UNDERSTANDING & PREVENTING FRAUD

Regions Treasury Management
CONNIE PAYNE, SENIOR VICE PRESIDENT ONLINE SOLUTIONS
NOTICE

This presentation has been prepared for discussion purposes only. No representations or warranties are given or implied, no guarantee is made as to the accuracy or completeness of the information herein, and no guarantee is made that the information herein does not contain errors. This presentation does not confer any rights, and neither Regions Financial Corporation nor any of its affiliates accepts any liability for the content of this presentation or for any actions taken or not taken in reliance on such content. Financial products and services provided by Regions Financial Corporation and/or its affiliates are subject to the terms and conditions of the applicable product and service agreements. Electronic banking and financial services customers are solely responsible for providing for and maintaining the physical, electronic, procedural, administrative, and technical security of data and systems in their possession or under their control.
Fraud is a Prevailing Threat

Percent of Organizations Subject to Attempted and/or Actual Payments Fraud

Nearly two-thirds of organizations have been victims of fraud

› 50% of organizations with less than $1 billion in annual revenue experienced payments fraud
› 67% of organizations with over $1 billion in annual revenue experienced payments fraud
Losses Impact the Bottom Line

- Organizations in the U.S. lose about 5% of their revenue to fraud

- Checks are the most vulnerable payment type to fraud attacks

- Many fraud incidents within a small business involve employees

- The average fraud scheme goes undetected for 18 months

Typical loss due to fraud -- $20,300
Education is Key to Prevention

QUESTIONS TO ADDRESS

- Are your funds and information being transferred securely?
- Are you losing revenue to fraud?
- Are your internal controls strong enough?
- Are you receiving phishing emails and malware attempts?
- Are you aware of the latest fraud trends?
- Are you keeping company information private?
- Are your vendors legitimate?
- Are you aware of the latest fraud trends?
Bookkeeping Fraud can Greatly Impact Small Businesses

› Perpetrated by a trusted employee
› Arises when full authority has been given to issue and reconcile payments which is especially common in small businesses
› May also be associated with investment schemes, sales schemes or identity theft

Red Flags:
✓ Living beyond their means
✓ Financial difficulties
✓ Unusually close association with vendors or customers
✓ Excessive control issues
Preventing Bookkeeping Fraud

- Never Sign Blank Checks
- Establish Dual Control for Check Issuance & Account Reconciliation
- Ensure all Employees are Aware and Adhere to Internal Controls & Financial Reporting
- Restrict Employee Access to Accounting Systems & Online Functions; Audit Periodically
- Implement an Approval process for New Vendors
Payments Best Practices

› Reconcile accounts in a timely manner.

› Convert paper payments to electronic.

› Securely store check stock, deposit slips and bank statements then destroy securely.

› Place stop payment on any check that has left your possession.

› Utilize Positive Pay services for checks and ACH.
Cyber Attack Target: Business Accounts

- High dollar balances in checking accounts

- Money can be moved quickly
  - Real-time using Wire Transfer
  - Near real-time using ACH

- Commercial computers represent a target-rich environment for other corporate information
Where Are the Fraudsters?

- Ringleaders and Malware authors are in Russia and Ukraine
- Software is for sale on the Darknet (underground internet)
- Command and Control servers along with botnet servers are for rent
  - These are used to disperse the malware
- The actual thief may be in the house or office next door
Methods of Attack

- Phishing emails with malicious links or attachments
- Banner ads on prominent surf engines and news sites
- Social networking sites (your friends may not be your friends)
- Probing for un-patched, vulnerable machines and attacking directly
Methods of Attack

User opens email, clicks a malicious link or clicks a banner ad and the root kit is installed by the fraudster.
Methods of Attack

- Root kit installs itself deep within the client’s operating system.
- Root kit “phones home” across the internet to a Command and Control server. It tells the Command and Control server “I am here. Send me the rest of the malware payload.”
Malware disables anti-virus software. (The indicator in the system tray isn’t necessarily affected, so the user doesn’t know that anti-virus has been disabled.)
Software (malware) is running in the background as a service. It waits for the user to connect to iTreasury, or any online banking service. As soon as that happens, an instant message is sent out to the criminal, alerting him that the user is online.
Methods of Attack

User enters logon credentials and token pin and malware executes a “man in the browser” attack

- Code is injected onto the user’s web page with a message such as “iTreasury is down” or “OnePass is down;” “please try again in 15 minutes”
Meanwhile, key logging software in the malware has captured the logon credentials which are sent via Instant Messaging to the bad guy.
The criminal now logs on to the financial service.

He now has the ability to do everything that the user is entitled to do.
Methods of Attack

For any financial service requiring a token for ACH and Wire Transfer release, the criminal can create the transaction and wait for another opportunity to release the transaction.

IF the client is using dual authorization and the approver is NOT infected, then there won’t be fraud.

Also, with the introduction of Regions OnePass and Regions Out of Band Authentication, Regions is helping to prevent this type of fraud.
Money is usually sent to mules, who are recruited to accept Wire Transfers and/or ACH payments. The mules then withdraw the funds and wire the money outside the U.S.
Internet Banking Best Practices

• Dual Control for transaction initiation
  – Wire and ACH
  – E-mail Alerts for Approvals

• Daily reconcilement

• Secure environment
  – Dedicated PC and/or limit web surfing
  – Firewall, Anti-virus, Anti-malware, Anti-spyware

• Use strong passwords and protect them

• Don’t click on links in suspicious e-mails
Fraud Prevention Best Practices for payments, online and bookkeeper fraud can be found at regions.com/stopfraud

Other resources:

- Internet Crime Complaint Center
  www.ic3.gov

- Safe Checks Fraud Bulletin
  http://www.safechecks.com/services/fraudbulletin.html

Surveys and Other Sources Cited:

2013 AFP Payments Fraud and Control Survey
Association of Certified Fraud Examiners (acfe.com)