

Cyber security:
What your treasury division should know
Addressing Fraud in Electronic Payments

Presented by: Mike Crossley

Learning Objectives

At the end of this session, you will be able to

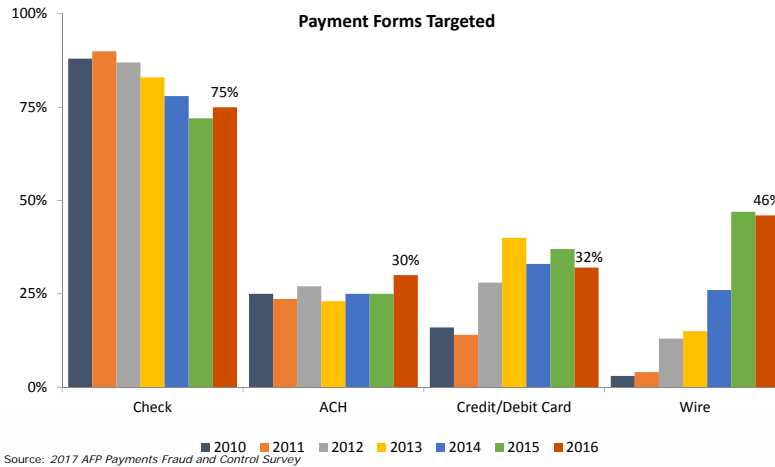
- Discuss some of the latest schemes and methods seen in electronic payment fraud
- Recall tactics available to local governments to mitigate electronic payment fraud

Agenda

- Fraud trends
- Online account takeover fraud
- Impostor fraud
- Call to action

WannaCry.....?

Payment fraud trends



5

Poll #1

How prepared do you think your organization is to thwart potential cyber fraud attacks?

- A. Very prepared
- B. Somewhat prepared
- C. Not prepared
- D. Not sure



6

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

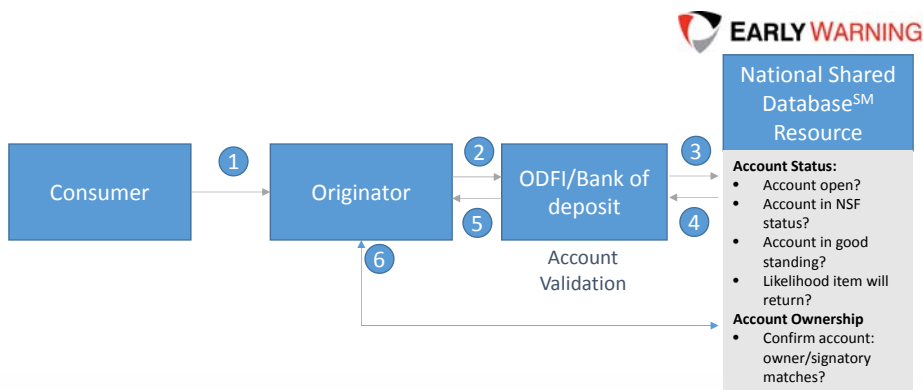
Market Landscape

Situation	Check fraud is still prevalent Electronic payment fraud rising New techniques emerge constantly
Need	More education Better Technology Faster information sharing
Impact	Constituents expect more prevention Greater focus on risk management More Tool Development

Who are you? – The next frontier is here

- ▶ Validate — in real time — the person or business that owns the deposit account (account openings or wire transfers)
- ▶ Reduce the number of unauthorized transactions
- ▶ Decrease ACH NSF and administrative ACH returns
- ▶ Make it easier for your customers to pay using the ACH system

How Account Validation services works



Account Validation services

Account Status	Account Ownership
<p>Confirm a deposit account (checking or savings) is open/valid and see if there's a risk of returning ACH or check transactions</p>	<p>Confirm your payee has authority to transact on the account</p>

Use cases for Account Validation services

Receivables	Payables
ACH	
<ul style="list-style-type: none"> ▪ Collections of taxes, fines, levies or other fees ▪ Child support ▪ ACH enrollment ▪ Recurring payments ▪ One-time payments ▪ Established constituent updating banking information 	<ul style="list-style-type: none"> ▪ Tax refunds ▪ Vendor/supplier payments ▪ Court-ordered funds distribution ▪ College savings plan (529) disbursements ▪ Retirement benefits ▪ Customer support payments
Check	
<ul style="list-style-type: none"> ▪ DMV fees ▪ Permit and license fees ▪ Court fines and payments ▪ Risk screening check payments 	
Wires	
<ul style="list-style-type: none"> ▪ Vendor/supplier payments ▪ Retirement benefits 	

