Reducing Risks; What you need to know about Payment Fraud

Wells Fargo Customer Training

© 2016 Wells Fargo Bank, N.A. All rights reserved. For public use.
Agenda

- Fraud trends
- Online account takeover fraud
- Impostor fraud
- Call to action
Remain vigilant in payment fraud

72% of organizations experienced attempted or actual payments fraud

42% of them report that the number of fraud incidents increased

48% of organizations were exposed to wire fraud— a significant increase from the previous survey

Source: 2016 AFP Payments Fraud and Control Survey
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

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
## Phishing successes explained

<table>
<thead>
<tr>
<th>Cybercriminal excellence</th>
<th>Social media explosion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accurate logos, professionally written communications, personalization of content increase believability</td>
<td>Users are sharing an alarmingly amount of information through social media platforms</td>
</tr>
<tr>
<td>Targets are more likely to click on the links and/or open attachments, which download malware</td>
<td>Provides criminals with the fodder necessary to construct personalized and believable messages</td>
</tr>
</tbody>
</table>

### 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
Example of malware

- Customer receives phishing email and inadvertently downloads malware.
- Malware enables the fraudster to divert the customer to a 'fake' Commercial Electronic Office® (CEO®) Portal and obtain credentials, including token codes.
- Page displays a delay message while the fraudster is busy logging on to the CEO Portal and initiating payments.
- Malware also allows the fraudster to insert pop-up messaging requesting customer contact information.
- Fraudster calls the customer claiming to be from Wells Fargo to discuss the customer’s unreported ‘system issues’.
- Fraudster is looking to engage other users to log into the CEO Portal using the same device in order to compromise their credentials and circumvent Dual Custody.
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.

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

Monitor accounts daily and use notification and alert services.

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

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

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

<table>
<thead>
<tr>
<th>The fraudster</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Poses as a person or entity you know and trust</td>
<td></td>
</tr>
<tr>
<td>Contacts you by email, phone, fax, or mail</td>
<td></td>
</tr>
<tr>
<td>Requests a payment, submits an invoice, or asks to change vendor payment instructions</td>
<td></td>
</tr>
</tbody>
</table>

If you fall for the scam, any payments you send go to the fraudster — not where you intended.
Contact by email
Example of executive email spoofing

Send to: Janet Spelling (jspelling@hubertotindustries.com)
Cc: 

Subject: FW: Wire instructions

Janet, please execute wire per Pat’s request. Let me know when it’s ready to approve.

Alex (Controller)

From: James Hilbert [mailto: jhilbert@hubertotindustries.com]
Sent: Tuesday, February 10, 2015, 1:15 p.m
To: Alex Wong
Subject: Fwd: Wire instructions

Process a wire for $432,884.59 using attached wire instructions, and code to proper GL. Send me Fed reference # when done.

Jim (CFO)
------------- Forwarded message -----------------
From: Pat Line <pline@hubertotindustries.com>
Date: February 10, 2015
Subject: Wire Instructions
To: jhilbert@hubertotindustries.com

Jim,

Per our conversation, here are the wire instructions. Please send me wire confirmation when complete.

Pat (CEO)
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, 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.
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
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
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

<table>
<thead>
<tr>
<th>Red flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request to remit payment to new/different <strong>bank account</strong> you've never</td>
</tr>
<tr>
<td>sent money to before</td>
</tr>
<tr>
<td>Request to remit payment to new/different <strong>country</strong> you've never</td>
</tr>
<tr>
<td>sent money to before</td>
</tr>
<tr>
<td>Request for secrecy around payment (confidential/top secret)</td>
</tr>
<tr>
<td>Switch from commercial beneficiary to individual beneficiary:</td>
</tr>
<tr>
<td>XYZ Manufacturing vs. Jane Smith</td>
</tr>
<tr>
<td>Slightly blurred logo on vendor letterhead or invoice indicating item</td>
</tr>
<tr>
<td>may have been altered</td>
</tr>
</tbody>
</table>
## 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
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
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.
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
Thank you