

# Fraud insights and prevention discussion presentation

---

**Laurel Hill, Senior Vice President & Senior Relationship Manager  
Government Banking**

October 3, 2022

Avoid exposure by taking measures to prevent fraud related to...



# Fraud is imminent, will you be...

susceptible  
with impacts to

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

or

prepared





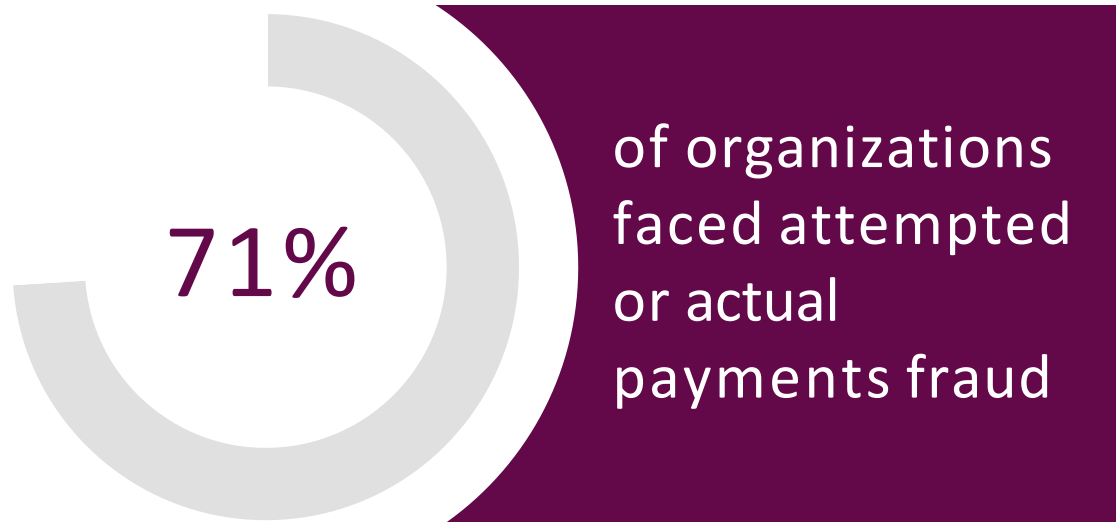
Avoid exposure by taking measures to prevent fraud related to...



# Payment fraud continues to be a significant business risk

It only takes one incident for your organization to be compromised

## 2021 fraud statistics



Companies of  
all sizes,  
across all industries  
are at risk

What are you doing to reduce your exposure?



# 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

# 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







Avoid exposure by taking measures to prevent fraud related to...



# 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

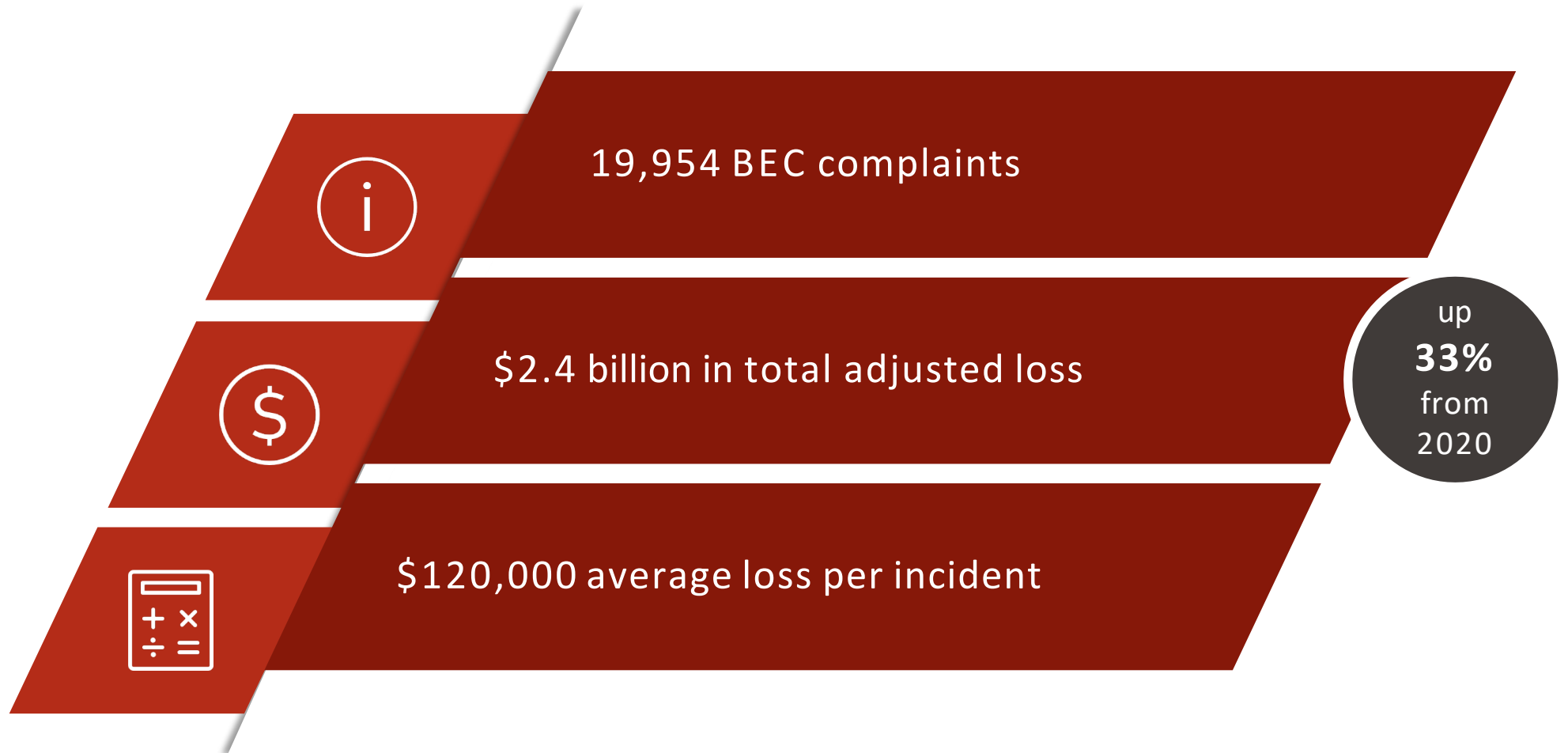
- Attempts **appear legitimate** at first