Account Validation services

The value of community and collaboration

Provide broader visibility

Deliver actionable intelligence

Reduce fraud, manage risk, comply with industry rules & regs

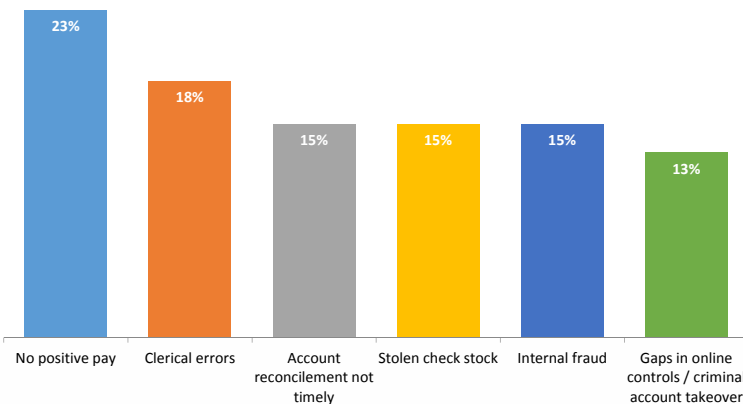
Provide greater insight so you can better serve your customers



13

Reasons for check fraud losses

Organizations incurred financial loss due to check fraud for various reasons:



Source: 2017 AFP Payments Fraud and Control Survey



14

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



Source: 2016 AFP Payments Fraud and Control Survey | Source: 2017 AFP Payments Fraud and Control Survey



The basics

How you can protect your entity from check fraud

- | | | | |
|--|---|---|--|
| <ul style="list-style-type: none"> • Use positive pay and payee validation services | <ul style="list-style-type: none"> • Monitor and reconcile accounts and invoices daily • Secure check stock | <ul style="list-style-type: none"> • Know your employees and vendors | <ul style="list-style-type: none"> • Conduct audits and/or rotate assignments |
| <ul style="list-style-type: none"> • Implement segregation of duties – and use it properly • Separation of check writing, positive pay decisions, and reconciliation functions • Dual control for sending check issue information to the bank | <ul style="list-style-type: none"> • Ensure authorized signers on bank accounts are kept up to date | <ul style="list-style-type: none"> • Code of conduct • Hotline for tips • Fraud training | |



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

Positive Pay
99.4%
effective

* Wells Fargo metric

Forged endorsement

How you can protect your entity

Ensure that controls are in place to prevent tampering with vendor information, including addresses

Reconcile vendor statements and invoices timely

Outsource check printing to a reliable vendor

Know that endorsement fraud is often not detected until a payee reports not receiving funds

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



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 link to infected sites.

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

Moves funds from your account to theirs.

Today's financial industry security threat landscape

Increased targeting of informational assets for monetary gain

Evolved ecosystem

- Business growth drives more systems in the environment
 - Massive complexity and asset intimacy
 - Harder to understand all technical risks
- Requires more complex application / system development
- Attack surface has expanded significantly (mobile, wireless, cloud)

Adds to defense in depth

Today's financial industry security threat landscape

Increased targeting of informational assets for monetary gain

External threat landscape

- More attackers, characterized as:
 - Sophisticated
 - Better resourced than their targets
 - Engaging in monetized-incented attacks
 - Targeting security controls (e.g., tokens)
- Targets no longer limited to certain industry sectors
- Emergence of social engineering

Shifting threat landscape

How online accounts can be compromised

- Phishing
 - Most attacks by email, convince victim to click link
 - Link looks authentic but injects malware
 - Victim's credentials stolen
- Fake mobile banking apps
 - Users tricked into downloading app
 - Credentials harvested and sent to fake app author
- Malware/Remote Access Trojans (RATs)
 - Remote admin capabilities provided, allow threat actor to control victim's computer

Five tips to protect yourself and your company

- 1 Create strong passwords
- 2 Avoid suspicious links
- 3 Limit personal information online
- 4 Stay current on updates and patches
- 5 Safeguard your devices

Poll #2

How often are your employees trained on cyber fraud security?

