
WELLS
FARGO
Facing the new faces of fraud
Tackling today's biggest security threats

Today’s agenda

- New and evolving threats in the fraud landscape
- Critical strategies your organization needs for fraud protection

The sobering reality of fraud

of companies were victims of payments fraud in 2017

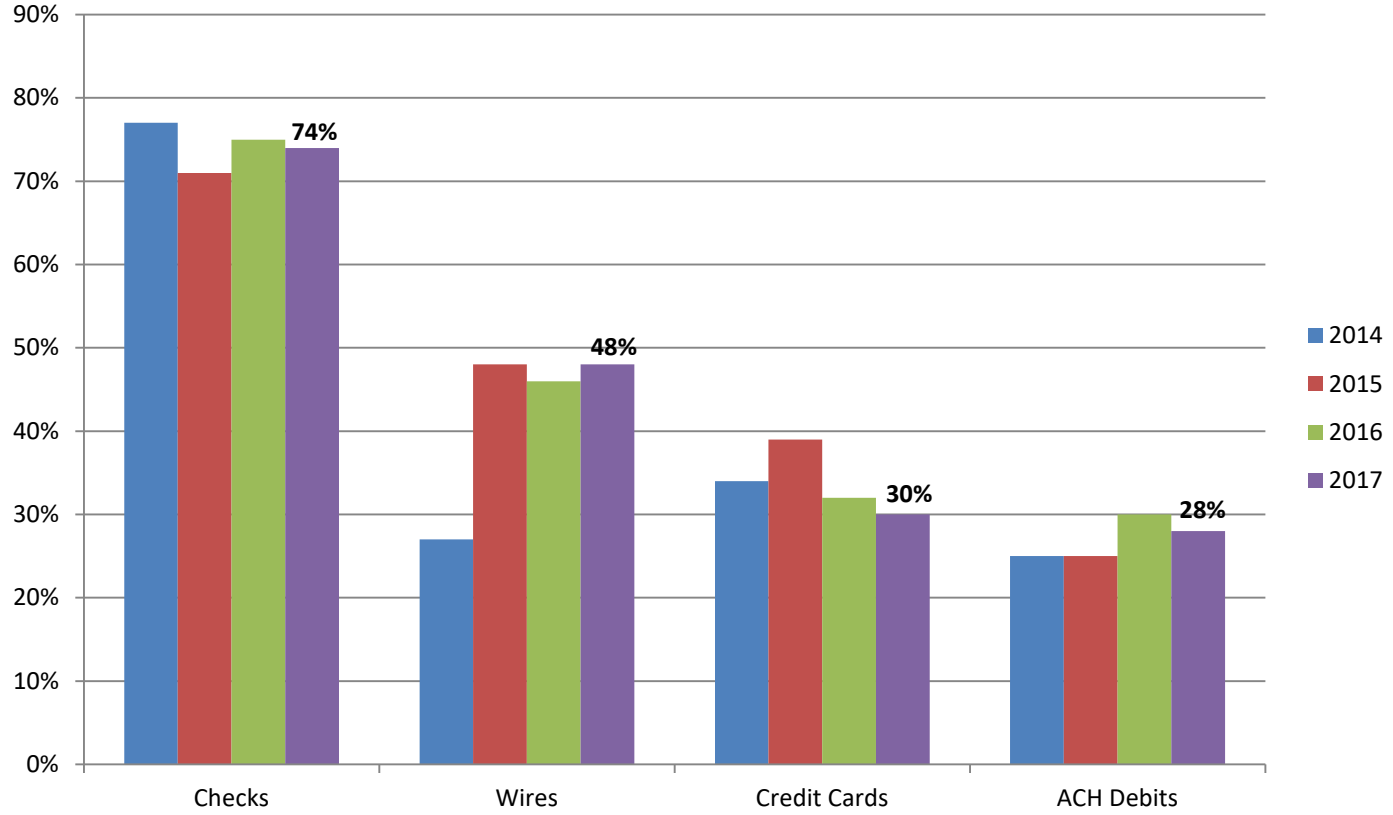
of companies were exposed to business email (BEC) compromise scams

