

Fighting cyber fraud: Are you as prepared as you think?

Stephen Lenehan, Relationship Manager

Jackie Kobialko, Treasury Management Consultant

Lynn Nieves, Treasury Management Consultant

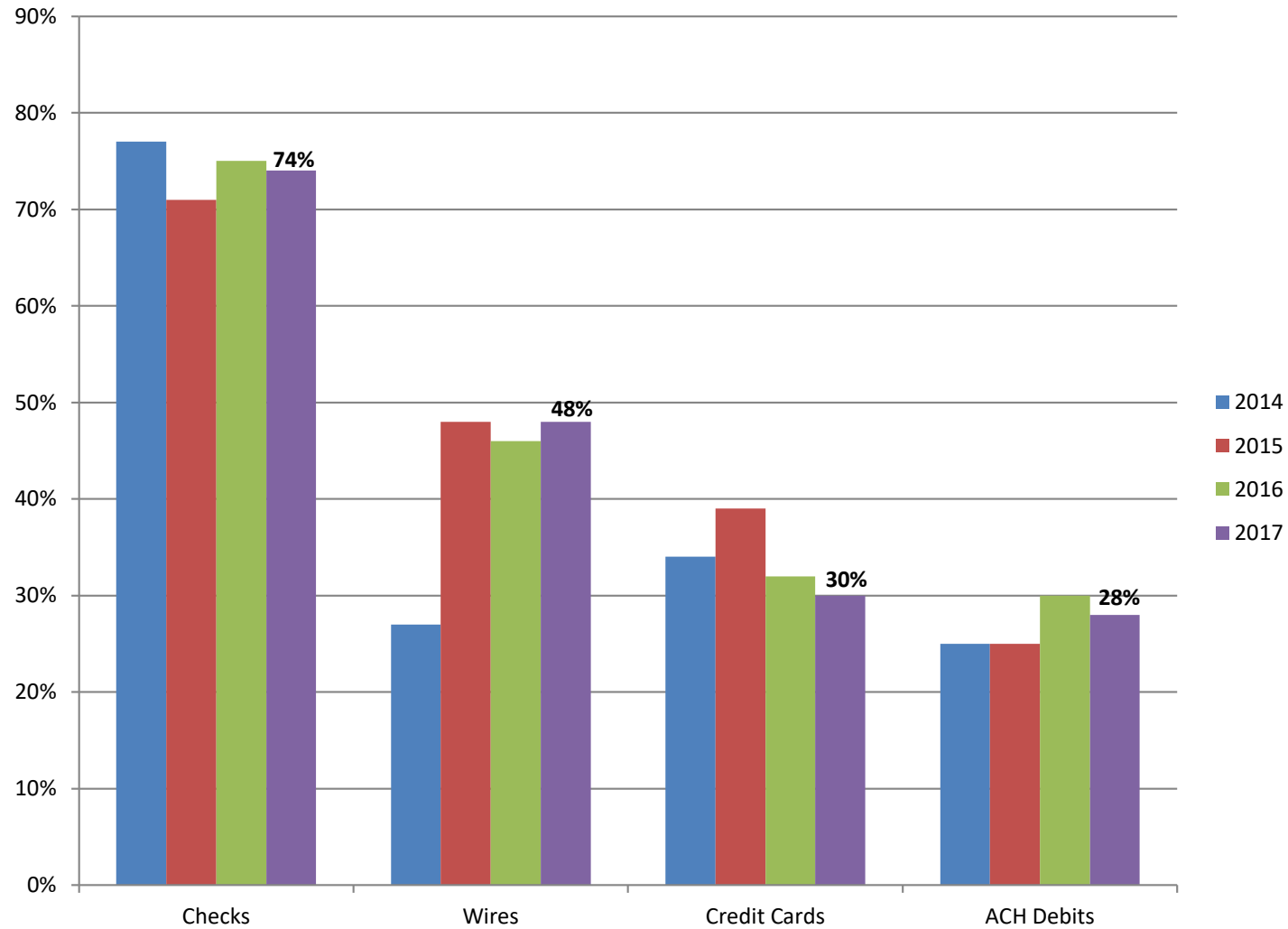
John Kolar, Fraud Prevention Manager

June 14, 2018

Agenda

- Industry trends
- Check Fraud/Positive Pay
- ACH Fraud
- Cyber payment fraud vs. security breach
- Cyber Fraud – Impostor and Account Takeover
- Mobile security threats and safeguards

