E-Banking Regulatory Update

Hal R. Paretchan, CISA, CISSP, CFE
Information Technology Specialist
Federal Reserve Bank of Boston
Supervision, Regulation & Credit
(617) 973-5971 – hal.paretchan@bos.frb.org
Objectives

• Why is the guidance needed?
• E-Banking Background
• Regulatory Guidance - SR Letter 05-19
• Risk Assessment
• Effective Authentication System
• Outsourcing Responsibility
• Questions
Threat Assessment

From the perspective of the Internet user

• Malicious code
• Phishing attacks
• Vishing attacks
• Pharming
Malicious Code

• There are number of ways malicious code can get on your PC

• Visiting the wrong website

• Email attachments
  – Viruses: Zero-Day attacks go undetected
Malicious Example: World Cup

What was the big story of the World Cup?

Malicious Code: Keylogger
• Software sold on Russian Site
• As little as $20
• Capture all your keystokes and send them to attacker.
• For every website you log into – your username and password are captured.
Malicious Example: Pop-up Window

- American Express customers targeted in May 06.
- A virus attached to victim’s Internet Explorer browser
- Once victim visited the legitimate site, a pop-up window appeared asking for account information
Phishing Example

Goal: Get user’s personal information

Two main elements:
1. Email
   - Penalty for non-compliance
   - Time sensitive
   - Convenient link to company’s website

2. Phony Website
   - Has look and feel of the real website
   - Requires you to provide your credentials
   - Some even pass you through to real website
Phishing Example: PayPal

Source:
http://www.antiphishing.org/
Vishing Example: PayPal

Similar to Phishing but instead you are given a phone number to call.

Again you are asked for personal information.
Pharming Explained

Domain Name Server (DNS) poisoning

- DNS is like a phonebook for the Internet
  www.anyurl.com = 198.27.1.200

- Good IP addresses are replaced with bad ones redirecting user

- Your browser would not know the difference
What do all these attacks have in common?

- Thieves want your credentials

- They want them to enter your username & password and get access to your funds

- Or they want to sell them to other thieves
How does this make money?

A credit card can be worth $1000.00

In the Pay Pal scams, if you send 100,000 emails…
and 1% of the recipients thinks it is real and goes to the phishing website…
and 1% of them actually submits their information…
you just stole 10 credit cards.

10 @ $1,000.00 = $10,000
e-Banking Background

E-Banking is:
‘the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels’

FFIEC E-Banking Booklet – August 2003
Two Types of Websites

Informational
- Provides customers with general information on bank’s products and services
- Includes contact information

Transactional
- Provides customers with the ability to conduct transactions through the website
  - Initiating banking transactions
  - Buying products and services
Transactional e-Banking Retail/Wholesale Products & Svcs.

**RETAIL**
- Account Management
- Bill payment and presentment
- New account opening
- Consumer wire transfer
- Investment/Brokerage services
- Loan application and approval
- Account aggregation

**WHOLESALE**
- Account Management
- Cash management
- Commercial wire transfer
- Business-to-business payments
- Employee benefits/pension administration
SR 05-19 Interagency Guidance on Authentication in an Internet Banking Environment

- Updates and replaces 2001 FFIEC guidance entitled ‘Authentication in an Electronic Banking Environment’
SR 05-19 Key Points

- A High-Risk Transaction is a transaction that involves access to Customer Information or the movement of funds to other parties.

- Using single factor authentication as the only control mechanism is inadequate for High-risk Transactions.

- Not “Multifactor”
SR 05-19 Compliance

By December 31, 2006:

• Financial Institutions are require to have completed a risk assessment of all their e-Banking products and services and identify all High Risk transactions.

• Develop and fully implement a plan to mitigate the risks.
Risk Assessment

The risks should be assessed based on the following:

- Type of customer (e.g. retail or commercial)
- Customer’s transactional capabilities (e.g. bill payment, wire transfer, loan origination)
- Sensitivity of customer information
- Ease of using communication method
- Volume of transactions

Based on the assessment a Financial Institution will determine what level of authentication is required.
Effective Authentication Systems...

- Safeguard Customer Information
- Prevent Money Laundering
- Prevent Terrorist Financing
- Reduce Fraud
- Inhibit Identity Theft
- Promote legal enforceability of electronic agreements and transactions
Strong Authentication

Combination of 2 or more of the following:

1. Something you KNOW
   - PIN, Password, Account #, UserID

2. Something you HAVE
   - Token, SecureID, Card, Smart Card
   - Geo Location

3. Something you ARE
   - Biometrics

4. Mutual authentication

*Single Factor authentication uses only one!*
Single Factor vs. Multifactor Authentication

**Single factor** (Used for low risk product and services) :
Pros – cheaper, easier to implement, less burden on customer
Cons – weak security and more susceptible to phishing attacks

**Multifactor** (Used for High Risk products and services) :
Pros – greater level of security and non-repudiation
Cons – expensive, complicated to implement and puts a greater burden on customer

Guidance does not specifically require the use of Multifactor authentication; layered security and other means are permitted.
Authentication Methods

- Customer passwords
- Bingo Cards
- Personal identification numbers (PINs)
- Digital Certificates using public key infrastructure (PKI)
- Smart Cards
- One-time passwords
- USB plug-ins
- Transaction profile scripts
- Biometric identification
- Mutual Authentication
- Out of Band Authentication
Layered Security

• Analyze customer activities to identify suspicious patterns

• Establish preset transaction limits

• Establish preset list of transaction recipients

• Out of band confirmations
Outsourcing Responsibility

While the institution does not have to manage the daily administration of the website component systems, its management and board remain responsible for the content, performance, and security of the e-banking system.
Third Party Oversight

Types of monitoring reports:
• E-banking service availability
• Activity levels and service
• Performance efficiency
• Security incidents
• Vendor stability
• Quality assurance
E-BANKING

Questions
Useful Links

• Report ID Theft to FTC
  www.consumer.gov/idtheft

• FFIEC E-Banking Handbook
  www..ffiec.gov/ffiecinfolbase/booklets/e_banking/e_banking.pdf

• SR 05-19 Guidance on Authentication in an Internet Banking Environment

• SR 04-14 FFIEC Brochure with Information on Internet "Phishing"