New Faces of Fraud: Tackling today’s biggest threats

April 16, 2019
Agenda

• Cyber Security Overview
  – What we are seeing from the bankers chair
  – Mindset of a Fraudster
  – Trends

• New and evolving threats in the fraud landscape

• Critical strategies your organization needs for fraud protection
The Sobering Reality of Fraud

Financial losses from impostor fraud exceed $1.2B worldwide

Payment Fraud Trends – Up or Down?

Payment Forms Targeted

*Source: The AFP Fraud and Controls Survey, 2018
**Source: The AFP Fraud and Controls Survey, 2017
Traditional Fraud

### Check Fraud
- Checks stolen
- Change payee’s name
- MICR-line used to create fraudulent checks

### ACH Fraud
- MICR-line information stolen from legitimate check
- Sell information to fraud rings
- Fraud rings originate ACH transactions using legitimate account numbers

### Mobile Deposit Fraud
- Involves remote deposit capture via a mobile device
- Same item subsequently negotiated a 2nd time, usually at a branch, retailer, check cashier
- Payee receives funds twice

### Online Account Takeover
- Impersonates a trustworthy entity
- Tricks you into:
  - giving banking credentials
  - installing malware
- Moves funds from your account to theirs

### Controls
- Positive Pay
- Payee Validation
- Timely Account Reconciliation
- Online controls
- ACH Filter to review or stop unauthorized ACH debits
- Return unauthorized ACH debits promptly
- Timely account reconcilement
- Dual custody
- Authorization limits for individual users
- ACH payment templates
- Receivables service to provide “proxy” account numbers for customers
- Encourage the use of direct deposit or prepaid card
- Incorporate into ethics training/agreements
- Include in new hire packet and details
- Monitor accounts/timely reconcilement

### Training
- Training is essential
- Educate employees to recognize phishing and suspicious activity
- Monitor accounts/timely reconcilement
- Protect your email account

### Mobile Deposit
- Mobile Deposit Fraud

### Online
- Online Account Takeover
## Business Email Compromise

- Takes over full access to email account
- Studies email patterns, checks, calendars
- Sends emails from the user’s account undetected
  - will intercept a reply to a hacked email and continue to perpetrate the scheme

- Check for spoofed emails
- Do not open emails from suspicious senders.
- Ongoing training

## Imposter Fraud

- Highly scalable, multiple companies attacked at once
- Not quickly identified, difficult to recover funds; especially if sent by wire
- Authorized users make and authorize payments; payments look normal to Bank

- Verify the Request:
  - Watch for red flags
  - Different methods of verification
  - Only use contact information on file
  - Dual custody
  - Monitor accounts/timely reconcilement
  - Never give login credentials to anyone

## Ransomware

- Ongoing training
- Ensure you are using latest anti-virus and firewall security
- Avoid suspicious emails/links
- Educate employees to recognize phishing and suspicious activities

- Check for spoofed emails
- Do not open emails from suspicious senders.
- Ongoing training

---

Cyber security – Today’s hot topic

• Feedback from customers
• Increase in fraud cases/cyber attempts
• Confusion on cyber security
• Mutual interests
• Risk exposure
• Are you ever truly protected?
News coverage

How Burger King revealed the hackability of voice assistants

Los Angeles college pays $28,000 in ransomware

Majority of workers blindly open email attachments

New Android malware found every 10 seconds
Mindset of a fraudster
Cyber threat landscape
What is account takeover fraud?

A fraudster

→ Tricks you into giving up your online banking credentials.

or

→ Tricks you into installing malware on your device.

Impersonates a trustworthy entity.

 Sends infected attachments or links to infected sites.

 Records on-screen actions, redirects browsers, or displays fake web pages.

 Moves funds from your account to theirs.
Online account takeover fraud - Malware

Malware
Malicious software secretly downloaded onto your device to capture your keystrokes over time in order to gain access to your secure system
Online account takeover fraud - Malware

Email becomes the **weapon of choice** once again.