## Types of imposter fraud

- **Executive**
- **Vendor**
- **Payroll**

# The cost of BEC

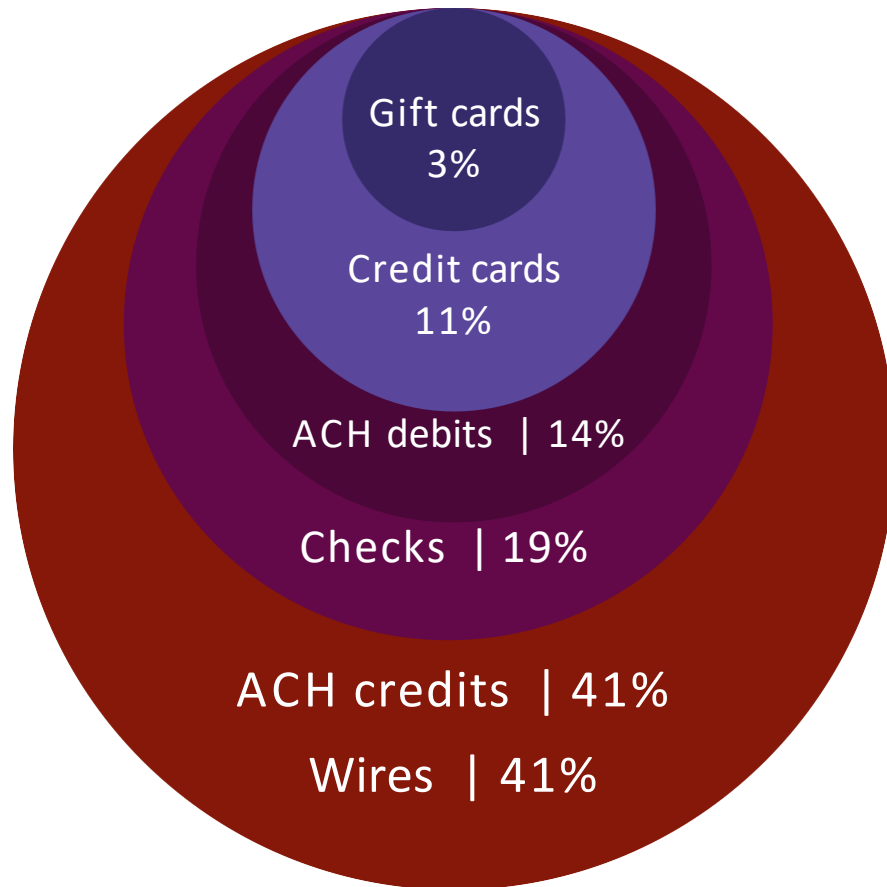
According to the FBI Internet Crime Report for 2021





