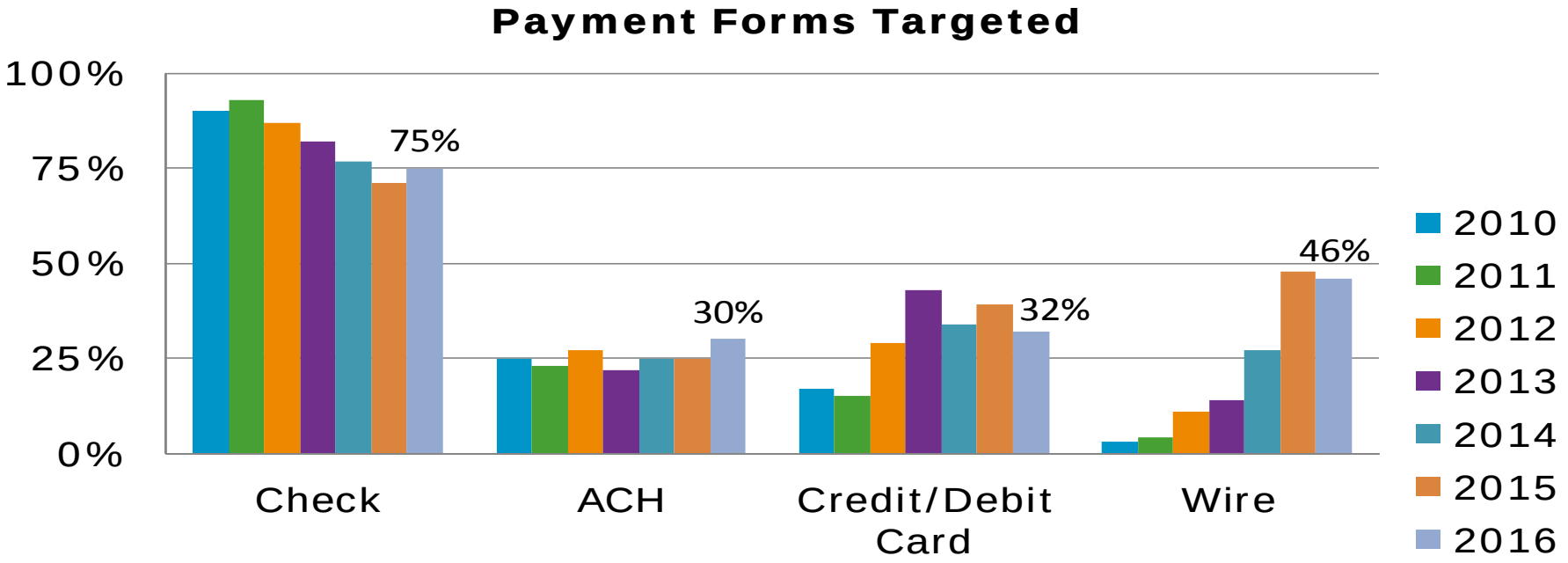
Fraud Protection in the Cyber Age

Mark D. Haggen

SVP – Treasury Management Consultant

June 8, 2017

Payment fraud trends



Source: *2017 AFP Payments Fraud and Control Survey*

Wire / ACH fraud (aka Imposter fraud)