*1/131 emails* | sent in 2016 were malicious, the highest rate in five years.
Impostor fraud

The fraudster

Poses as a person or entity you know and trust

Contacts you by email, phone, fax, or mail

Requests a payment, submits an invoice, or asks to change vendor payment instructions

If you fall for the scam, any payments you send go to the fraudster — not where you intended.
Checking for a spoofed email by hitting reply

Warning: Do not actually reply. You’d be replying to the fraudster.
Email hacking

The fraudster

• Takes over full access to the email account
• Studies email patterns, checks calendars
• Sends emails from the user’s account undetected
  – Will intercept a reply to a hacked email and continue to perpetrate the scheme
Fraud Case 1 – Email hacking (Executive Imposter Fraud)

- Large Retailer
  - Internal request for $280K wire to pay vendor in China from CFO’s email account

- Wire initiated – Dual custody approved
  - Payments to China are common within the organization

- Result - $280K Loss
Fraudsters are willing and ready to interact with you. They anticipate that you may question the request.

They’re prepared to respond to your follow-up emails and phone calls.
Executives make perfect targets to impersonate

- Always on the move
- At the top of the approval hierarchy
- May occasionally request ad hoc payments
- Can be very demanding
- Business needs trump accounting rules
Vendors also impersonated

Companies often have many vendor relationships

Correspondence with vendors is typically conducted via email

Vendors often supply new account numbers
Fraud Case 2 – Vendor imposter fraud

- Large public school district
  - Heavy on email communication with vendors

- Contacted by large vendor – Food supplier
  - Requested change of entity name
  - Change of account details for payment

- Result - $2.8MM Loss (Still being recovered)
Fraud Case 3 – Payroll fraud

• University
  – Payroll System hacked

• Contacted all employees by email
  – Requested validation of payroll account information
  – Captured keystrokes to access profiles
  – Changed account information

• Result - $10K Loss (Unrecovered)
Best practices for fighting fraud
Fight this fraud with a multipronged approach

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Computer icon" /></td>
<td>Don’t trust email</td>
</tr>
<tr>
<td><img src="image" alt="Phone icon" /></td>
<td>Verify phone instructions</td>
</tr>
<tr>
<td><img src="image" alt="Network icon" /></td>
<td>Add multiple layers of control and separation</td>
</tr>
<tr>
<td><img src="image" alt="Bank icon" /></td>
<td>Eliminate bank account information from your payment system</td>
</tr>
</tbody>
</table>
Educate your staff, vendors, and partners about potential threats.

Never give out your online banking credentials.

Review policies, procedures, and controls.

Monitor accounts daily and use notification and alert services.

Be wary of token prompts that appear at sign-on. Disregard onscreen messages requesting immediate action.
Taking charge: how you can fight fraud

Make contingency plans.

Engage your banks.

Get to know your cyber security group.

Don't click links, open any attachments, or install programs from unknown senders. Update antivirus programs.
For payments, especially ...

Pay close attention to details.

Implement dual custody and ensure both users are on different devices.

Generate financial transactions from a stand-alone PC with email and web browsing disabled.

Empower staff to question any unusual payment requests.

Authenticate all requests:
- Verify by a channel other than that through which the request was received.
- Use official contact information on file to verify; never use contact information provided in the request.
Know your organization’s critical needs

• One size does not fit all: integrate your security measures to reflect your organization’s priorities

• Have an actionable plan in place to respond in case of a fraud attack
## Managing the risks

<table>
<thead>
<tr>
<th>Education</th>
<th>Awareness of exposure of “internal” data</th>
<th>Handheld devices</th>
<th>BYOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit data maintained or made available</td>
<td>Encrypting laptops, smartphones, etc.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mock breaches – aka “tabletop exercises”</td>
<td>Limit online access to data storage servers</td>
<td>Policies not enough</td>
<td>Destruction of hard drives to remove all PII</td>
</tr>
</tbody>
</table>
Watch for red flags— if something seems wrong ... it probably is