of companies were victims of BEC fraud via wire transfers

Financial losses from BEC fraud exceed $5.3B worldwide

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

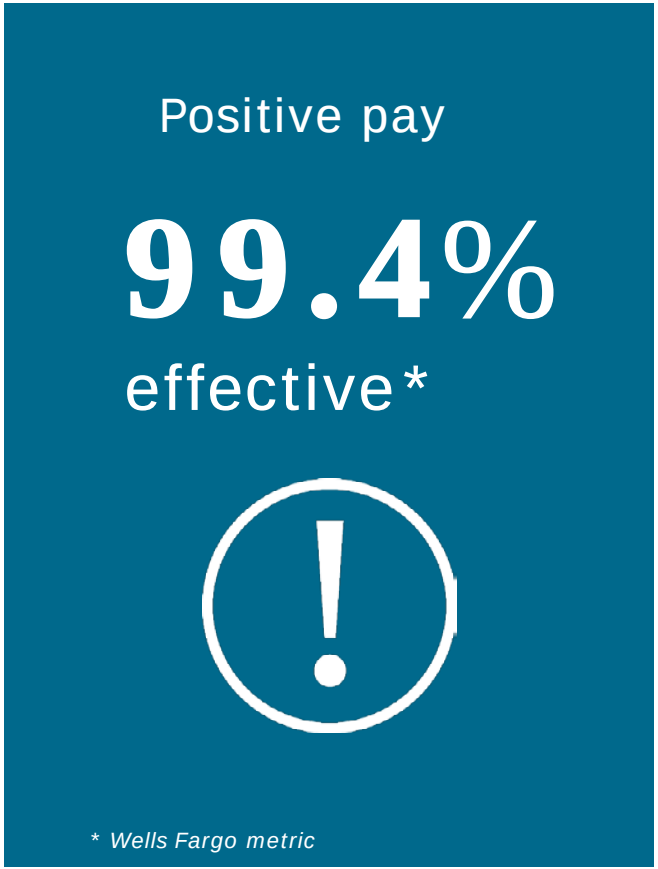
Trends by payment type



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

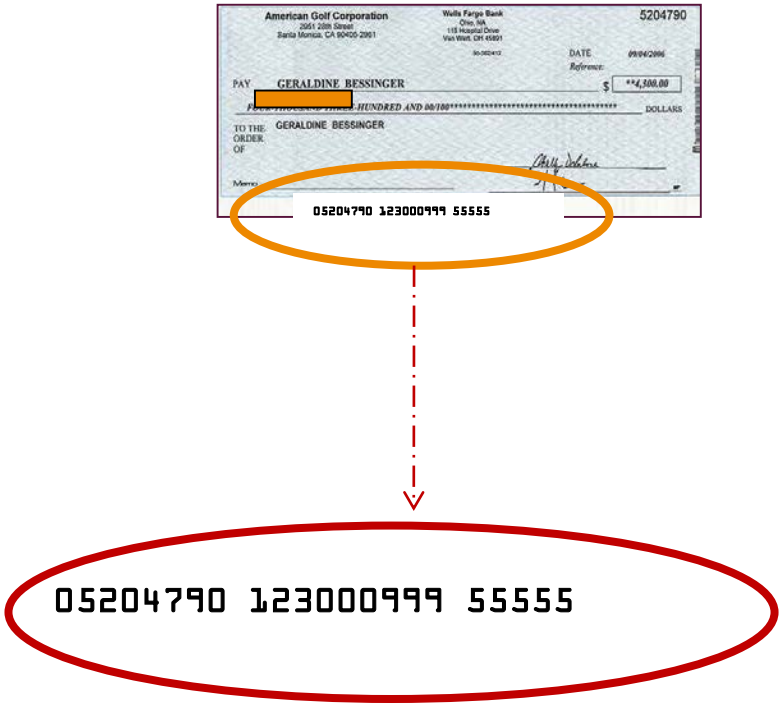
Positive pay effectiveness

- 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



ACH Debit Fraud

- 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

Attacks spanning large to small organizations

Real estate and higher education industries

Smaller organizations, fewer controls and security measures

Source: FBI PSA dated 4 May 2017, Alert # I-050417-PSA

New threats in the world of fraud

Mobile banking on the rise:

Increased risk for carelessness or speed

Mobile security threats

Mobile malware

Social engineering

Unauthorized apps

Fraudulent apps

Lost Devices

To protect your organization, be aware of these threats.

Mobility and technology best practices

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

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

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

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

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

Fraud attacks: the schemes that stand out

But the biggest threat for 2018 and beyond?

Business email compromise

Sophisticated fraudsters +

Time and patience =

Significant losses

When impostor fraud strikes

- Impostor fraud attempts always appear legitimate at first
- Fraudsters time attacks for vulnerable organization transitions
- Keep good data and records

3 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.

☑ **Verify Using A Different Method.** Do not respond directly to the request. For example, if a vendor contacts you by email, confirm by phone.

☑ **Only Use The Contact Information On File.**
Never use the information provided in the request, as it may also be fraudulent.

3 steps to protect against impostor fraud

2. Implement dual custody.

Dual custody requires two users on different computers or mobile devices to initiate and approve online payments 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.

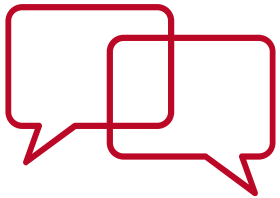
☑ **Confirm Any Changes Have Been Verified Before Approving A Payment.** Do not assume the initiator has verified the requested changes and examined the payment details thoroughly.

3 steps to protect against impostor fraud

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.



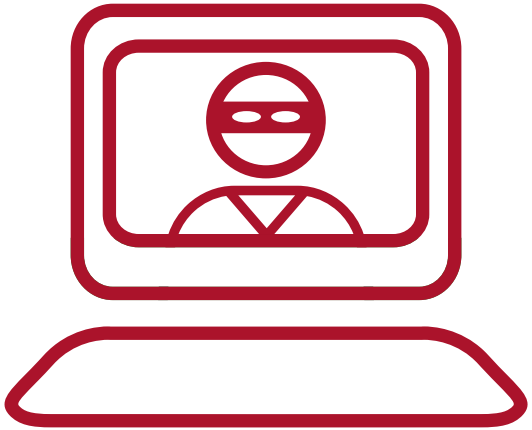
If you suspect fraud, contact your banker or relationship manager immediately.

"The amount we lost from impostor fraud was nearly the same as our annual earnings."