The fraudster

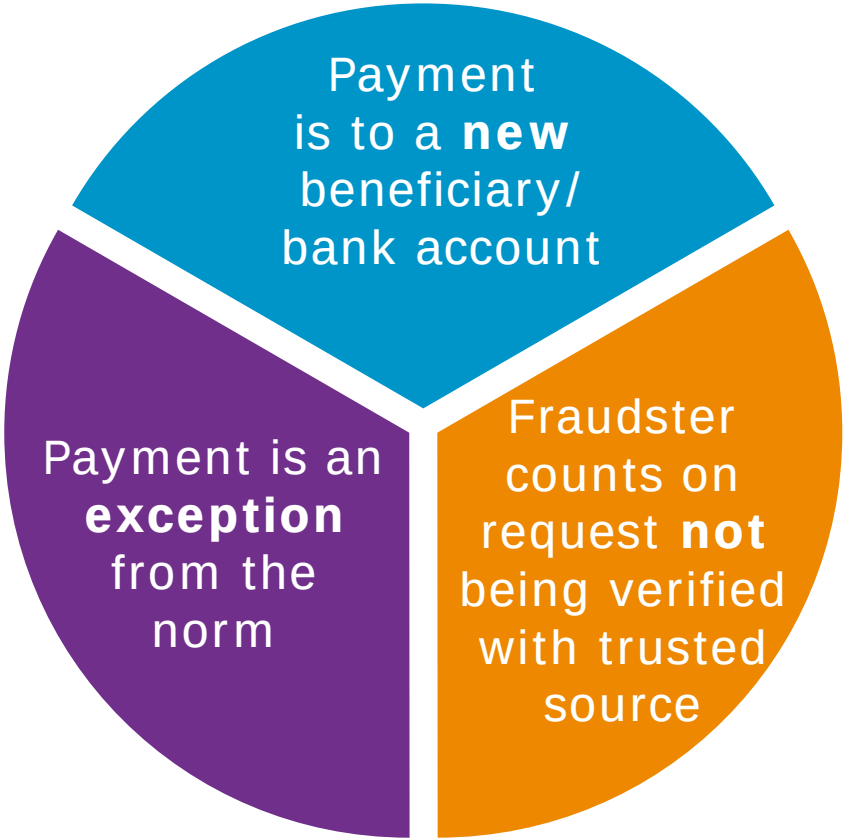
Poses as a person or entity you know and trust

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.

Impostor fraud — common denominators



Authenticate all requests

- Verify electronic or unusual 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 requests received by email — even from executives

Alert vendors and partners

- Warn vendors that they are targets for fraud, too
- Tell vendors you no longer accept changes to bank account information by email
- Instruct your trading partners not to change their remittance information without verifying the request with you

Online account takeover fraud

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.

Ransomware: A rapidly growing threat

Best practices to reduce your risk

- **Keep your antivirus software** and operating systems up to date
- **Back up critical data regularly** — and store that data offline
- **Do not select links in emails or text messages**, download attachments, or install programs, unless you're certain they're from trusted senders
- **Never sign on to your banking portal with a direct link** in an email or text message. Instead, go directly to the sign-on page

In 2015, there were 2,453 reported ransomware incidents in which victims paid $24.1 million total.[1]

1 Devlin Barrett, "FBI Says Threat From 'Ransomware' Is Expected to Grow," The Wall Street Journal, March 10, 2016.

Best practices

Ways you can protect your business

Never give out your online banking credentials.

Monitor accounts daily and use notification and alert services.

Be wary of token prompts that appear at sign-on. Disregard on-screen messages requesting immediate action.

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

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

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

If something doesn't seem right,
it probably isn't.

Electronic Payment Fraud is on the rise.....

74%
of organizations experienced attempted or actual payments fraud

74%
reported they have been exposed to BEC impostor fraud

46%
were exposed to wire fraud — a significant increase from the previous survey

30%
reported ACH debit fraud which is higher than previous years' could indicate new type of fraud

Source: *2017 AFP Payments Fraud and Control Survey*

Positive pay for fraud prevention

Positive Pay
The best way to prevent check fraud

- Compares incoming checks with check issue information provided by the customer
- Checks that don’t match are shown to the customer for decision (exceptions)
- Customer makes return or pay decision
- Unauthorized checks are returned

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

Internal embezzlement

How you can protect your entity from wire fraud

Require more than one approver for wires

Restrict Freeform Wire and Template Maintenance user entitlement to only those individuals with a real business need