- A. Regularly
- B. Occasionally
- C. Not at all

Social engineering strategies

Classic phishing

Email messages sent to large populations designed to obtain confidential information
Emails purport to be from trustworthy sources with which victims have established relationships

Vishing and smishing

Vishing is where fraudsters connect with their victims via phone
Smishing is when a fraudulent text message is sent to the victim

Spear-phishing

Targeted phishing attack directed at a small group of potential victims
Emails are focused, have a high degree of believability and a high open rate

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

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

Phishing successes explained

Cybercriminal excellence

- Accurate logos, professionally written communications, personalization of content increase believability
- Targets are more likely to click on the links and/or open attachments, which download malware

Social media explosion

- Users are sharing an alarmingly amount of information through social media platforms
- Provides criminals with the fodder necessary to construct personalized and believable messages

Credulous users

- Users are the first line of defense, yet organizations do not have robust training programs to heighten users' sensitivity to phishing attempts

Bottom Line: Phishing attempts are becoming more challenging and more difficult to address

1 in 244

Email malware rate

Source: Symantec Internet Security Threat Report, Volume 20, April 2015

Malware improvements



Malware has evolved to where it can now:

- Detect a sandbox and will not execute its code until deemed 'safe'
- Remain dormant for an extended period in order to evade traditional anti-malware solutions
- Operate another malware that appears to be innocuous
- Require user interaction, such as clicking on a button in a dialog box, before it goes into action

Online account takeover fraud

How does Wells Fargo work to protect your business?

Protection



- Multi-layered approach
- Safeguarding credentials
- Product security
- Fraud protection services

- Advanced detection technology
- Unusual activity monitoring
- Transaction risk evaluation
- Industry partnerships/
- law enforcement coordination

Detection



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.

Impostor fraud

The fraudster

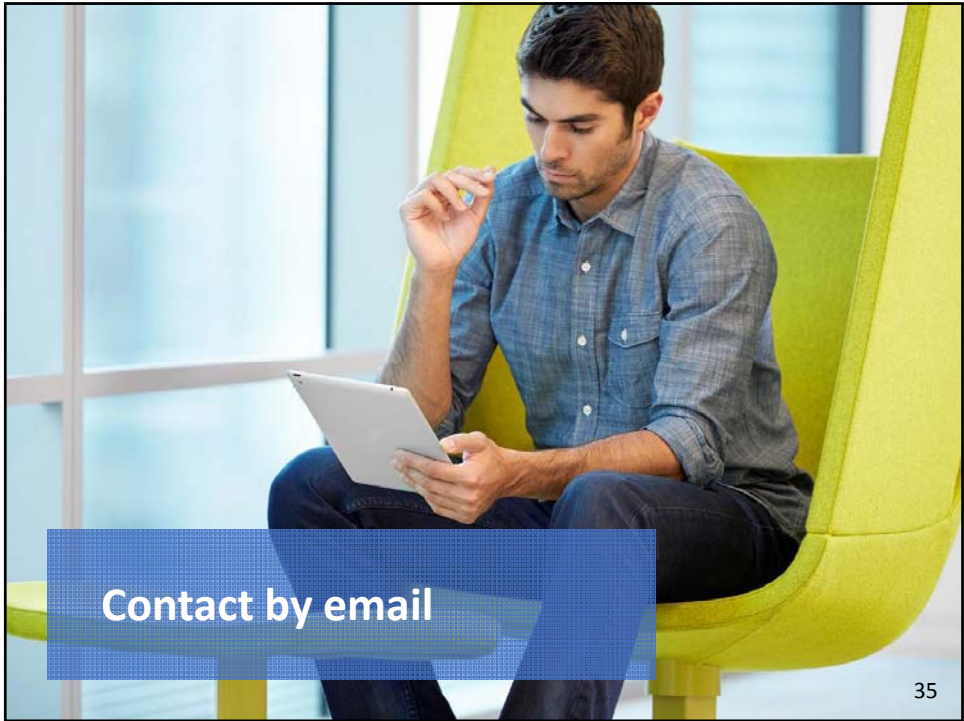
Poses as a person or entity you know and trust

