Risky Business: How Companies Fall Victim to Fraud

Presented by:

Tony Okray

Julie Latchaw

Julie Lombardi

FIRSTMERIT Bank

Member FDIC

Agenda:

- Fraud Statistics– Fun With Numbers
- Check Fraud & ACH Fraud
- Your Role in Preventing Fraud
- Fraud Schemes Targeting Your Organization
- Fraud Techniques

FIRSTMERIT Bank

Fraud Statistics:

2016 Association for Financial Professionals Fraud & Control Survey:

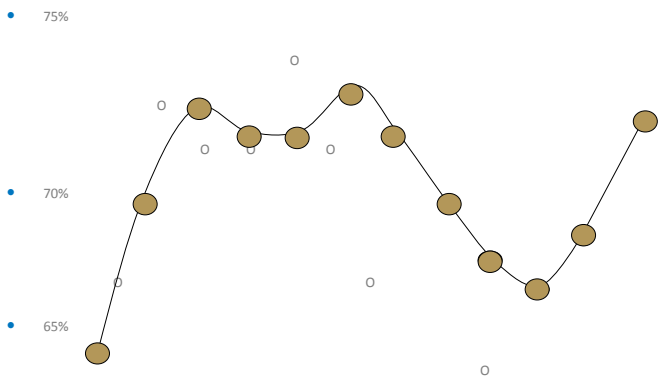
- 73% of organizations surveyed experienced attempted or actual fraud in 2015
- 11% increase in fraud incidents compared to 2014
- Checks were the payment format most frequently targeted for fraud, with 71% of attacked organizations reporting that their checks were involved. Other payments formats targeted were:
  - Wire fraud 48%
  - Corporate/debit cards 39%
  - ACH debit 25%

FIRSTMERIT. Bank

Fraud Statistics:

2016 AFP Fraud & Control Survey Historical Data:

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



FIRSTMERIT. Bank

Fraud Statistics:

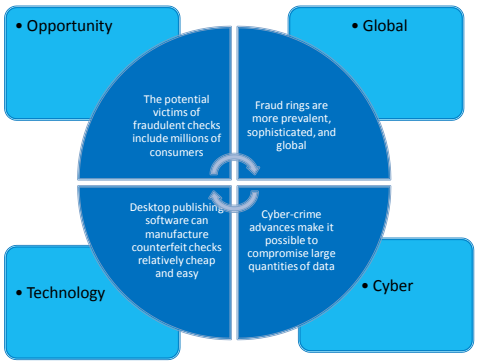
2016 Association for Financial Professionals Fraud & Control Survey:

- 17% of companies – had no financial loss
- 25% of companies – potential loss was less than $25,000
- 29% of companies - $25,000 – 249,999
- 27% of companies – greater than $250,000

Payment Method Responsible for Largest Dollar Amount Loss:

FIRSTMERIT. Bank

Why is Fraud So Prevalent?



FIRSTMERIT. Bank

Fraud Statistics:

- Organizations used a number of fraud prevention control services provided by banks, including:
  - Check Positive Pay (used by 88%)
  - Daily reconciliations (77%)
  - Segregation of account (69%)
  - Payee Positive pay (56%)

FIRSTMERIT Bank

Types of Check Fraud:

- Forged Signatures
- Forged & Improper Endorsements
- Counterfeit Checks
- Altered Checks

FIRSTMERIT Bank

Check Fraud: Organizational Preventative Measures

- Division of Responsibility – Assign A/P function to more than one person. This approach makes it more difficult for employees to tamper with checks and payments.
- Reconcile all accounts promptly and regularly – quick fraud detection increases the likelihood of recovery.
- Protect accounts payable – verify all new supplier entries.
- Protect accounts payable – physical controls on check stock.
- Safekeeping of paid checks via online or CD.
- Destruction of checks deposited via Remote Deposit Capture
- Enforce mandatory vacation policies

FIRSTMERIT. Bank

Check Fraud: Bank-Assisted Preventative Measures

- Positive Pay (Bank-Match)
  - Organization creates an electronic file that contains each check generated from the A/P or Payroll accounting system.
    - This file is securely transmitted to the Bank where it is added to a master outstanding list and later matched to the actual check when it is presented for payment.
  - When a check is presented for payment, the Bank compares the check against the positive pay file. Any discrepancy (i.e. dollar amount or check number) trigger a stop in the processing of the check.
  - The Bank notifies the organization that an information mis-match has been identified and requires a pay / no-pay decision on the item.
    - A no-pay decision returns the check to the bank of first deposit and eliminates the potential loss to the organization

FIRSTMERIT. Bank

Check Fraud: Bank-Assisted Preventative Measures

- Reverse Positive Pay (Client-Match)
  - Organization does not create an electronic check file.
  - All checks are presented for payment against the account.
  - Organization works on a 'prior-day' basis to match bank postings against internal postings.
    - MUST be reviewed each business day
  - Organization is responsible for notifying Bank of any checks that need to be returned to the bank of first deposit.
- Check Block
  - Account is restricted to depository and/or electronic (ACH) activity only.

