Texas A&M AFR

August 2022
Key topics for discussion

01 Fraud
02 NACHA Rules
03 Report Clean Up
Fraud is imminent, will you be...

susceptible

with impacts to

- revenue
- proprietary data
- trust
- reputation
- relationships
- employees
- regulations

or

prepared
New threats in the world of fraud
Current threat landscape
Key fraud threats impacting Wholesale customer-facing digital channels

**Business email compromise (BEC) aka imposter fraud**
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)**
Cyber criminals access your online accounts to make unauthorized transactions, including transferring funds, or stealing sensitive customer information.
Organizations impacted by BEC

Percent of organizations experiencing actual BEC fraud

<table>
<thead>
<tr>
<th>Year</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>2021</td>
<td>68%</td>
</tr>
<tr>
<td>2020</td>
<td>76%</td>
</tr>
<tr>
<td>2019</td>
<td>75%</td>
</tr>
<tr>
<td>2018</td>
<td>80%</td>
</tr>
<tr>
<td>2017</td>
<td>77%</td>
</tr>
<tr>
<td>2016</td>
<td>74%</td>
</tr>
<tr>
<td>2015</td>
<td>64%</td>
</tr>
</tbody>
</table>

Source: Association for Financial Professionals, 2022 AFP® Payments Fraud and Control Report

68% of organizations were targeted by BEC in 2021
The cost of BEC

According to the FBI Internet Crime Report for 2021

- 19,954 BEC complaints
- $2.4 billion in total adjusted loss
- $120,000 average loss per incident

up 33% from 2020
Business email compromise (BEC) – aka Imposter fraud

Sophisticated fraudsters + time and patience = significant losses

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
Wire transfers continue to be a prime target for BEC scams with 41% of financial professionals reporting impacts with ACH credits growing from 34% last year to match wires at 41%.
Departments most vulnerable to BEC fraud

Percentage of organizations impacted by department type

- Accounts Payable (AP): 58%
- Treasury: 15%
- AR, HR, and Procurement: 5%
- C-Suite: 7%

Source: Association for Financial Professionals, 2022 AFP® Payments Fraud and Control Report
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 you have in your system of record

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
Current threat landscape

Key fraud threats impacting Wholesale customer-facing digital channels

**Business email compromise (BEC) aka imposter fraud**
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)**
Cyber criminals access your online accounts to make unauthorized transactions, including transferring funds, or stealing sensitive customer information.
Account takeover (ATO)

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.
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.

1. The sender's email address uses an inappropriate domain name
   - In the example, the email domain is “comcast.net” not “wellsfargo.com”

2. The includes an urgent call to action in the subject line and the message copy

3. Phishing emails may also contain extra spacing or unusual punctuation, grammar, capitalization, or language

4. It contains a suspicious link that could lead to a fraudulent website
   - 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

From: WellsFargo – Support_Online
From: WellsOnlineBank2@comcast.net
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

Thank you for bringing this matter to our attention.

Sincerely, Wells Fargo Online Banking Team.

wellsfargo.com | Fraud Information Center

This is an example email only
Triumph over takeover

Nine steps to help protect against ATO

1. Beware of unexpected token prompts or on-screen messaging
2. Protect your credentials
3. Implement dual custody
4. Require multi-factor authentication
5. Never click on links from unknown senders
6. Monitor accounts
7. Sign up for alerts services
8. Update antivirus software
9. Initiate transactions from stand-alone PCs that restrict email and web browsing
Know your organization’s critical needs

- **One size does not always fit all:** integrate your security measures to reflect your organization’s priorities
- **Have an actionable plan** in place to respond in case of a fraud attack
- **Simple processes** can be some of your most powerful safeguards
- **Watch** the fraud course you have developed
Payment fraud continues to be a significant business risk

It only takes one incident for your organization to be compromised

2021 fraud statistics

71% of organizations faced attempted or actual payments fraud

Companies of all sizes, across all industries are at risk

What are you doing to reduce your exposure?

Source: Association for Financial Professionals, 2022 AFP Payments Fraud and Control Report
Are your payments a target for fraud?

Organizations that experienced fraud in 2021 by payment type

- ACH credits: 24%
- Corporate/Commercial credit cards: 26%
- Wire transfers: 32%
- ACH debits: 37%
- Checks: 66%

Source: Association for Financial Professionals, 2022 AFP® Payments Fraud and Control Report
Steps to help protect against payments fraud

- Dual approval for high-risk transactions
- Positive pay and ACH fraud filter
- Account validation services
- Mobile access to fraud features
- Employee training and increased awareness
Avoid exposure by taking measures to prevent fraud related to...

01 Fraud

02 NACHA Rules

03 Report Clean Up
NACHA Changes

**Micro Entries for AVS**
- ACH less than $1
- Must have “ACCTVERIFY” in description
- Standard SEC to be used

**Supplemental Data Security**
- Originators that send greater than 2 million payments a year
- Data must be rendered unreadable at rest or stored electronically
- Encryption, Truncation, and Tokenization
Avoid exposure by taking measures to prevent fraud related to...

01 Fraud
02 NACHA Rules
03 Report Clean Up
Questions