

# ONLINE FRAUD AND CYBER CRIME

## UNDERSTANDING RISKS AND GUIDANCE



Presented by:

PAUL A. CARRUBBA

Adams and Reese LLP

Phone: (601) 292-0788

E-Mail: [paul.carrubba@arlaw.com](mailto:paul.carrubba@arlaw.com)

ADAMS AND REESE LLP

***Paul Carrubba***

Adams and Reese LLP

# Paul Carrubba

ADAMS AND REESE LLP

- Paul is a partner in the law firm of Adams and Reese LLP. His primary focus is on Banking Law and legal issues dealing with payments system laws and regulations and bank operations issues. He has over 37 years of experience in the banking industry as a Bank Operations Manager, a consultant, an author, and an attorney. Mr. Carrubba is the author of five books including: *Revised UCC Article 3 and 4*, *A Banker's Guide to Checks* and *Principles of Banking*. He is the co-author, with Dan Fisher, of both *Remote Deposit Capture – Practical Considerations* and most recently, *Risk Management Series – Remote Deposit Capture*.

# Presentation Content

THIS PRESENTATION IS DESIGNED TO PROVIDE ACCURATE AND AUTHORITATIVE INFORMATION REGARDING ITS SUBJECT MATTER. IT IS PRESENTED WITH THE UNDERSTANDING THAT THE PRESENTER IS NOT RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF LEGAL ADVICE OR OTHER EXPERT ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT.

# Introduction

4

- FFIEC 2001 Guidance
- FFIEC 2005 Guidance
- FFIEC Supplemental Guidance
- Case Law

# BACKGROUND – FFIEC 2001 GUIDANCE

5

Authentication in an Electronic Banking Environment – August 8, 2001

- Risk Assessment
  - ▣ Enterprise – Wide approach
  - ▣ Method of Authentication
  - ▣ Single factor may not be sufficient
  - ▣ Should consider multifactor authentication
  - ▣ Agreement term
- Account Origination and Customer Verification
  - ▣ Customer Identification
  - ▣ Positive Verification
  - ▣ Logical
  - ▣ Negative
- Monitoring and Reporting

# Background – FFIEC 2005 Guidance

6

## MULTIFACTOR AUTHENTICATION

- Issued October 12, 2005
- Updates 2001 Guidance
- December 2006 Compliance Date
- Applies to Retail and Commercial Customers

# FFIEC 2005 GUIDANCE

7

- Risk Assessment
- Single-Factor Authentication is Inadequate
- FI's Should Use Effective Methods of Authentication
- Authentication Should Be Appropriate to the Risks
- Single-Factor Authentication Results in Fraud and ID Theft
- Financial Institutions Should Implement:
  - Multi Factor Authentication
  - Layered Security
  - Other Controls to Mitigate Risk

# FFIEC 2005 GUIDANCE

8

## MULTIFACTOR AUTHENTICATION

- Authentication Factors
  - ▣ Something a Person Knows
    - Shared Secrets – Password – PIN
    - Mortgage Amount – Mother's Maiden Name
  - ▣ Something a Person Has
    - USB Token – Smart Card
    - Password – Generating Token
  - ▣ Something a Person Is
    - Biometrics – Fingerprints – Face – Voice
    - Retinal and Iris Scan

# SUPPLEMENTAL GUIDANCE ON INTERNET BANKING AUTHENTICATION

9

## PURPOSE OF GUIDANCE

- Reinforce Risk-Management Framework of the 2005 Guidance
- Growth of Electronic Banking and Sophistication Threats have Increased
- Substantial Losses from Account Take-over
- Effective Security is Essential

# SUPERVISORS EXPECTATIONS

10

## □ RISK ASSESSMENTS

- Reiterates 2005 Guidance to Perform Risk Assessments
- Review and Update Existing Risk Assessments Prior to Implementing New Service – at Least Every 12 Months

## □ RISK ASSESSMENTS SHOULD CONSIDER

- Changes in Internal and External Threat Environment
- Changes in Customer Base
- Changes in Functionality
- Actual Incidents of Security Breach

