



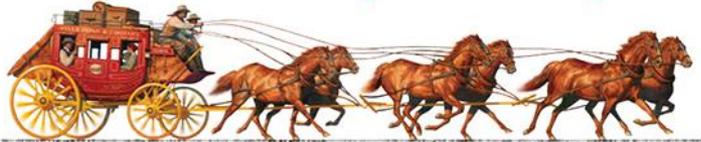
Cyber security: What your treasury division should know

Daniel D Haifley

Senior Vice President, TPC Manager

November 13, 2017

Together we'll go far



Agenda

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

Remain vigilant in payment fraud

73%

of organizations experienced attempted or actual payments fraud

64%

reported they have been exposed the BEC impostor fraud

48%

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

42%

of them report that the number of fraud incidents increased

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.

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

91% of all cyberattacks start with a phishing email



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

1 in 220

Email malware rate

Example of malware

The screenshot shows a web browser window with the URL [https://wellsfargo.com/ceportal/signon/index.jsp?TYPE=3355433&REALMID=06-3909f54-0002-0012-0000-407400004074&GLID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=\\$\\$!](https://wellsfargo.com/ceportal/signon/index.jsp?TYPE=3355433&REALMID=06-3909f54-0002-0012-0000-407400004074&GLID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$$!). The page features the Wells Fargo logo in the top left and navigation links for "Locations", "Contact Us", and "Home" in the top right. A "Return to Commercial Services" link is centered above the main content area. On the left, there is a "Bookmark this page" button. The central focus is a form titled "Commercial Electronic Office®" which includes input fields for "Your contact phone number" and "Your contact name", and a red "Continue" button. A red arrow points from the Wells Fargo logo to this form, and a red rectangular box highlights the entire form area. Below the form is a section for users not yet enrolled in commercial internet services, with links to "View Our Online Solutions" and "Contact Us". On the right side, there are two promotional banners: "Don't be a victim of impostor fraud" with a "Learn more" link, and "Forgot your password? Reset it now" with a "Watch the tutorial" link. The footer contains links for "About Wells Fargo", "Careers", "Privacy, Security & Legal", and "Sitemap", along with the copyright notice "© 1999 - 2014 Wells Fargo. All rights reserved."

Online account takeover fraud

How does Wells Fargo work to protect your business?

Protection

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



Detection

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



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.

Customer testimonial

Precision, Inc.

Impostor fraud

The fraudster

Poses as a person or entity you know and trust

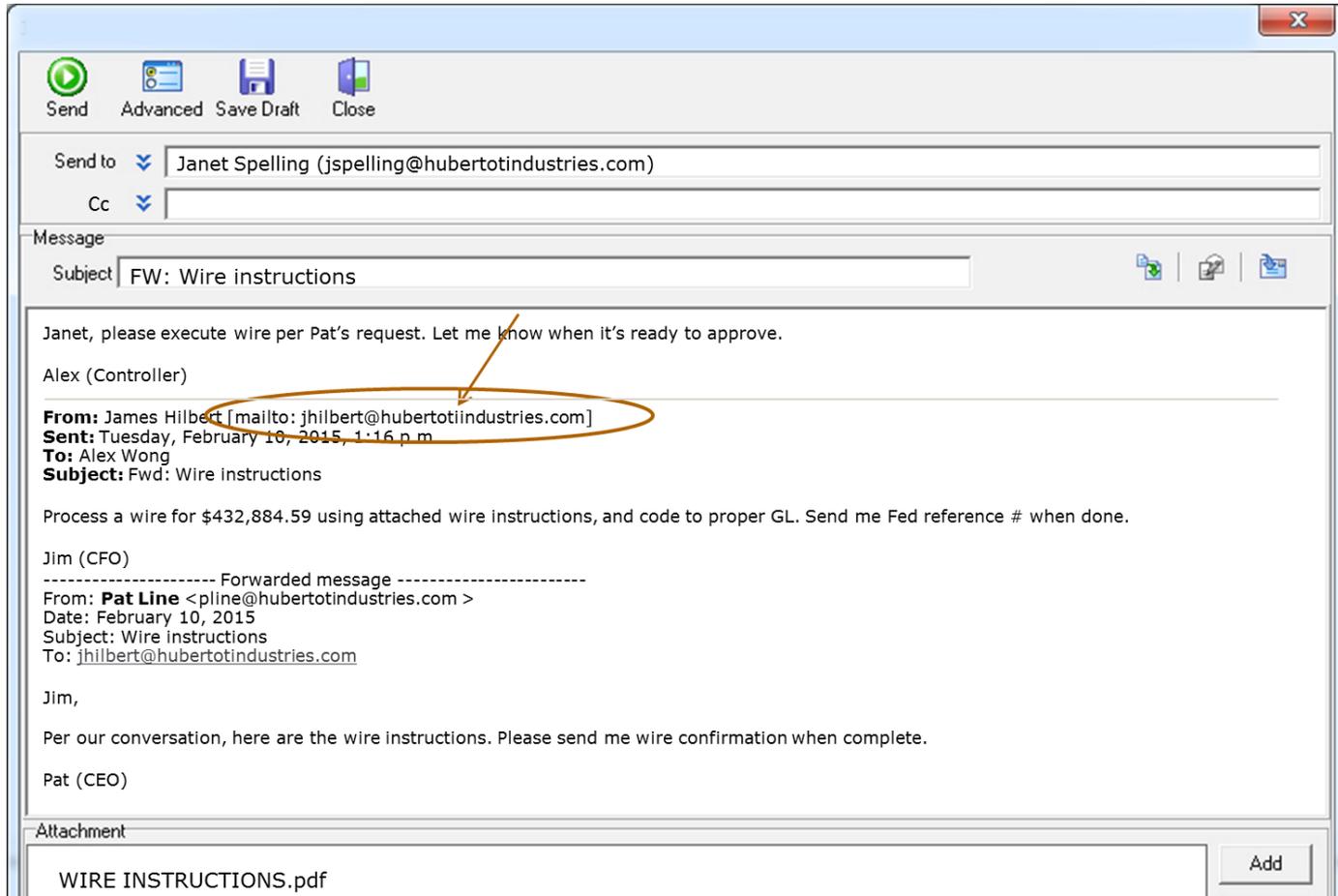
Contacts you by email, phone, fax, or mail