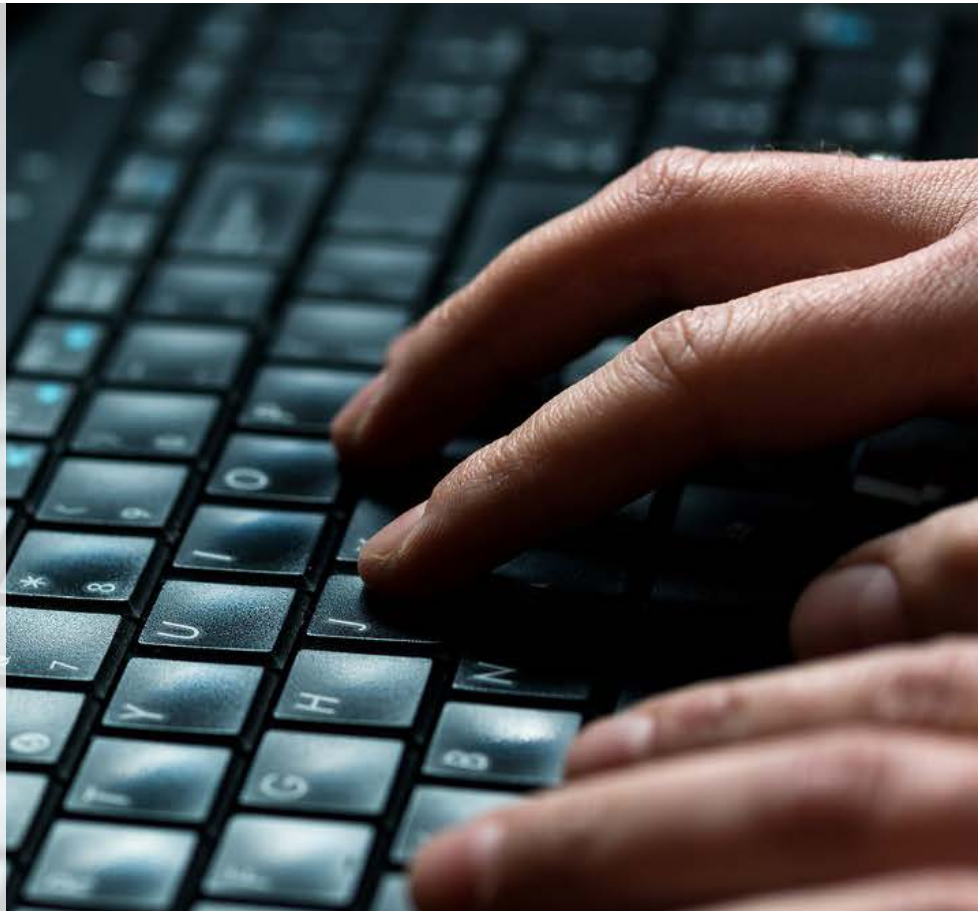
Perform credit and background checks on all new employees who have access to wires

