul Rainbow, Manager  
David Dyk, Manager

**MOSS ADAMS** LLP  
Certified Public Accountants | Business Consultants

*Acumen. Agility. Answers.*



The material appearing in this presentation is for informational purposes only and is not legal or accounting advice. Communication of this information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although these materials may have been prepared by professionals, they should not be used as a substitute for professional services. If legal, accounting, or other professional advice is required, the services of a professional should be sought.

# PRESENTERS



Paul Rainbow, Manager  
IT Consulting  
Moss Adams LLP



David Dyk, Manager  
IT Consulting  
Moss Adams LLP

# AGENDA

- Defining the Problem
- Overview of the Updated FFIEC Guidance
- Options for Compliance
- Advice for Community Banks and Credit Unions
- Questions and Answers



## DEFINING THE PROBLEM

- Dramatic rise in Internet Banking fraud in 2009-2011, due to improvements in malware
- Cross-channel fraud
- Commercial channel focus, with ACH and Wires being highest risk
- Some risk with consumer accounts and small business accounts with bill payment and account transfers to money mules

# THE INTERNET BANKING ENVIRONMENT

- Internet banking fraud risks are increasing, significantly growing in 2009 and 2010
- Resulting lawsuits for account takeovers of business accounts have left liability questions related to UCC 4a murky
- The Regulatory Environment
  - The prior (2005) guidance focused on authentication. The guidance specifically instructed institutions to implement authentication that is stronger than a single factor. Many Financial Institutions implemented device recognition with challenge questions to implement this

# MULTI-FACTOR AUTHENTICATION

- Single factor authentication involves something that the user knows like a password
- A second factor would be something that the user has, like a token
- Many institutions currently have hybrid systems
  - Attempt to validate a password, and recognize the workstation
  - If the workstation is not identified, then an additional “challenge” questions are validated (possibly including out-of-pocket questions)
  - These systems are increasingly less effective. Fraudsters can use malicious software on customer computers to steal challenge questions and passwords, or even steal a time sensitive one-time passcode during authentication
  - Result: These authentication solutions are inherently compromised technologies that no longer provide strong security

## UPDATED FFIEC GUIDANCE

- Regulators and examiners have been considering this issue in recent years, and provided updated guidance in June 2011
- Regulatory scrutiny in the area has increased, and institutions should carefully examine their Internet banking to determine if they are going to need to increase the security of high risk transactions such as ACH batches and wire transfers
- Recent June 2011 guidance will be used by examiners beginning in 2012



# OVERVIEW OF THE GUIDANCE

## OVERVIEW OF THE GUIDANCE - 1

- Differentiation between retail and business transaction risk
  - “Agencies recommend that institutions offer multifactor authentication to their business customers.”
- Continued focus on Risk Assessment
- Continued, increased emphasis on Layered Security Programs

## OVERVIEW OF THE GUIDANCE - 2

- Controls in Layered Security
  - Fraud detection and monitoring systems
  - Include consideration of customer history and behavior and enable a timely and effective institution response
  - Dual customer authorization through different access devices
  - Out-of-band verification for transactions
  - Use of “positive pay,” debit blocks, and other techniques to appropriately limit the transactional use of the account
  - Enhanced controls over account activities; such as transaction value thresholds, payment recipients, number of transactions allowed per day, and allowable payment windows (e.g., days and times)

## OVERVIEW OF THE GUIDANCE - 3

- Controls in Layered Security (continued)
  - Internet protocol (IP) reputation-based tools
  - Policies and practices for addressing customer devices identified as potentially compromised and customers who may be facilitating fraud
  - Enhanced control over changes to account maintenance activities performed by customers either online or through customer service channels
  - Enhanced customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate the risk

## OVERVIEW OF THE GUIDANCE - 4

- Guidance downplays two common controls
  - Device authentication
  - Challenge questions; Encourages remaining challenges to focus on “out of wallet” questions

Security Question

In order for us to verify your identity, please answer the following security question. This question is one that you previously set up with USAA.

