Payment fraud and risk

August 2023
Introductions

Stephen Callahan
Relationship Manager
469-498-6582
Stephen.F.Callahan@wellsfargo.com

Amy Blayney
Treasury Management Consultant
816-401-1076
amy.blayney@wellsfargo.com

Chanda Brookshire
Treasury Management Analyst
801-246-4716
Chanda.brookshire@wellsfargo.com
Agenda

• Current fraud landscape
• New and evolving threats
• Business email compromise
• Account takeover
• Critical strategies your organization needs for fraud protection
• Fraud education resources
Payment fraud continues to be a significant business risk

It only takes one incident for your organization to be compromised

2022 fraud statistics

65% of organizations faced attempted or actual payments fraud

Companies of all sizes and across all industries are at risk

What are you doing to reduce your exposure

Source: Association for Financial Professionals, 2023 AFP® Payments Fraud and Control Survey
Are your payments a target for fraud?

Organizations that experienced fraud in 2022 by payment type

<table>
<thead>
<tr>
<th>Payment Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACH credits</td>
<td>30%</td>
</tr>
<tr>
<td>ACH debits</td>
<td>30%</td>
</tr>
<tr>
<td>Wire transfers</td>
<td>31%</td>
</tr>
<tr>
<td>Corporate/Commercial credit cards</td>
<td>36%</td>
</tr>
<tr>
<td>Checks</td>
<td>63%</td>
</tr>
</tbody>
</table>

Source: Association for Financial Professionals, 2023 AFP® Payments Fraud and Control Survey
Current threat landscape
Key fraud threats impacting Wholesale customer-facing digital channels

Business Email Compromise (BEC)
BEC is where a fraudster impersonates a vendor, company executive, or another trusted trading partner — ultimately tricking you into making the payment to them.

Online Account Takeover (ATO)
Thieves gain access to make unauthorized transactions, including transferring funds, or stealing sensitive customer information.
The cost of BEC

According to the FBI Internet Crime Report for 2022

21,832 BEC complaints

$2.7 billion in total adjusted loss

$124,000 average loss per incident

up 13% from 2021
Business email compromise (BEC) aka Imposter fraud

<table>
<thead>
<tr>
<th>Sophisticated fraudsters + time and patience = significant losses</th>
</tr>
</thead>
</table>

### How they target you
- Spoofed email address
- Compromised email account

### Why it works
- Attempts appear legitimate at first

### Types of imposter fraud
- Executive
- Vendor
- Payroll
# What is phishing?

Phishing is the fraudulent attempt to obtain sensitive information, such as usernames, passwords, and account details, typically through an email, text message, or even a phone call.

## Example Phishing Email

**From:** WellsFargo – Support Online
**Date:** December 8, 2017 at 2:23:01 PM EST
**To:** Undisclosed-Recipients;

**Subject:** !Alerts! Security Information Regarding your Account.

We are sorry, For your protection and security reasons, your Wells Fargo account has been locked.

Please click on the following link to unlock your account.

Log-in to: [https://www.wellsfargo.com/online-banking/updating](https://www.wellsfargo.com/online-banking/updating)

Thank you for bringing this matter to our attention.

Sincerely, Wells Fargo Online Banking Team.

---

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>The sender's email address uses an inappropriate domain name</td>
</tr>
<tr>
<td></td>
<td>- In the example, the email domain is “comcast.net” not “wellsfargo.com”</td>
</tr>
<tr>
<td>2.</td>
<td>The includes an urgent call to action in the subject line and the message copy</td>
</tr>
<tr>
<td>3.</td>
<td>Phishing emails may also contain extra spacing or unusual punctuation, grammar, capitalization, or language</td>
</tr>
<tr>
<td>4.</td>
<td>It contains a suspicious link that could lead to a fraudulent website</td>
</tr>
<tr>
<td></td>
<td>- When using a laptop or desktop computer, check the link's URL by hovering over it with the cursor. The URL will show in the browser window</td>
</tr>
</tbody>
</table>

This is an example email only
Departments most vulnerable to BEC fraud

Percentage of organizations impacted by department type

Accounts Payable departments were reported as the most targeted area for BEC

Source: Association for Financial Professionals, 2023 AFP® Payments Fraud and Control Survey
Steps to help protect against BEC fraud

Verify the request
- Watch for red flags, especially if a request seems out of the ordinary
- Verbally verify and confirm the request
- Only use the contact information on file

Implement dual custody
- Serves as a second chance to identify potential fraud
- Verify changes and pay attention to the details
- Confirm changes are verified before approving payment

Monitor accounts
- Reconcile bank accounts daily and pay close attention to account activity
- Protect your email account and login credentials
Account takeover

Fraudster steals confidential information to access online accounts directly

- Fraudster typically leverages Social Engineering and Malware to execute an account takeover incident
- Social Engineering, such as phishing, manipulates you into divulging confidential information
- Malware is malicious software installed on your computer without your consent or knowledge
- Malware allows a fraudster to access accounts and send unauthorized payments
Steps to help protect against ATO fraud

Don’t

• Don’t share online banking credentials
• Don’t click on links or download programs or attachments in emails or text messages—unless from a trusted sender

Caution

• Be wary of unsolicited phone calls concerning unreported system issues—Immediately contact your Wells Fargo bank representative

Do

• Use notification and alert services to receive text or email notifications regarding electronic debits from your accounts
• Implement dual custody
• Use multi-factor authentication, or at least two-factor authentication, for access to your company networks and for payments initiation
• Keep antivirus software current on all your work devices and on any personal devices that you use to access your company’s networks
• Install all system and application updates for patching security flaws in timely manner
Create a cyber security culture

- Establish a regular and ongoing process for educating staff
- Instruct all staff, especially AP staff, to question unusual payment or account change requests received by email—even from executives
- Alert management and supply chain personnel to the threat

Vendor and trading partner awareness

- Educate your vendors and trading partners—they are targets for fraud, too
- Define a communication process for payment and account changes

Educate your entire staff

Share your knowledge and best practices
Internal control methods for ACH fraud

Establish rules and outline responsibilities

Recommended practices

- Document procedures on vendor validation process for new or updated relationships
- ACH debit controls
- Utilizing account validation services
- Daily reconciliation
Internal control methods for check fraud

Establish rules and outline responsibilities

Recommended practices

• Positive pay
• Payee validation
• Daily reconciliation
• Segregation of accounts
• Check block for non-disbursing accounts
Resources for more fraud protection information

Wells Fargo fraud websites for additional fraud assets

• Treasury Insights Fraud & Security page

• Wellsfargo.com fraud page
  https://www.wellsfargo.com/com/fraud

External resources

• FBI Internet Crime Complaint Center (IC3)
  https://www.ic3.gov

• Cybersecurity & Infrastructure Security Agency (CISA)
  http://www.cisa.gov/

Note: to use the links, highlight the link, right click and select “Open Hyperlink” – if reading hard copy, enter the https address on your browser.
Thank you