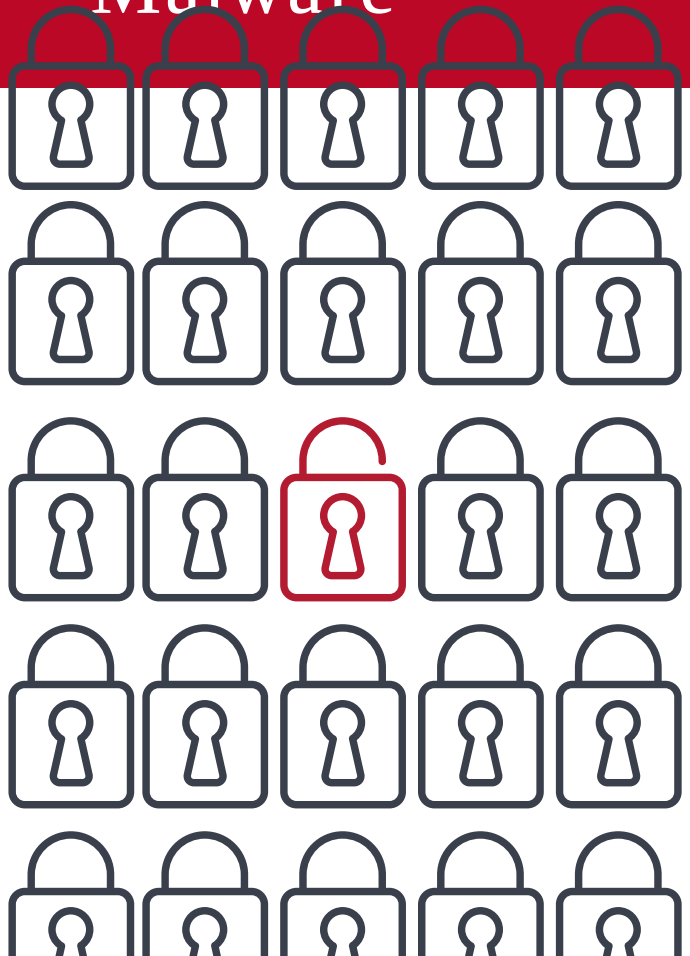
Anonymous customer

Account takeover fraud

- Fraudsters use your online credentials to gain access to your email system, “taking over” as you to make and authorize payments.
- Commonly happens through malware, a form of social engineering.



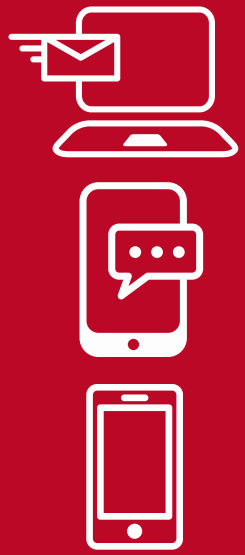
Malware



Malicious software secretly downloaded onto your device to capture your keystrokes over time in order to gain access to your secure system

Social engineering

Tools fraudsters use to target fraud attempts



Phishing / Spear Phishing: false emails appearing to be from trustworthy sources sent to gain confidential information or download malware

Smishing: fraudulent texts to download malware on a mobile device or try to trick the recipient into giving up secure information

Vishing: fraudster uses phone to make contact

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

Taking charge: How your organization can fight fraud

Simple processes can be some of your most powerful protection.

Best Practices

Authenticate all requests

- Verify all requests – payment or account change 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

Educate your executives and staff

- Alert management and supply chain personnel to the threat of vendor and executive impostor fraud
- Instruct all staff, especially AP staff, to question unusual payment or account requests received by email — even from executives

Vendor/Trading partner awareness

- **Educate** - They are targets for fraud, too
- **Instruct** – Define a process for them to communicate payment and account changes and how those changes must be verified by you
- **Review/Train** - your employees responsible for vendor management and payment processing on the use of the process

Ransomware

What is it:

- Looks for vulnerabilities in technologies
- Usually requires Cyber currency ransom
- Can lock down one pc or entire organization’s networks

What can the bank do for you:

- Help with payments that need to go out
- Throttle user and entity payment limits
- User management
- Cannot advise on the actual incident

Call to Action

Help increase awareness of fraud

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

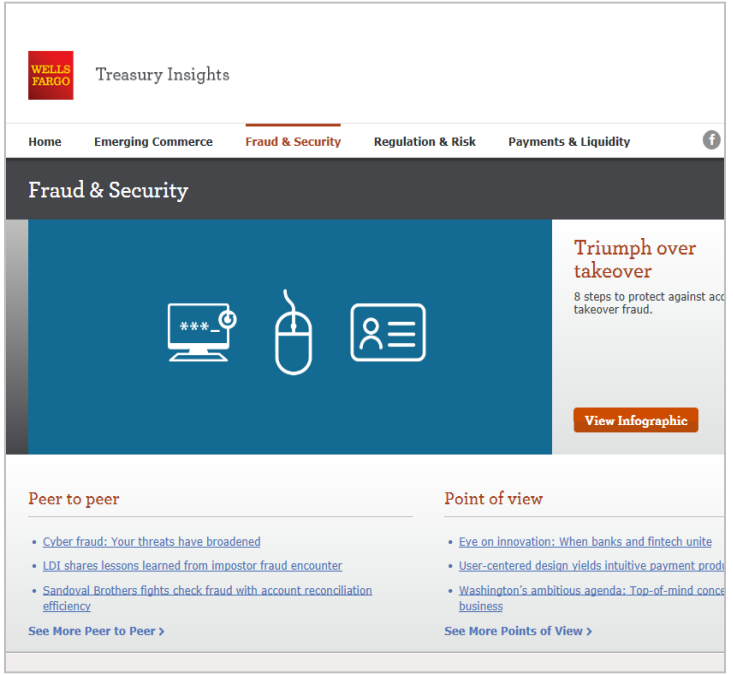
Resources for more fraud protection information