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

Positive pay

99.4%

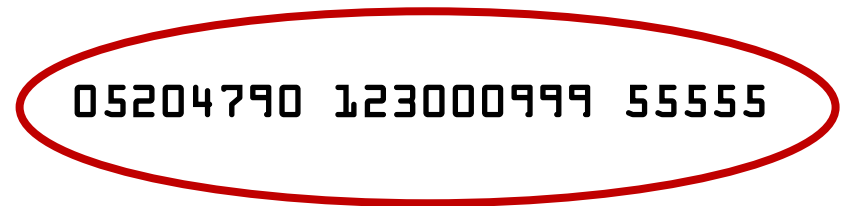
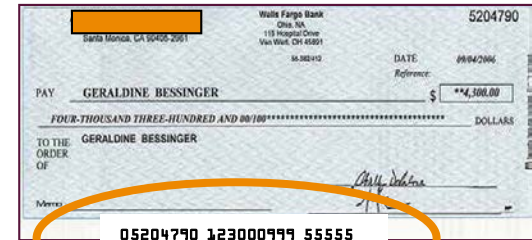
effective*



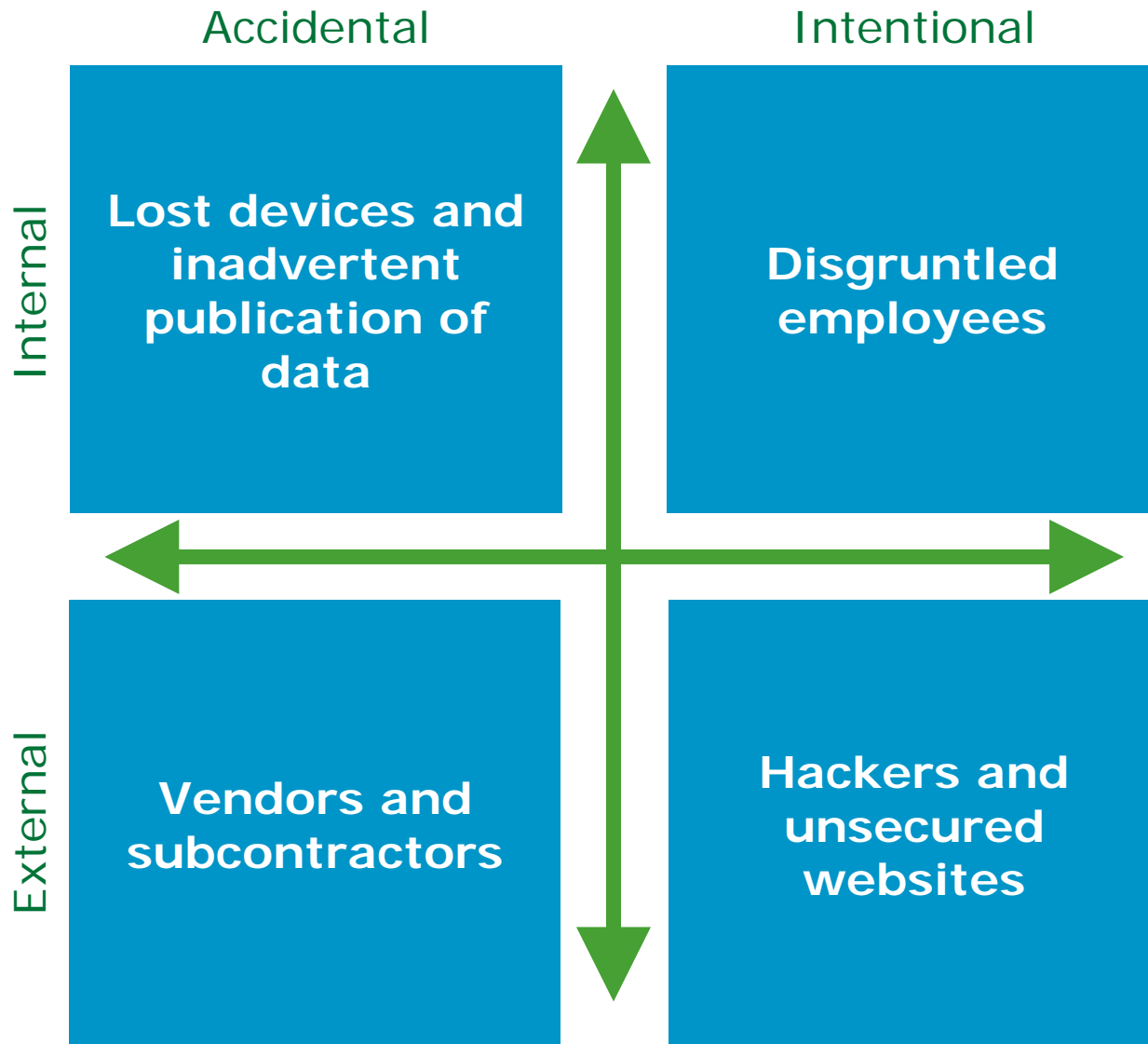
* Wells Fargo metric

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



How do data breaches occur?



Cyber payment fraud

The sobering reality of fraud



of companies were victims of payments fraud in 2016



of companies were exposed to business email compromise



of companies have been exposed to wire fraud



Financial losses from impostor fraud exceed \$1.2B worldwide

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

Social engineering via phishing example

From: Wells Fargo Online
Sent: Wednesday, January 28, 2009 6:15 AM
To: Customer@wellsfargo.com
Subject: security issues (message ref: 7992225933)

Dear Wells Fargo Bank customer,

Awkward greeting
Typos

You have recieved this alerting message, as you are listed to be an Commercial Electronic Office® user.

We would like to inform you that we are currently carrying out scheduled maintenance for banking software, that has operates customer database for Commercial Electronic Office® users. Customer database is based on a client-server protocol, so, in order to finish the update procedures, we need customer direct participation. Every Commercial Electronic Office® user has to complete a Commercial Customer Form. In order to access the form, please use the link below. The link is unique for each account holder and expires within a certain period of time. If you don't fill in Commercial Customer Form before your unique link expires, the system will automatically send you a new notification message.

Incorrect grammar

<http://wellsoffice.wellsfargo.com/session-id-4937/portal/form/do.jsp?uniquelinkid=12041450815305977383397514037683>