FIRSTMERIT Bank

Understanding ACH Fraud:

- Automated Clearing House (ACH) debit fraud is the risk that a transaction will be initiated or altered in an attempt to misdirect or misappropriate the funds.
- ACH fraud is relatively simple to perpetrate:
  - ACH is easy to process by banks
  - ACH is a widely-accepted transaction
  - ACH offers flexibility for a variety of payment applications
- Any ACH debit may post to your account if no proactive fraud prevention measures are in place.
- Critical elements of ACH fraud – the account number and the routing number can be obtained from any given check
- Corporate Account Takeover – online access is hacked

FIRSTMERIT Bank

ACH Fraud: Organizational Preventative Measures

- Division of Responsibility – Segregation of duty between setting up an ACH, initiating an ACH and sending.
- Watch for inflated batch files.
- Watch for alerts to changes being made to batches.
- Review audit logs.
- Have ACH limits in place.

FIRSTMERIT Bank

ACH Fraud: Bank-Assisted Preventative Measures

- Positive Pay (Electronic Payment Authorization / ACH Filtering)
  - Organization sets limits and thresholds around what companies are authorized to debit the account electronically.
  - Any debit request received outside of these parameters triggers a stop in the processing of the ACH.
  - The Bank notifies the organization that an information mis-match has been identified and requires a pay / no-pay decision on the item.
    - A no-pay decision returns the ACH to the originating financial institution and eliminates the potential loss to the organization
- ACH Debit Block
  - Allows **no** ACH debit transactions to post to the account
    - Ideal for a deposit-only account
  - ACH is immediately returned to originating financial institution as 'Not Authorized'

FIRSTMERIT Bank

Fraud Statistics:

- The Internet Crime Complaint Center (IC3) sent out an alert this week that cybercriminals stole nearly $215 million from businesses between October 2013 and December 2014 through a scam known as the business email compromise (BEC). The scam will sound all too familiar to many corporate treasurers."

AFP Fraudwatch: "Think Twice Before Sending that Wire"
Andrew Deichler
January 30, 2015

FIRSTMERIT Bank

Understanding Wire Fraud & Prevention

- Fraudulent email request to customer or bank.
  - Red flag examples in fraudulent emails to request an outgoing wire include: death in the family; needs immediate attention; urgent business purpose, **improper grammar or punctuation.**
  - Emails often go from management (CEO, CFO) to Accounting staff
- Latest trend: You receive an email request from your supplier, whose email accounts have been hacked. The email asks you to expedite payment to a newly opened US account or just a new bank account. The email contain new wiring instructions.
- Prevention: Token authentication; dual control, dollar limits, call-back procedures.

FIRSTMERIT Bank

Reduce Your Risks of Fraud:

- Convert as many payments as possible to electronic delivery
- Implement Check Positive Pay *and* ACH Positive Pay
- Reconcile accounts throughout the month
  - Use online reporting for faster reconciling
- Place physical controls on check stock
  - Secure storage and access to excess check stock
  - Utilize policies on how check stock is ordered and by whom
- Update bank records immediately after staffing changes
  - New signature cards, delete user ID from online system, etc.
- Screen new employees and temporary help

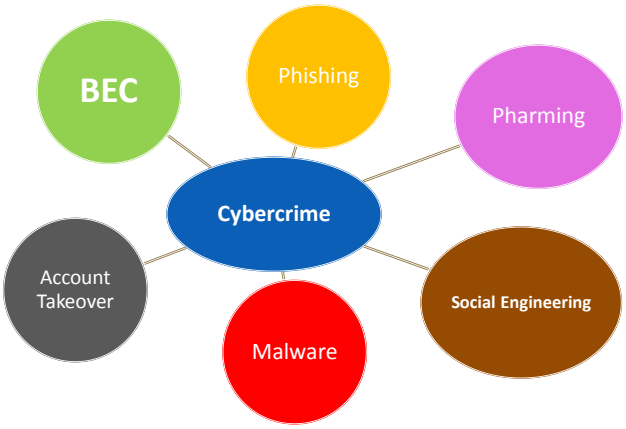
FIRSTMERIT Bank

Reduce Your Risks of Fraud:

- Separate accounts
  - Collection and disbursement activity
  - Check and electronic payments
  - Payroll and accounts payable
- Review and strengthen internal process
  - Awareness and training for employees
  - Document and enforce internal policies and procedures
  - Develop a disaster plan
  - Form an internal anti-fraud committee
  - Segregation of duty and dual authorization
- Know who you do business with
  - Vendors,Clients
  - Employees

FIRSTMERIT Bank

Fraud Happens



FIRSTMERIT Bank

Fraud Schemes: Phishing, Vishing, & SMiShing …

- Phishing Defined
  - An attempt to acquire sensitive, confidential information by masquerading as a trustworthy entity in an electronic communication (e-mail).
    - Most common include AOL, PayPal, eBay, and financial institutions.
    - Victims typically compromise their bank account numbers, credit card numbers, user ID's, and/or passwords.
    - Identity theft or financial loss often results
- Avoid Phishing
  - Be suspicious of *any* e-mail that…
    - Threatens to close or suspend your account if you do not take 'immediate action'
    - States there are unauthorized charges of your account
    - Advises your account has been compromised or there has been third-party activity on the account
    - Requests you to enter your user ID, password, or account numbers into an e-mail or unsecure website

FIRSTMERIT Bank

Fraud Schemes: Phishing, Vishing, & SMiShing …

- Avoid Phishing
  - Do not use links in an e-mail to advance to a website of you suspect the message might not be authentic.
  - Regularly check your online accounts as well as bank and credit card statements.
  - Avoid filling out forms in e-mails that ask for personal financial information
  - Ensure that the web browser you are using is up-to-date and all security patches are applied

FIRSTMERIT Bank

Fraud Schemes: Phishing, Vishing, & SMiShing …

- Vishing Defined
  - Combination of 'voice' and 'phishing'
  - An attempt to acquire sensitive, confidential information over the telephone system, most often using features facilitated by Voice over IP (VoIP).
  - A phishing e-mail can become a vishing opportunity by providing a fraudulent phone number instead of a website address
    - When the victim calls the number, it is answered by automated instructions to enter their credit card number or bank account number on the key pad.
    - Once the consumer enters their credit card number or bank account number, the visher has the information necessary to make fraudulent use of the card or to access the account.
    - The call is often used to harvest additional details such as security PIN, expiration date, date of birth, etc.

FIRSTMERIT Bank

Fraud Schemes: Phishing, Vishing, & SMiShing …?

- SMiShing Defined
  - Phishing via Short Message Service (SMS) text messages
  - Uses cell phone text messages to deliver the 'bait' to get you to divulge your personal information.
    - The text message may be a web site URL; however, it has become more common to see a phone number that connects the victim to an automated voice response system.
    - The smishing message usually contains something that wants your 'immediate attention'.
  - An example of a smishing message in current circulation: "Notice - this is an automated message from (a local financial institution), your ATM card has been suspended. To reactivate call urgent at 866-###-####."

FIRSTMERIT Bank

Fraud Schemes: Phishing, Vishing, & SMiShing …?

- Avoid Vishing and SMiShing
  - Both examples typically convey urgency and often state negative consequences for failing to respond.
  - Messages are not consistent with other phone/text messages
  - Education is your best defense – know what to look for and what to do.
  - REMEMBER… Financial institutions will not send a consumer an e-mail or text message asking to verify or supply account information.
  - If in doubt, call the entity using the known published number (not the number you are given in the e-mail or text) and verify the accuracy of the request.

FIRSTMERIT Bank

Fraud for 2016 … and Beyond:

- Malware Defined
  - 'Malicious Software' designed to infiltrate or damage a computer system without the owner's knowledge or informed consent.
  - Used to obtain confidential information resulting in fraud
  - First appeared in the late 80's / early 90's – still a significant problem
- Types of Malware
  - Adware – displays advertising
  - Spyware – gathers information about you and your Internet habits
  - Keyloggers – records keystrokes and sends to a third party
  - Viruses – dangerous executable files hidden in attachments
- Protect Yourself Against Malware
  - Use anti-virus and anti-spyware software as well as pop-up blocker
  - Require 'Administrator' access to update PC and install software
  - Set rules for Internet usage
  - Turn off CD-ROM drives and USB ports

FIRSTMERIT Bank

Final Thought:

"Punishment for fraud and recovery of stolen funds are so rare,
prevention is the only viable course of action."

- Frank W. Abagnale

FIRSTMERIT Bank