Contacts you by email, phone, fax, or mail

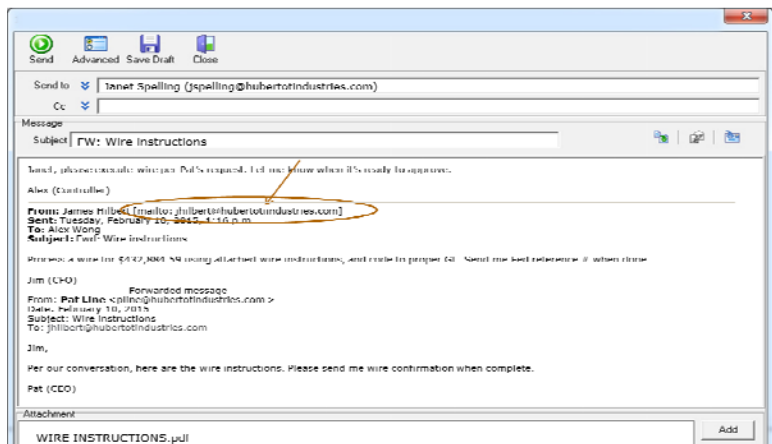
Requests a payment, submits an invoice, or asks to change vendor payment instructions



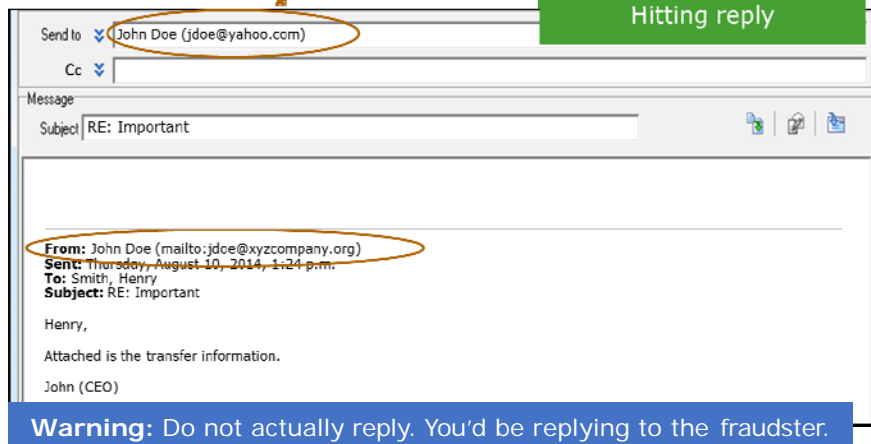
If you fall for the scam, any payments you send go to the fraudster — not where you intended.



Example of executive email spoofing



Checking for a spoofed email by hitting reply



Email hacking

The fraudster

- Takes over full access to the email account
- Studies email patterns, check calendars
- Sends emails from the user's account **undetected**
- — Will intercept a reply to a hacked email and continue to perpetrate the scheme



Impostor fraud is different

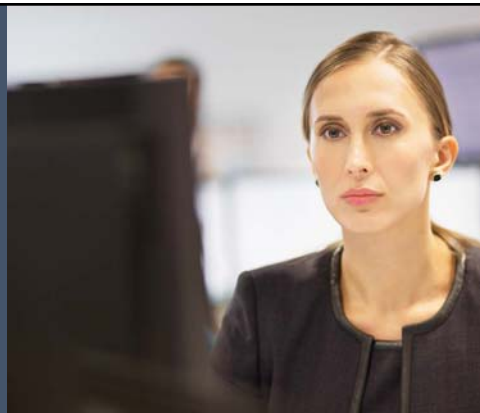
It's highly scalable — multiple companies attacked at once

It's not quickly identified — and it's hard to recover funds, especially if sent by wire

Fraudsters don't steal online banking credentials and make payments (like in account takeover fraud)

Instead, your authorized users make and authorize payments. Payments look normal to your bank.

And the biggest difference is ...



Fraudsters are willing and ready to interact with you. They anticipate you may question the request.

They're prepared to respond to your follow-up emails and phone calls.