Fraud websites for additional fraud assets

- Treasury Insights Fraud & Security page
  - https://digital.wf.com/treasuryinsights/fraud-security/)
- Wellsfargo.com fraud page
  - https://www.wellsfargo.com/com/fraud

Fraud checklists

- 3 steps to combat impostor fraud checklist
  - https://digital.wf.com/treasuryinsights/portfolio-items/tm3162/
- Triumph over account takeover checklist
  - https://digital.wf.com/treasuryinsights/portfolio-items/tm3167/



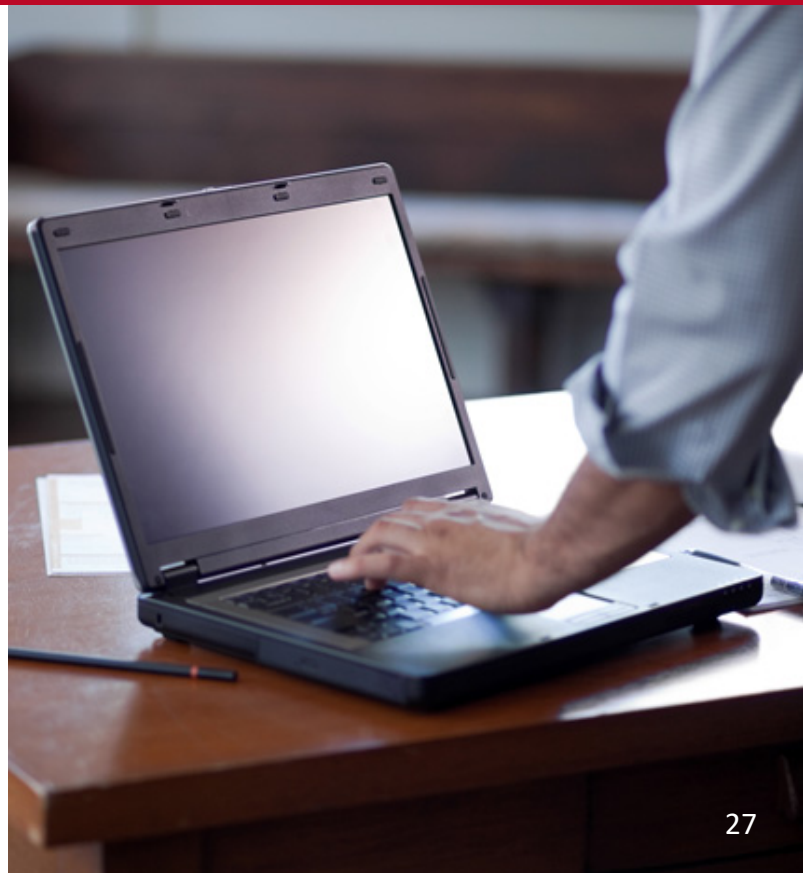
Note: to use the links, highlight the link, right click and select "Open Hyperlink" – if reading hard copy, enter the https address on your browser.

For questions and comments

Contact your respective financial institution for additional information.

Or

Email us at TreasurySolutions@wellsfargo.com




Thank you!
WELLS FARGO
&
CO.