# CUSTOMER AUTHENTICATION

11

- HIGH RISK TRANSACTIONS
  - ▣ Access to Customer Information
  - ▣ Movement of Funds to other Parties
- RETAIL/CONSUMER BANKING
  - ▣ Access Account Information
  - ▣ Bill Pay, Intra-bank Transfers
  - ▣ Wire Transfers and P to P
  - ▣ RISK LESS THAN LARGE COMMERCIAL TRANSACTIONS
  - ▣ IMPLEMENT LAYERED SECURITY

# BUSINESS / COMMERCIAL BANKING

12

- ▣ High Dollar, Frequent Transactions
- ▣ Internal Transfers
- ▣ ACH Debits and Credits, Third Party Providers and Senders
- ▣ Wire Transfers
- ▣ Implement Layered Security and Multifactor Authentication

# LAYERED SECURITY

13

- DIFFERENT CONTROLS AT DIFFERENT POINTS
- CAN STRENGTHEN OVERALL SECURITY
- LAYERED SECURITY PROGRAM
  - ▣ Fraud Detection and Monitoring
  - ▣ Dual Customer Authentication through Different Devices
  - ▣ Out-of-Band Verification
  - ▣ Positive Pay – ACH Block
  - ▣ Transaction Limits – Amount and Numbers
  - ▣ Establish Calendars
  - ▣ Internet Protocol to Block Connections
  - ▣ Address Customer Device Compromise
  - ▣ Controls over Account Maintenance
  - ▣ Customer Awareness

# MINIMUM LAYERED SECURITY PROGRAM

14

- DETECT AND RESPOND TO SUSPICIOUS ACTIVITY
  - Initial Login Authentication
  - Monitor and Track Transactions
- CONTROL OF ADMINISTRATIVE FUNCTIONS
  - Change in System Configuration
  - Verification of Changes
  - Out-of-Band Verification

# EFFECTIVENESS OF CERTAIN AUTHENTICATION TECHNIQUES

15

## □ DEVICE IDENTIFICATION

- ▣ Cookies may be copied
- ▣ Geo-Location or IP Address may be Manipulated
- ▣ Single Simple Device Identification is not Effective
- ▣ Use “One-Time” Cookies

## □ CHALLENGE QUESTIONS

- ▣ Questions can be Compromised
- ▣ Use “Out of Wallet” Questions
- ▣ Use Multiple Sophisticated Questions

# CUSTOMER AWARENESS AND EDUCATION

16

- APPLICABILITY OF REG E AND PROTECTIONS
- UNSOLICITED CONTACT BY FINANCIAL INSTITUTION
- SUGGEST COMMERCIAL CUSTOMERS PERFORM RISK ASSESSMENTS (PUT IN AGREEMENT)
- LIST OF ALTERNATIVE RISK CONTROL MECHANISMS
- LIST OF INSTITUTIONAL CONTACTS

# CONTROLS

17

- ❑ ANTI-MALWARE SOFTWARE
- ❑ TRANSACTIONS MONITORING/ANOMALY DETECTION SOFTWARE
- ❑ OUT-OF-BAND AUTHENTICATION
- ❑ USB DEVICES TO ENABLE A SECURE LINK
- ❑ FUNDS TRANSFER BENEFICIARY LISTS
- ❑ LAYERED SECURITY CONTROLS

# UCC 4A

## CASE LAW

# UCC 4A, Reg E

19

## UCC ARTICLE 4A

- Applies to Funds Transfers
- Does Not Apply to Transfers Governed by EFTA (Reg. E)
- Authorized Transfers Enforceable
- Unauthorized Transfers Enforceable if:
  - Verified Pursuant to Security Procedure
  - Security Procedure is Commercially Reasonable
  - Bank Accepted it in Good Faith and in Compliance with Security Procedure

# UCC 4A, Reg E

20

## UCC ARTICLE 4A

- Unauthorized Transfers Not Enforceable if:
  - ▣ Bank Agrees not to Enforce
  - ▣ No Security Procedure
  - ▣ Security Procedure is not Commercially Reasonable
  - ▣ Not Made by Authorized Person or Person Entrusted with Security Procedure
  - ▣ Not Made by Person who Obtained Access to Transmitting Facility
  - ▣ Made by Person that Obtained Security Procedure from a Source not Controlled by the Customer