Regularly review/audit user entitlements

Email take over

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

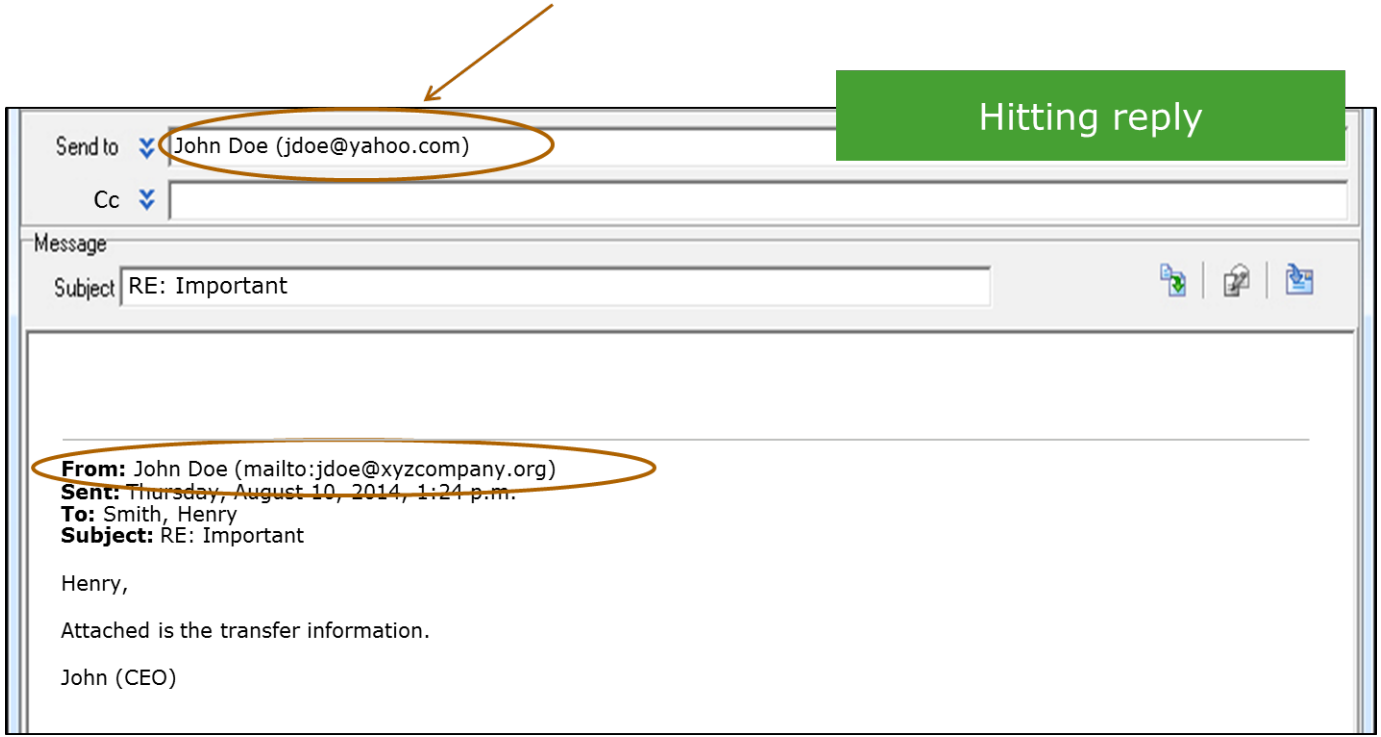


1 in 220

Email malware rate

Source: Symantec, *Internet Security Threat Report*, Volume 21, April 2016

Checking for a spoofed email by hitting reply



Warning: Do not actually reply. You'd be replying to the fraudster.

Vendors also impersonated

Companies often have many vendor relationships

Correspondence with vendors is typically conducted via email

Vendors often supply new account numbers

Mobile deposit fraud with duplicate presentment – what is it?

This type of check fraud involves remote deposit capture via a mobile device (smartphone, tablet, etc.).

The same item is subsequently negotiated a second time, usually at a bank branch, retailer, or check casher.

The payee receives funds twice for the same item.

Mobile deposit fraud trends

- Many mobile deposits with duplicate presentments are “honest mistakes.”
- However, the increase in mobile deposit use has created new opportunities for fraudsters.
  - Bank losses related to remote and mobile deposit capture are increasing.
  - Losses and impacts are also increasing for business customers.