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



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



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 (as 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 that you may question the request.

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



How fraudsters get
away with it

Executives make perfect targets to impersonate

A photograph of three business executives in professional attire standing on a balcony of a modern glass-walled building. They are engaged in a conversation. The background shows a clear blue sky and the architectural lines of the building.

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

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 — continued



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.

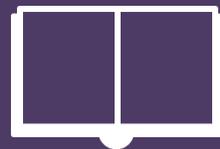
Best practices for fighting impostor fraud





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

“We’ve put all the best practices in place . . . now what?”

Insurance Solutions

Insurance considerations

Unless your policy includes an affirmative coverage grant, the answer is “probably not.” Targeted impostor fraud is a relatively new phenomenon, and traditional policies are not written to cover this type of exposure.



How can I get coverage?



Am I already covered?

Coverage can usually be added to a crime/fidelity policy, which is designed to cover fraud and theft of funds.

Insurance coverage

- Carriers may use many different names to cover this exposure
- It is important to recognize nuances
 - Ensure coverage applies to impostors posing as internal contacts (CEO, CFO) as well as external contacts (vendors, clients)
 - Confirm that there is no “look back” provision allowing a carrier to deny coverage if any of the standard verification procedures were not followed

Impostor fraud

Social engineering fraud

Spear-phishing

Payment instruction fraud

Fraudulent inducement

The underwriting process



- Coverage will be offered with a sub-limit, usually between \$50,000 and \$250,000.
- An additional premium will usually apply —typically about 10% of the theft coverage premium.
- Most carriers will require a short supplemental application to confirm internal controls (these can also be a useful tool to identify best practices!).
- If larger limits are needed, insureds will generally need to access the London or Bermuda markets.
 - Attached to a crime policy
 - Expensive
 - Minimum \$1M retention

Where do we go from here?

The insurance marketplace is continuing to evolve on this issue as frequency and severity both increase. Some London underwriters are considering offering a stand-alone product, although the scope and cost of coverage are yet to be determined.

Currently, the most appropriate way to structure coverage for impostor fraud is by adding an affirmative coverage endorsement to a crime policy. However, cyber liability carriers are exploring adding the coverage to their policy based on the underlying network security breach.



Network security and privacy
(aka cyber) insurance

What is a privacy breach/security breach?

Privacy breach

The theft, loss, or unauthorized disclosure of personally identifiable nonpublic information (PII) or third-party corporate confidential information that is in the care, custody, or control of the organization or an agent or independent contractor that is handling, processing, sorting, or transferring such information on behalf of the organization



Computer security breach:

- The inability of a third party, who is authorized to do so, to gain access to an organization's systems or services
- The failure to prevent unauthorized access to an organization's computer systems that results in deletion, corruption, or theft of data
- A denial of service (DOS) attack against an organization's internet sites or computer systems
- The failure to prevent transmission of malicious code from an organization's systems to third-party computers and/or systems

Network security and privacy insurance

- Continue to see insurers grow their loss prevention and loss mitigation services for midsize companies
- Network security risk is not going away — everyone is waking up
- For any insurance carrier that has pulled capacity, or has been hesitant to enter, another has stepped in
- Most organizations are looking to transfer the risk to an insurance product
- Cyber insurance market is expected to reach \$5B in written premiums by 2020



