Wire Authentication Best Practices
April 10, 2018

Meredith Piotti, CPA, CIA
Nicholas Jesi, CISA
Before we get started…

• Today’s presentation slides can be downloaded at www.wolfandco.com/webinars/2018.

• The session will last about 45 minutes, and we’ll then have time for Q & A.

• Our audience will be muted during the session.

• Please send your questions in using the “Questions Box” located on the webinar’s control panel.
About Wolf & Company, P.C.

- Established in 1911
- Offers Audit, Tax, and Risk Management services
- Offices located in:
  - Boston, Massachusetts
  - Springfield, Massachusetts
  - Livingston, NJ
- Over 250 professionals

As a leading regional firm founded in 1911, we provide our clients with specialized industry expertise and responsive service.
Financial Institution Expertise

• Over 75 Risk Management Professionals:
  – IT Assurance Services Group
  – Internal Audit Services Group
  – Regulatory Compliance Services Group
  – WolfPAC® Solutions Group

• Provide services to over 300 financial institutions:
  – Approximately 85 FIs with assets > $1B
  – Approximately 40 publicly traded FIs
  – Constant regulatory review of our deliverables

• Provide Risk Management Services in 27 states and 2 U.S. territories
Meet Today’s Presenters

Meredith Piotti, CPA, CIA
Internal Audit Senior Manager
Phone: 617-933-3353
Email: mpiotti@wolfandco.com

Nicholas Jesi, CISA
IT Assurance Manager
Phone: 617-933-3373
Email: njesi@wolfandco.com
Today’s Agenda

• Evolving World of Internet Banking

• Required Controls
  – Corporate Account Take Overs
  – Security Awareness Training
  – Customer Authentication
  – Callbacks
  – Customer Activity Monitoring

• Current Environment
  – Examples of When Good Controls Fail
  – Putting it in Action
The Rise of Technology

- Growth and expansion of internet banking and mobile technologies
- New and evolving threats
- Key control factors to implement to help mitigate risk
Customer Session Controls

- Multifactor authentication
- Complex passwords
- Password Expiration
- Account Lockout
- Inactivity time
- Up to date certificate encryption
- Complex device printing
- IP address matching / geo location (behavioral analysis)
The three most common categories are often described as:

- something you know (the knowledge factor)
- something you have (the possession factor)
- something you are (the inherence factor).
Multi-Factor Authentication

• Required Systems

• Testing

• MFA Risk Assessment - Authentication in an Internet Banking Environment (AIBE)
Wire Transfer Risks
Customer Authentication – Fraud Risks

• Internal Threats
  – Controls allow for employees to bypass
  – No review of bypass

• External Threats
  – Caller is trying to gain information
  – Caller has some fake information
  – Customer has allowed credentials to be compromised
  – Fraudster has installed call forwarding
  – Fraudster has intercepted email or changed email address
Customer Authentication – Balancing Security

Types of Transaction
- Viewing Account
- Wire
- ACH Origination

Access Controls
- Passwords
- Tokens
- Out of Wallet
Customer Authentication – Stolen Credentials

- 64,000 security incidents; 2260 breaches tallied by Verizon
- Public, entertainment, finance, and information sectors
- Majority of actors motivated by money
- Hacking, malware, phishing
- Prevention techniques: email filtering, employee awareness, and training.

Food for Thought: Think about the weakest link.
Customer Authentication

Challenge Questions… it’s about what you can’t find here
Customer Authentication

• Challenge questions need to be “out of wallet”
  
  – What’s the magic number?
  
  – Trick the fraudster
  
  – One by one
Customer Authentication

- Policies
  - What transactions can take place?
  - Permissible channels
  - Authentication Process
  - Exceptions
  - Denial of access
Customer Authentication - Exceptions

• All customer’s have PINS except….  
  – If the account was opened before 2010  
  – The customer complained  
  – They haven’t responded to our requests

• Exception monitoring process  
• Client acknowledgement  
• Cutting off access
Customer Authentication – Denial of Access

- 1, 2, 3 strikes?
- Leading the witness
- Training the front line
Other things to consider:

- Complaint monitoring
- Other channels
- Coverage of monitoring
Call Back Risks

Technology is a useful servant but a dangerous master.