What was the high school mascot at the last high school you attended?

> Submit



# OPTIONS FOR COMPLIANCE

# TRADITIONAL TWO-FACTOR AUTHENTICATION

- Can be implemented with physical tokens or “soft tokens”
- Relies on public key encryption generate one-time passcodes that are time sensitive
- This is a relatively effective control, although man-in-the-browser malware can bypass it, so it should not be used alone with high risk transactions

# OUT OF BAND AUTHENTICATION

- Involves confirmation using a channel other than the browser
  - SMS Text Message
  - Voice phone call
- Most effective when:
  - Performed at the transaction level
  - Includes transaction details
  - Requests a positive affirmation (such as a PIN code) to proceed with the transaction
- This is an emerging technology that is quickly gaining industry traction for high risk transactions

# SECURING THE BROWSER

- Generally offered as an “opt in” offering to business customers
- Can be deployed easily as a “bolt on” to existing Internet Banking environments
- Provides software that:
  - Creates a client-to-server encrypted tunnel
  - Prevents keyloggers and other malware from operating
  - May provide an encryption key for additional authentication
- Can be deployed in two ways:
  - Software only (e.g. Trusteer Rapport), using a downloadable program for clients to use
  - Bundled with a USB hardware token (e.g. IronKey), using a secured browser in a virtual operating system

# TRANSACTION MONITORING

- Regulators very clearly indicated these controls can be automated or manual
- Technology solutions focus on identifying unusual patterns, payees, times of day, or other indicators of risk
- The solutions will escalate those high risk transactions for follow-up and manual validation
- To be effective:
  - Implement technology along with an overall anti-fraud or other program
  - When possible, select and implement solutions that examine transactions from multiple channels

# CUSTOMER AGREEMENTS AND LIMITS

- Traditional controls designed to limit fraud risk can be re-visited
  - Credit Limits
  - Customer Agreements
    - Thresholds for volume or dollar limits defined, and enforced by the system
    - Responsibility for implementing and maintaining controls (consider UCC 4a)
- Validate that exposure limits and other customer controls are identified and enforced
- Consider implementing two limits
  - Lower limits for simple authentication only
  - Higher limits with out-of-band verification or other secondary controls that the customer opts-in to

# DEVICE IDENTIFICATION AND REPUTATION

- Generally offered as a cloud-hosted service
- Identifies the source of transactions using large databases across a variety of industries (banking, gambling, large retailers) and assigns a transaction risk score
- To be effective:
  - Requires configuration to assign specific actions (block, escalate for followup, permit) to risk scores
  - Requires a consideration of customers (for example, likelihood of international travel)
  - Requires significant scale and source data from the vendor (e.g. Iovation, Kount)



# CONCLUDING

# CONCLUDING ADVICE FOR SMALLER INSTITUTIONS - 1

- The updated FFIEC guidance reiterates the requirement for regular risk assessment, and provides guidance regarding appropriate controls for internet banking authentication
- The major Internet banking service providers will be rolling out authentication improvements to many of their customers, reducing those costs for any one institution.

## CONCLUDING ADVICE FOR SMALLER INSTITUTIONS - 2

- Smaller community banks with limited volume should consider manual controls, such as verifying high risk transactions through the phone and revisiting credit limits, as a cost effective first step
- Deployment of technical controls such as multi-factor tokens, out of band, enhanced device reputation management, and others should be considered as internet banking providers begin offering them in standard offerings

# RESOURCES

- FFIEC Authentication Guidance
  - <http://bit.ly/FFIEC-AuthGuid11>
- Related Moss Adams authored WIB newsletter articles:
  - <http://bit.ly/MA-InternetBankingArticles>
- Ask us!

# QUESTIONS?

[david.dyk@mossadams.com](mailto:david.dyk@mossadams.com)

503-512-0004



[paul.rainbow@mossadams.com](mailto:paul.rainbow@mossadams.com)

509-777-0230