Compelling or urgent language

Strange or unfamiliar links

<http://www.fraudulentsite.com.module.html>

Sincerely,

Wales Fargo Online Customer Service

Mis-spelled company name

Malware

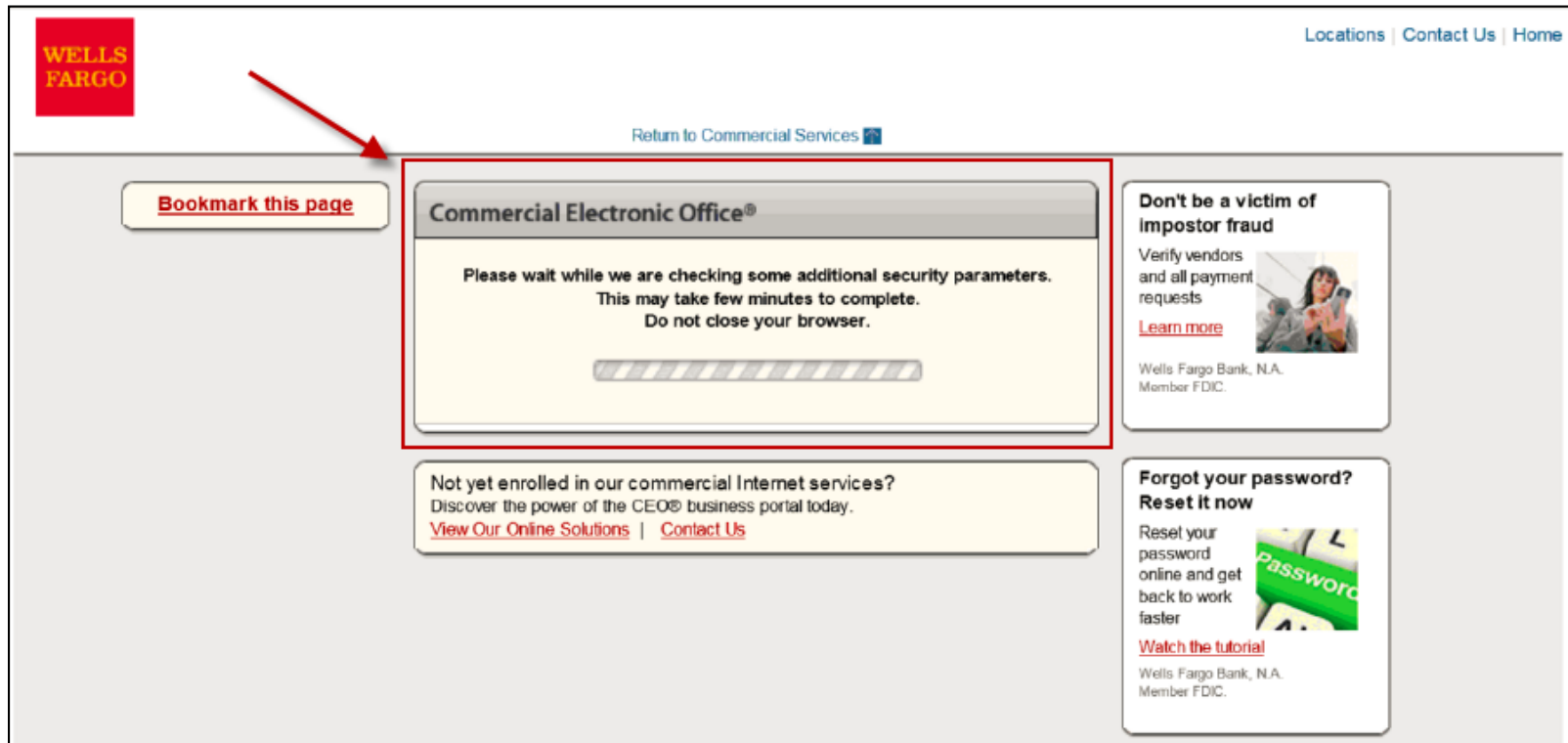
- The fraudster can obtain your confidential information by installing Malware onto your device.
- Once the malware is installed the fraudster will be able to manipulate you into performing actions or divulging confidential information by impersonating a trustworthy entity.
- This will allow the fraudster to capture all on-screen actions and supports session take-over activities.



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

Malware example

Page displays delay message. Fraudster logs on to *CEO* portal and initiates payments.



The screenshot shows the Wells Fargo CEO portal interface. At the top left is the Wells Fargo logo. At the top right are links for "Locations", "Contact Us", and "Home". Below the logo is a "Bookmark this page" button. A red arrow points to a central "Commercial Electronic Office®" box. This box contains a security delay message: "Please wait while we are checking some additional security parameters. This may take few minutes to complete. Do not close your browser." Below the message is a progress bar. To the right of the delay message are two promotional boxes: "Don't be a victim of impostor fraud" and "Forgot your password? Reset it now". At the bottom of the page, there is a box for "Not yet enrolled in our commercial Internet services?".

WELLS FARGO

Locations | Contact Us | Home

Return to Commercial Services

[Bookmark this page](#)

Commercial Electronic Office®

Please wait while we are checking some additional security parameters.
This may take few minutes to complete.
Do not close your browser.

Not yet enrolled in our commercial Internet services?
Discover the power of the CEO® business portal today.
[View Our Online Solutions](#) | [Contact Us](#)

Don't be a victim of impostor fraud
Verify vendors and all payment requests
[Learn more](#)
Wells Fargo Bank, N.A.
Member FDIC.

Forgot your password? Reset it now
Reset your password online and get back to work faster
[Watch the tutorial](#)
Wells Fargo Bank, N.A.
Member FDIC.