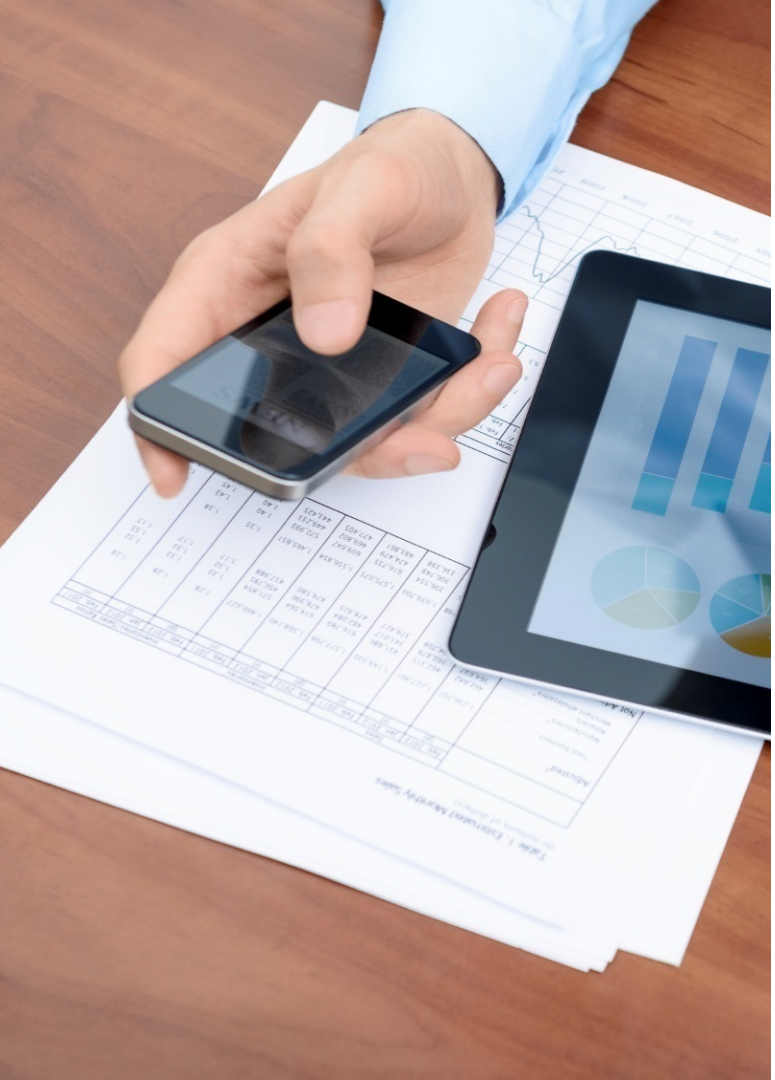
1 in **7**

Americans have deposited a check using a mobile device within the past year

Survey conducted for ABA by Ipsos Public Affairs, July 8–13, 2015.

Cases for mobile deposit fraud **more** than **doubled** from 2013 to 2015

Source: Wells Fargo wholesale check fraud cases



Additional safeguards to protect your accounts

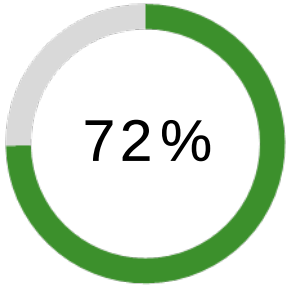
- Monitor accounts regularly
- Protect log-on information and lock your mobile device
- Don’t follow untrusted links in emails or messages, and report suspicious emails or messages
- Delete text messages from your financial institution
- If you lose your smartphone or change your number, remove your old number from your online banking profile

43%

Workers who use a smartphone at least once per week for work-related activities. **20%** use a tablet device.

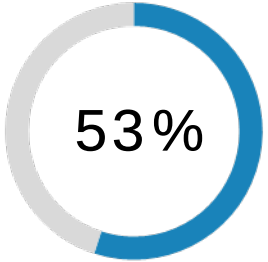
Source: Forrester

Key mobile security concerns



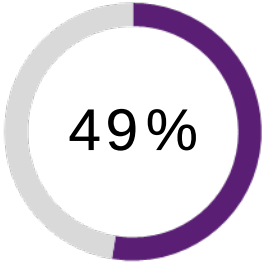
Device security

Are mobile transactions secure?



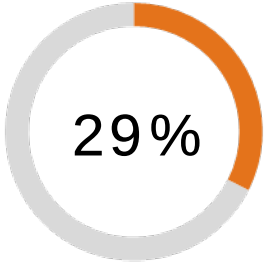
Lost phones

Potential exposure of information if phone is lost



Carrier security

Overall security of transmitting data over cell networks



Access process

Are the methods for authentication and access secure?

Source: *2017 AFP Payments Fraud and Control Survey*

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

Thank you