# SECURITY PROCEDURES

21

## Security Procedure

- Procedure to Verify Authenticity
- Procedure to Detect Error

## Commercially Reasonable Security Procedure

- Question of Law Considering
  - Circumstances Known to Bank
  - Alternative Security Procedures Offered
  - Security Procedures in General Use

# CASES

22

- PlainsCapital Bank v. Hillary Machinery, Inc.
- Shames-Yeakel v. Citizens Financial Bank
- Experi-Metal v. Comerica
- Patco Construction Company, Inc. v. Peoples United Bank

# PlainsCapital Bank v. Hillary Machinery

23

- Account Takeover
- Transferred \$800,000
- Bank Recovered \$600,000
- Bank Filed Suit for Declaratory Judgment
  - Bank Followed Security Procedures
  - Security Procedures were Commercially Reasonable
  - Transfers are Enforceable
- Hillary Machinery Counter Claimed
- Case Settled

# SHAMES-YEAKEL V. CITIZENS BANK

24

- Plaintiff Operated Accounting and Bookkeeping Company
- Linked HELOC to Business Account
- \$26,500 Unauthorized Transfer Made
- Ten Days Later, Plaintiff Contacts Bank
- Agreement Provides for Password and Company ID
- Expert Opined Security Procedures were Commercially Reasonable
- Plaintiff Claimed Bank did not Comply with 2005 FFIEC Guidance
- Court Held Procedures not Commercially Reasonable for Failure to Comply with Guidance

# EXPERI-METAL V. COMMERCIA BANK

25

- ❑ EMI Employee Responded to Phishing E-Mail
- ❑ Clicked on Site and Entered PIN, Password and Token Password
- ❑ Over 90 Transfers Initiated
- ❑ Bank Filed Motion for Summary Judgment
- ❑ Court Partially Granted Holding Security Procedures were Commercially Reasonable
- ❑ Did Bank Accept Transfer in Good Faith?
- ❑ Court Held Failed to Provide Evidence of Good Faith

# PATCO CONSTRUCTION V. OCEAN BANK

26

- Unauthorized Transfers Totaling \$588,000 were made over Several Days
- Ocean Bank Blocked \$243,000
- Transfers Made from Unrecognized Device and IP Address
- Banks Security Procedures Included:
  - Password and ID
  - Challenge Questions
  - Risk Profiling
  - Device Cookies
  - Dollar Amount Rule
  - Subscription to eFraud Network
  - Customer Should Review Transactions Daily

# Patco, cont.

27

- Court Held:
  - ▣ Agreement Provided for Security Procedures
  - ▣ Course of Dealing
  - ▣ Both Parties Relied on FFIEC 2005 Guidance
  - ▣ Authentication was Multifactor and Layered Security
  - ▣ Security Procedure was Commercially Reasonable
  - ▣ Security Procedure does not have to be the Best
  - ▣ Patco Could have Mitigated Damages
  - ▣ Grants Summary Judgment Motion

# AGREEMENTS

28

- Online/Internet Banking Agreements
- Wire Transfer Agreements
- ACH Origination Agreements

# AGREEMENTS

29

- Security Procedure
- Customer Agrees is Commercially Reasonable
- Customer Agrees to be Bound
- Customer will Safeguard Security Procedure
- Customer will Scan Personal Computer
- Customer will Give Notification of Unauthorized Transfer

# Conclusions and Questions

- [www.adamsandreese.com](http://www.adamsandreese.com)
- Email: [paul.carrubba@arlaw.com](mailto:paul.carrubba@arlaw.com)

# ONLINE FRAUD AND CYBER CRIME

## UNDERSTANDING RISKS AND GUIDANCE



Presented by:

PAUL A. CARRUBBA

Adams and Reese LLP

Phone: (601) 292-0788

E-Mail: [paul.carrubba@arlaw.com](mailto:paul.carrubba@arlaw.com)



***Paul Carrubba***

Adams and Reese LLP