Network security and privacy GAP analysis

	Property	General Liability	Crime	K&R	E&O	Network Security & Privacy
First-Party Privacy/Network Risks						
Physical damage to data only		x		x		✓
Virus/hacker damage to data only		x	x	x		✓
Denial of service (DOS) attack		x	x	x		✓
Business interruption loss from security event		x	x	x	x	✓
Extortion or threat	x	x	x	✓	x	✓
Employee sabotage of data only	x	x		x		✓
Third-Party Privacy/Network Risks						
Theft/disclosure of private information	x		x	x		✓
Confidential corporate information breach	x		x	x		✓
Technology E&O	x	x	x	x	✓	x
Media liability (electronic content)	x		x	x		✓
Privacy breach expense and notification	x	x	x	x		✓
Damage to third-party's data only	x			x		✓
Regulatory privacy defense/fines	x	x	x	x		✓
Virus/malicious code transmission	x		x	x		✓

x No Coverage
 Possible Coverage
 ✓ Coverage

Network security and privacy liability insurance

Combines:

Third-party liability insurance

First-party reimbursement insurance

First-party business interruption and data asset loss

Different names depending on whom you talk to . . .

cyber risk,
cyber security,
data security,
privacy liability,
security liability,
network risk, etc.

They all essentially refer to the same thing.

Over 30+ markets with primary policy forms — which carriers will be around 5 years from now?

Insurance solutions

Third-party liability coverage

Privacy liability

Network security

Media liability

Regulatory action*
(sub-limit may apply)

*Notification expenses, credit monitoring, and other crisis management expenses are generally offered on a sub-limited basis and vary by carrier.

First-party reimbursement coverage

Privacy notification costs

Crisis management expenses

Credit monitoring costs

Forensic investigation

Other first-party reimbursement coverages

Cyber extortion

Business interruption

Data restoration

Call to action

Help increase awareness of online and impostor 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.

Insurance broker. Contact them to discuss insurance options.

Take action **now!** You can't afford to wait or do nothing.

Share this presentation. Fraud education is beneficial for everyone.

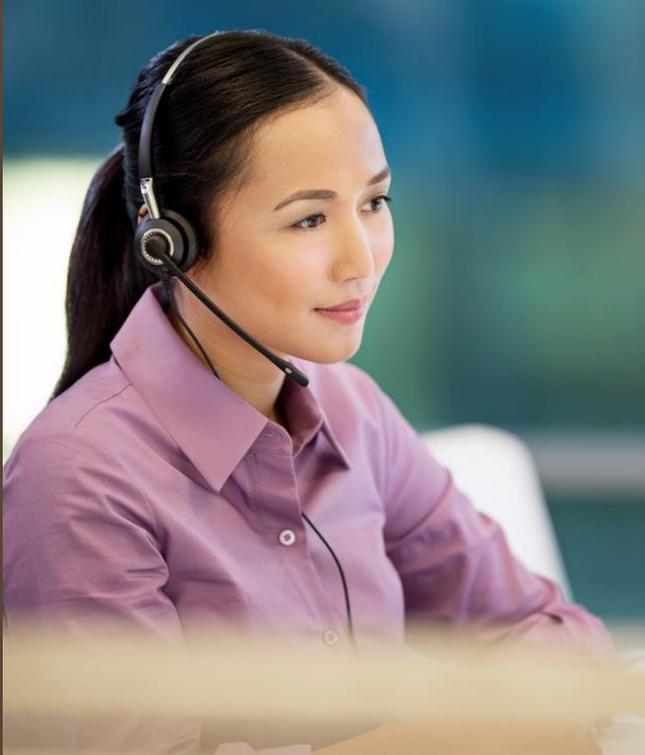
If you suspect fraud

Immediately contact your client services officer and **tell them you suspect fraud**, or call:

1-800-AT-WELLS



If we suspect fraud



Calls to validate transaction activity must be taken seriously.

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

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

Visit the Insurance Insights page:
<https://wfis.wellsfargo.com/Pages/default.aspx>

WELLS FARGO Treasury Insights

Home Working Capital Managing Payments Cash Positioning & Forecasting **Fraud Protection** Business Continuity Risk Management Library

Fraud Protection

Protect your business online and offline

See how businesses are beating fraud
Get Insights ▶

Most Recent Essentials Best Practices Real World Perspectives All

Impostor fraud: Customer scenarios
Three-part impostor fraud series that shares what impostor fraud is, how to recognize it, and what we can do together to prevent it from harming your business.
Watch YouTube Videos ▶

Impostor fraud: Do you know whom you're paying?
Beware of requests to make payments outside normal channels or to change vendor payment information.
Read Article ▶

Should you worry about data breaches?
If you have personally identifiable data on your employees or customers, the answer is yes.
Read Article ▶

Positive payments fraud trends
There's good news to be found in the 2014 AFP Payments Fraud and Control Survey.
Read Article ▶

49%

Fighting the threat of card fraud
Three fraud schemes and three ways banks can help you fight them.
Read Article ▶

55%
Webinar attendees were victims of fraud in last 12 months

Search

Twitter Facebook LinkedIn Email RSS

Poll
What your peers are saying
Question 1 (of 3)
How efficiently is your company converting sales to cash vs. three years ago?
 More quickly
 Less quickly
 The same
 Don't know
Next >
View Results

Mobile malware jumped by **58%** from 2011 to 2012

Thank you