How fraudsters get away with it



41

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

Human (staff) behavior

Rote processing, trying to get the work done

Conditioned to process not necessarily question

Desire to please

- Reluctant to question authority/ fear of consequences
- Do a good job for the executive

Human (staff) behavior — (cont'd)



Lack a direct relationship with a company executive or vendor

- With vendors, usually the buyer, supply chain manager, or account manager owns the relationship — not AP

AP staff usually just process the payments

Common denominators

Payment is an **exception** from the norm

Payment is to a **new** beneficiary/
bank account

Fraudster counts on request **not** being verified with trusted source

Impostor fraud red flags

Red flags

Request to remit payment to new/different **bank account** you've never sent money to before

Request to remit payment to new/different **country** you've never sent money to before

Request for secrecy around payment (confidential/top secret)

Switch from commercial beneficiary to individual beneficiary: XYZ Manufacturing vs. Jane Smith

Slightly blurred logo on vendor letterhead or invoice indicating item may have been altered

Impostor fraud red flags (cont'd)

Red flags

For email spoofing, subtle changes to company name in the email, such as:
ABCadditive.com vs. **ABCaddiitive.com**

Change in email address from a company domain to a public domain (e.g.,
@yahoo.com and @gmail.com)

Writing style may be off: either more formal than usual or less formal than usual —
e.g., Jonathan vs. Jon

Warning: If the email has been hacked, all email addresses will appear legitimate.

Best practices for fighting impostor fraud



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

50

Watch for red flags

- Pay close attention to the details of all payment requests
- If something doesn't seem right, it probably isn't

Protect your email account

- Never give your company email address or log-on credentials to anyone you don't know who contacts you by telephone, email, or text message

Use dual custody properly

- Pay close attention to the payment details
- Authenticate a request before initiating the payment and before approving the payment

51

Monitor your accounts daily



The sooner you spot a fraudulent transaction, the sooner you can start your recovery efforts and take steps to help ensure you don't become a victim again.

If we suspect fraud



Calls to validate transaction activity must be taken seriously.

Validate the authenticity of the payment request – follow best practices.

Three ways ACH fraud occurs

25.6 billion

Number of transactions processed through the Automated Clearing House network in 2016 valued at

\$43.7 trillion

1. Thieves obtain account information from a check's MICR line
2. Counterfeit and forged checks are converted to ACH debits
3. Thieves access your online banking system and initiate ACH credits

NACHA – The Electronic Payments Association, April 2017

Seven ways to foil ACH fraud

Protect your accounts with these best practices

1. Use ACH Fraud Filter service to stop all ACH debits except those you specifically preauthorize
2. Initiate online ACH payments using dedicated computers disabled from email and web browsing
3. Use repetitive ACH payment templates to prevent unauthorized modifications to key fields
4. Set authorization limits for each individual user of the ACH payment service
5. Implement dual custody — and use it properly
 - Require payments and user changes initiated by one user to be approved by a second user on a different computer or mobile device before they take effect
6. Reconcile accounts daily to identify unauthorized ACH debits
7. Return unauthorized ACH debits promptly

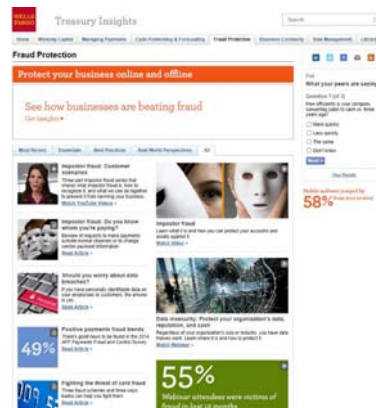
For more information on protecting your business online and offline:

Visit the Fraud Protection page on Treasury Insights

treasuryinsights.wellsfargotreasury.com

For your questions and comments, please email us at

TreasurySolutions@wellsfargo.com



Poll #3

What will be your top priority in 2017 and beyond for strengthening cyber security?

- A. Technology investment
- B. Employee training
- C. Policies, procedures, and controls
- D. Collaborate with cyber security group/info. security officer

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

<p>Device security</p> <p>Are mobile transactions secure?</p>	<p>Lost phones</p> <p>Potential exposure of information if phone is lost</p>
<p>Carrier security</p> <p>Overall security of transmitting data over cell networks</p>	<p>Access process</p> <p>Are the methods for authentication and access secure?</p>

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

Q&A



Carl Vinson
Institute of Government
UNIVERSITY OF GEORGIA



61

Thank you



Carl Vinson
Institute of Government
UNIVERSITY OF GEORGIA



62

Connect With Us!



Facebook

[facebook.com/VinsonInstitute](https://www.facebook.com/VinsonInstitute)



Twitter

[@CVIOG_UGA](https://twitter.com/CVIOG_UGA)



LinkedIn

**Carl Vinson Institute
of Government**



www.cviog.uga.edu