Online account takeover fraud

How does Wells Fargo work to protect your business?

Protection

- Multilayer approach
- Safeguarding credentials
- Product security
- Fraud protection services



Detection

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



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

Anonymous customer

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

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

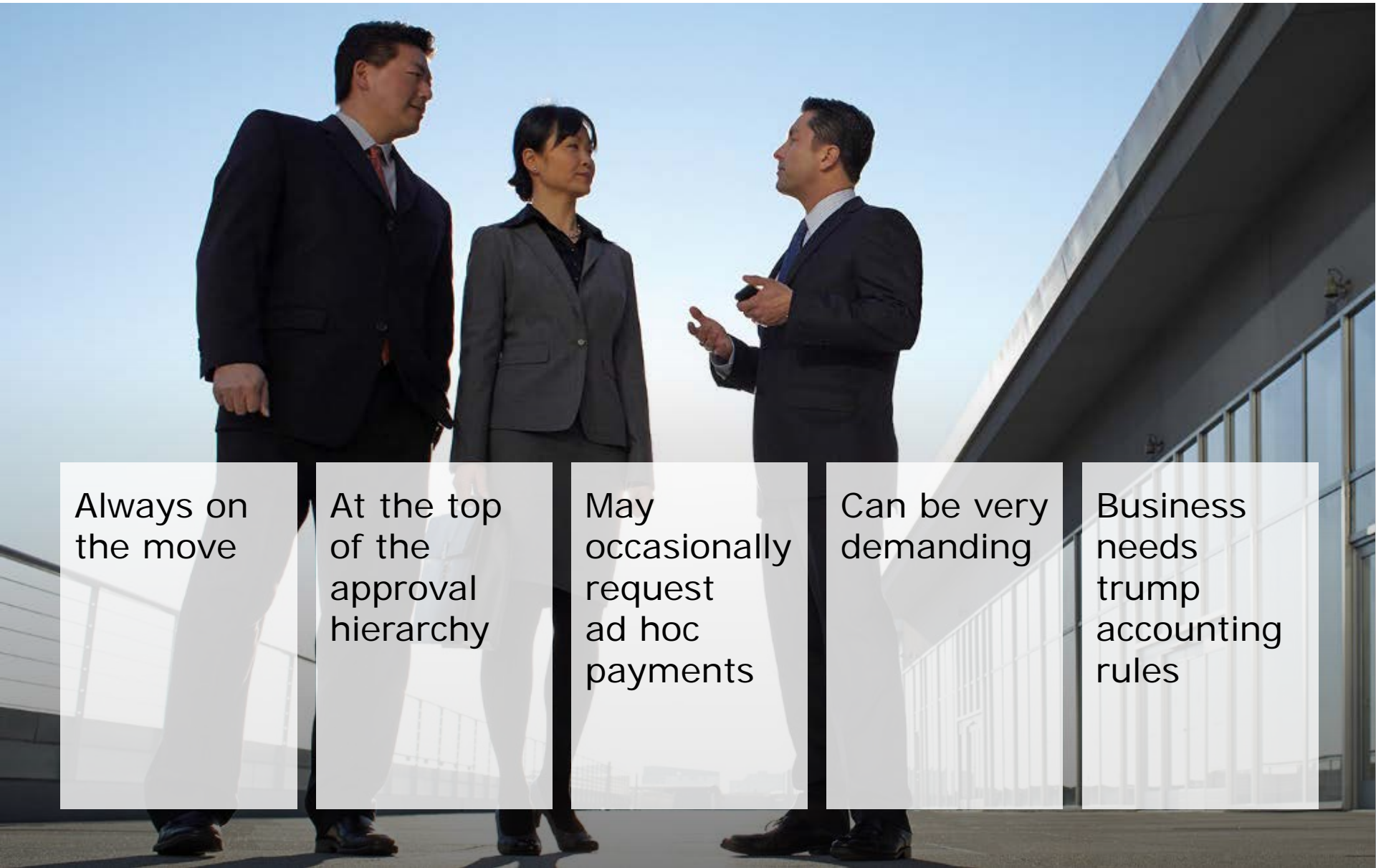


Fraudsters don't steal online banking credentials and make payments (as in account takeover fraud)



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

Executives make perfect targets to impersonate

A photograph of three business executives in professional attire walking and talking outdoors. The scene is set against a clear blue sky and a modern building with large glass windows. The executives are positioned in the upper half of the frame, with their lower bodies and legs visible through semi-transparent text boxes at the bottom.