- CHRISTIAN LOUS LANGE -
Call Back Risks

• Mitigating the risk
  – Only call back numbers on file
  – Ensure call back information is deemed a critical change
  – Do not permit requests by email
  – Institute PINs/biometrics
Customer Transaction Controls

- Behavioral Analysis
- Transaction limits
- Call back
Customer Transaction Controls

• Setting limits
  – Verify they are reasonable for activity
  – Business vs customer

• Who doesn’t get access?
  – Which products are restricted?
  – What history is needed to open restricted products?
Customer Behavior

- Millennials disrupted societal norms
- Looking beyond them
  - Born after Jan. 1 2001 and 9/11
  - The Internet of Everything
- “GenZ” will build
Corporate Account Take Over (CATO) Process

Phishing attack or social engineering

Malware is installed

Malware collects and transmits authentication details

Hacker logs into business online banking and initiates fund transfer to foreign bank

Mule withdraws transferred funds
CATO Threats

- Customer's lack of knowledge of the risks associated with online payment systems
- Customer can change a wire/ACH transaction without further authentication
  - Fraudulent transfer of customer funds via the online wire/ACH system
  - Inadequate institution staffing and risk awareness
- Unauthorized access to system
- Unauthorized access to Bank Admin Portal
CATO Controls - Oversight

• Assign responsibility
• IT Steering Committee meeting minutes
• Board reporting
• Risk assessments
• Project plans
CATO Controls – Specific

• Layered security controls
  – Administrative
  – Customer end point controls
  – Customer session controls
  – Customer transaction controls

• Incident response plan
• Risk Assessments
• Customer and Employee Education and Awareness
Customer Education and Awareness

- Methods by which the Bank would contact the customer and what they would ask for
  - Securing personal information and smart passwords
  - Warning signs that they have been compromised
  - Bank contact for suspected compromise
Customer Education and Awareness

- Advanced Security options (access levels, admin monitoring, segregation of duties, reports, optional controls)
- Network security (antivirus, firewall, patch management, access privileges, network segmentation, etc….)
- Informing customers that their money is not insured and recommending cyber security insurance
Fraud Scenario

• Fraud:
  “Anticipating that the bank typically validates a customer’s wire request by calling them, the criminal also processes a temporary call forwarding arrangement with the customer’s phone company. This enables the criminal to intercept the validation call and impersonate the customer by using more of the information gleaned from various online sources. The bank approves the wire. Funds are wired to an account at another institution, and immediately forwarded out the country.”

• Solution:
  Implementing a customer PIN program to validate wire transfer requests. This PIN can be stored in the bank’s core account system. It should never appear on a loan document stored in a local Registry of Deeds.
The Hack of a Retail Customer

2-3 weeks

1. Criminal social engineers user via a phone call (fake Microsoft support) and gets them to install malware

2. Criminal researches customer and finds home equity line of credit with over $200,000 in available funds. Criminal also finds spreadsheet with passwords

3. Criminal calls the bank multiple times to gather information on account (includes identifying the out of wallet questions)

4. Wife on bank account calls bank and notifies them that their PC has malware

5. Criminal goes to registry of deeds and obtains customer’s signature

Malware had C2 and keylogging functionality that compromised
- Online banking
- Time Warner Cable email address
- Time Warner Cable phone system
The Wire

**Day 1**

1. Criminal initiates 1st wire ($90,000) via phone and answers all in wallet and out of wallet questions

2. Bank performs call back

3. Hacker routes call to another number and authorizes wire

**Day 2**

4. Hacker initiates second wire (maximizing the funds available within HELOC) the next day

**Day 3**

5. Second wire triggers a BSA alert, money wired oversees

Bank responsible for 200,000 + fraudulent wire

Files claim with insurance agency
What went wrong?

- Suspicious activity
  - Calls into the bank did not raise a red flag with the customer support staff
  - Request for wire money to a different state using funds for a home equity line of credit based on customer’s history was suspicious
- Customer notification of hacked PC did not increase customer transaction monitoring or freeze any type of transactions
- BSA system failed to prevent the transaction, only notified after the fact of suspicious activity
Take Aways

• Customers can be the weakest link → Train them on the threats!

• Call Back alone are no longer enough → STRONG authentication controls are critical!

• Ensure you have controls to monitor compliance with Policy → Institute follow-up action for noncompliance

• Develop mechanism for spotting behavior anomalies → Increase level of authentication in these situations.
Questions?

Meredith Piotti, CPA, CIA
Internal Audit Senior Manager
Phone: 617-933-3353
Email: mpiotti@wolfandco.com

Nicholas Jesi, CISA
IT Assurance Manager
Phone: 617-933-3373
Email: njesi@wolfandco.com