# Payment methods impacted by BEC

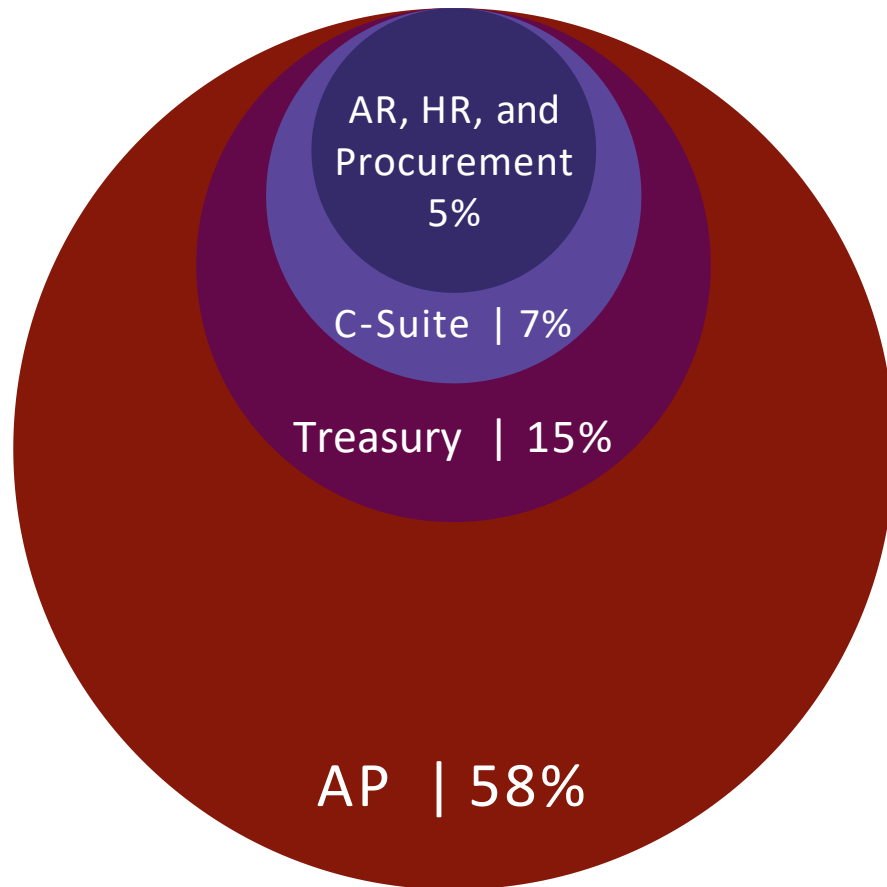
Percentage of organizations impacted by payment type



**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** departments were reported as the most targeted area for BEC

# Fraud attacks: the schemes that stand out



# 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.

<p><b>From:</b> WellsFargo – Support_Online <a href="mailto:WellsOnlineBank2@comcast.net">WellsOnlineBank2@comcast.net</a> <b>1</b></p> <p><b>Date:</b> December 8, 2017 at 2:23:01 PM EST</p> <p><b>To:</b> Undisclosed-Recipients;;</p> <p><b>Subject:</b> <b>!Alerts!</b> <b>2</b></p>	<p>1. The sender's email address uses an <b>inappropriate domain name</b></p> <ul style="list-style-type: none"><li>– In the example, the email domain is "comcast.net" not "wellsfargo.com"</li></ul>
<p> <a href="https://www.wellsfargo.com">wellsfargo.com</a></p>	<p>2. The includes an <b>urgent call to action</b> in the subject line and the message copy</p>
<p><b>Security Information Regarding your Account.</b></p> <p>We are sorry, For your protection and security reasons, your Wells Fargo account has been locked. <b>3</b></p>	<p>3. Phishing emails may also contain <b>extra spacing or unusual punctuation, grammar, capitalization, or language</b></p>
<p>Please click on the following link to unlock your account.</p> <p>Log-in to :<a href="https://www.wellsfargo.com/online-banking/updating">https://www.wellsfargo.com/online-banking/updating</a> <b>4</b></p> <p>Thank you for bringing this matter to our attention.</p> <p>Sincerely, Wells Fargo Online Banking Team.</p> <p><a href="https://www.wellsfargo.com">wellsfargo.com</a>   <a href="#">Fraud Information Center</a></p>	<p>4. It contains a <b>suspicious link</b> that could lead to a fraudulent website</p> <ul style="list-style-type: none"><li>– 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</li></ul>





Avoid exposure by taking measures to prevent fraud related to...



# 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

# 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



Avoid exposure by taking measures to prevent fraud related to...



# 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



# Education and awareness to help mitigate the risk

## Educate your entire staff

### 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

### Share your knowledge and best practices

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

# Resources for more fraud protection information

## Wells Fargo fraud websites for additional fraud assets

- Treasury Insights Fraud & Security page  
<https://global.wf.com/treasury-insights/fraud-security/>
- 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/>