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



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, to question unusual email payment requests – even those from executives

Alert vendors and partners

- Warn vendors that they are targets Tell vendors you no longer accept changes to bank account information by email
- Instruct them not to change their remittance information without verifying the request with you

Administrative risk assessment

- Review users' access
- Ensure the user has their own id
- Delete IDs no longer in use
- Implement dual control

Mobile security threats



**Mobile
malware**



**Social
engineering**



**Unauthorized
apps**



**Fraudulent
apps**



**Lost
Devices**

To protect your business, 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

In summary

The future of payment fraud

- Check fraud is not going away –try to go electronic
- Impostor or BEC fraud is becoming more prevalent
- Willing to interact with the target
- Fraudsters are moving to ACH from Wire
- ACH transactions are smaller amounts
- Targeting specific industries (i.e., real estate, higher ed)

To avoid phishing attempts

- Remember that most companies, banks, etc. will never request personal or sensitive information via email or text
- If in doubt, call the company to check, but don't use the phone number on the email
- Don't reply to a message that asks for personal or financial information
- Never follow a link to a secure site from an email, always enter the URL manually
- Use a phishing filter; many of the latest web browsers have them built in

Secure passwords are critical

- Create different passwords for different purposes
 - Social networking
 - Major shopping sites
 - Financial institutions
 - Separate passwords for infrequently visited sites
- Use passwords that cannot be easily guessed
 - No pet names, family names – they can be found on social media sites
 - A recent survey revealed that “password” and “123456” are very popular
 - Try using the first letters of a memorable phrase and make it more complex by replacing letters with characters or numbers

Maintain check security

- Require tight security of all check stock
 - Destroy obsolete check stock
 - Keep check stock in an area that is locked and secure
- Purchase check stock from a reputable vendor
 - Include safety features in checks
 - Require a secure method of delivery for new stock
- Inventory check stock at least quarterly
- Limit number of individuals who have access to check stock

If you suspect fraud

Immediately contact your bank representative and **tell them you suspect fraud.**



For more information on protecting your business online **and** offline:

Visit the Fraud & Security page on *Treasury Insights*
<https://digital.wf.com/treasuryinsights/fraud-security/>

or The Fight Fraud page on wells Fargo.com
<https://www.wellsfargo.com/com/fraud/>

WELLS FARGO Treasury Insights

Home Emerging Commerce Fraud & Security Regulation & Risk Payments & Liquidity

Real-time payments: Drivers, benefits, and the future
Insight into the influences of real-time payment adoption.
[Read Article](#)

3 P's of Receivables Automation
Improve receivables processes with small changes in how you Present, Pay and Post.
[Learn More >](#)

60
6 best practices to improve accounts payable
Streamline your process and maximize technology to accelerate accounts payable.
[Learn More >](#)

Commerce on the go
The emergence of connected consumer devices is changing the way we do business.
[Learn More >](#)

WELLS FARGO Treasury Management webinar

Cyber fraud: Your threats have broadened

317 million
New pieces of malware created last year — almost 1 million per day*

Dear Karen,

Credit card data fraud used to dominate the list of a company's cyber fraud risks. But top-of-mind threats now include account takeover, impostor fraud, and Denial of service (DoS) attacks. Fraudsters attack quickly and furtively, and their methods are sophisticated and evolving.

Join us on Tuesday, November 10, for **Cyber fraud: Your threats have broadened** — a complimentary webinar exclusively for

[Register Now](#)

Complimentary webinar

Tuesday,
November 10, 2015
11:00 a.m. Pacific Time
1:00 p.m. Central Time
2:00 p.m. Eastern Time

Program level:
Intermediate

Delivery method:
Group-internet based

Advanced preparation:

Thank you!