Cyber payments fraud

December 2019
Online Payments fraud agenda

- New and evolving threats in the fraud landscape
- Critical strategies your organization needs for fraud protection
- Call to Action
- Education essentials
Payment fraud trends

- 82% of Organizations experienced attempted or actual fraud
- 80% of companies reported BEC fraud
- 52% of the companies targeted by BEC experienced a financial loss as a result

$26.2 Billion dollars lost to BEC fraud

Sources: The 2019 AFP Payments Fraud Controls Report and The Federal Bureau of Investigation, Internet Crime Compliance Center (IC3)
Trends by payment type

Source: 2019 AFP Payments Fraud Controls Report
**Positive Pay effectiveness**

- Counterfeit continues to be the leading type of check fraud.
- Positive pay is highly effective at stopping counterfeits, but when isn’t it as effective?
  - Internal embezzlement
  - Forged endorsement
  - Ineffective use of the positive pay service
- Positive pay alone will not prevent payee alteration fraud
  - Original check with altered payee
  - Counterfeit check matches legitimate item but has a different payee

![Positive pay effectiveness](image)

99.4% effective*

* Wells Fargo metric
- Criminals get MICR-line information from a legitimate check
- Sell information to fraud rings
- Fraud rings originate ACH transactions using legitimate account numbers
New threats in the world of fraud

**Attack spanning large to small organizations**
- Real estate and higher education industries
- Smaller organizations, fewer controls and security measures

---

**Mobile banking on the rise: Increased risk for carelessness or speed**

- Mobile malware
- Social engineering
- Unauthorized apps
- Fraudulent apps
- Lost Devices

Source: FBI PSA dated 4 May 2017, Alert # I-050417-PSA
# Mobility and technology best practices

## Follow entity policies
- Education and monitoring
- Ensure controls with vendors

## Apps from trusted sites
- Known providers only
- Download from appropriate stores
- Be aware of unsecure sites

## Keep devices up to date
- Use latest software versions
- Stay informed on trends, issues, gaps

## Be aware of open networks
- Limit public WIFI or high-risk actions
- Use caution using shared, public machines

## Protect devices
- Use strong passwords and/or biometrics
- Guard against theft
- Be aware of confidential info on device

To protect your organization, be aware of these threats.
The biggest threat for 2019 and beyond?

**Sophisticated fraudsters + Time and patience = Significant losses**

- Imposter Fraud attempts always appear legitimate at first
- Fraudsters time attacks for vulnerable organization transitions
- Keep good data and records
Steps to protect against impostor fraud

1. **Verify The Request.**
   If you receive a request from a vendor or executive to change payment details such as account or invoice information, always make sure the request is authentic.
   - **Watch For Red Flags.** If a request seems out of the ordinary, follow up with the requestor, especially if the request is made electronically.
   - **Verbally Verify.** Do not respond directly to the request. Verbally confirm the payment or payment instruction change.
   - **Only Use The Contact Information On File.** Never use the information provided in the request, as it may also be fraudulent.

2. **Implement dual custody.**
   Dual custody requires two users on different devices to initiate and approve online payments, payment instruction changes and administrative changes. This serves as a second chance to spot a fraudulent payment before it goes out the door.
   - **Verify Payment Changes With Requestor Before Initiating A Request.** Pay close attention to the payment details, and note any changes from the information you have on file.
   - **Confirm Any Changes Have Been Verified Before Approving A Payment.** The approver must verify the payment and payment instructions.

3. **Monitor Accounts.**
   - **Reconcile Bank Accounts Daily.** Because impostor fraud may go unnoticed for up to 30 days, it’s important to pay close attention to your account activity.
   - **Protect Your Email Account.** Never give your login credentials to anyone you don’t know, especially online or over the phone.
What is Account Takeover fraud?

- Account Takeover fraud is when the fraudster steals your confidential information to access your online accounts directly.

- The fraudster typically leverages Social Engineering and Malware to execute an account takeover incident.
  - **Social Engineering**, such as **Phishing**, manipulates you into divulging confidential information.
  - **Malware** is malicious software installed on your computer without your consent or knowledge.

- Once malware is installed on your computer, a fraudster will access accounts and send unauthorized payments.
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
- Simple processes can be some of your most powerful protection.
Best Practices

**Verbally Authenticate** all requests for payment or account change requests
- Use contact information on file to verify; never use contact information provided in the request

**Vendor/Trading partner awareness**
- Educate your vendors and trading partners - they are targets for fraud, too
- Define a process for them to communicate payment and account changes

**Educate your entire staff**
- Alert management and supply chain personnel to the threat
- Instruct all staff, especially AP staff, to question unusual payment or account requests received by email — even from executives
- Review processes and retrain your employees
As soon as possible, meet with your:

- **AP staff** and internal partners. Any group could be an entry point for a fraudster.
- **Executives** - Make them aware of the threat and ask them to support necessary changes to mitigate risk.
- **Peers** - Contact them to help spread the word.
- **Treasury Management partners** - Learn more about fraud protection services.

If you suspect fraud, **immediately** contact your bank.
Fraud websites for additional fraud assets

- Treasury Insights Fraud & Security page
- Wellsfargo.com fraud page
  - [https://www.wellsfargo.com/com/fraud](https://www.wellsfargo.com/com/fraud)

Fraud checklists

- 3 steps to combat impostor fraud checklist
- Triumph over account takeover checklist
  - [https://digital.wf.com/treasuryinsights/portfolio-items/tm3167/](https://digital.wf.com/treasuryinsights/portfolio-items/tm3167/)

Note: to use the links, highlight the link, right click and select “Open Hyperlink” – if reading hard copy, enter the https address on your browser.
Contact your respective financial institution for additional information.

Or

Email us at
treasury solutions@wellsfargo.com
Thank you