WELLS FARGO

Treasury Management

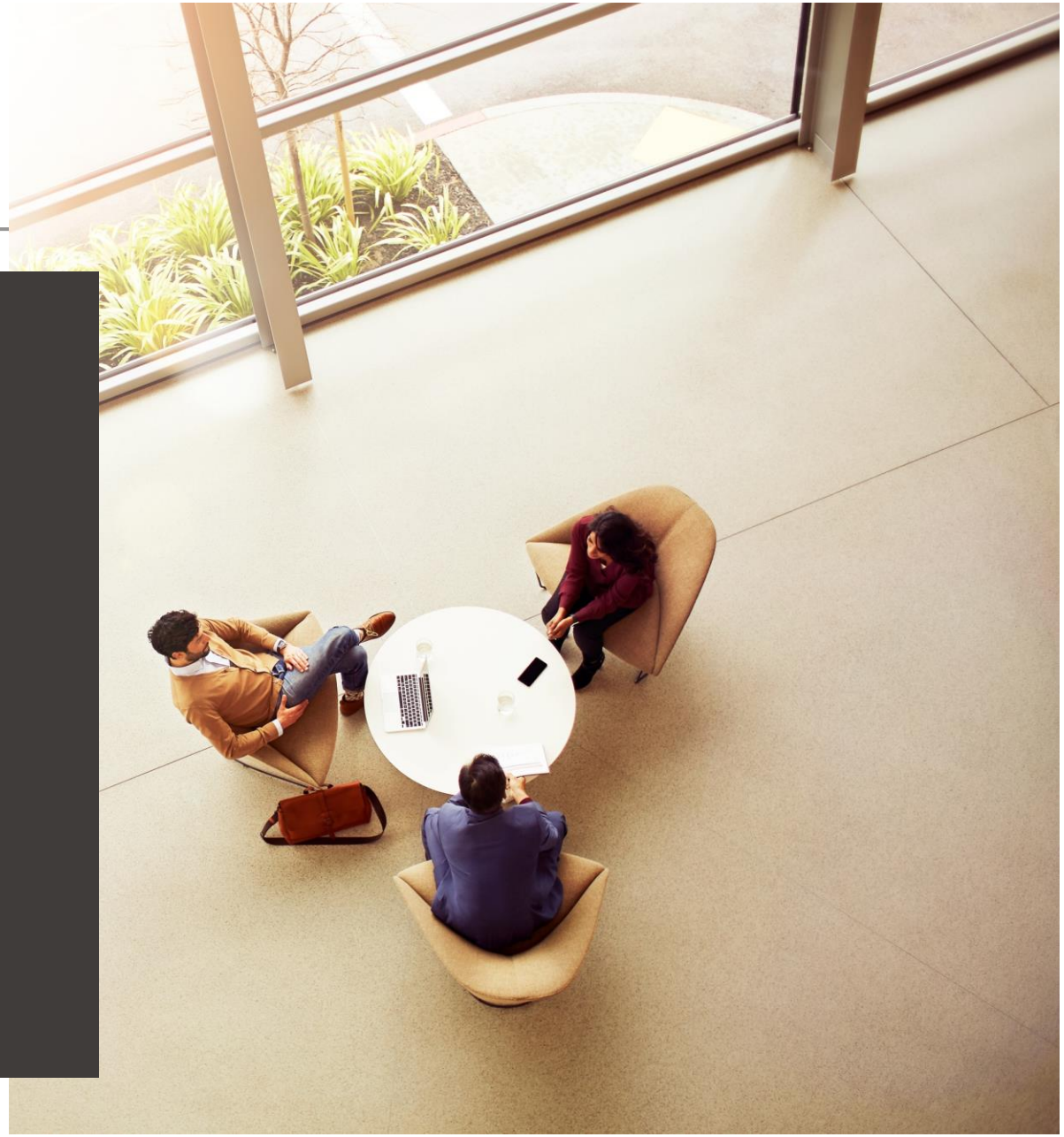
Mitigating cyber payments fraud and risk

April 27, 2023

Anil Khilnani, Fraud Education & Awareness
Zina Monroe, Relationship Manager

Agenda

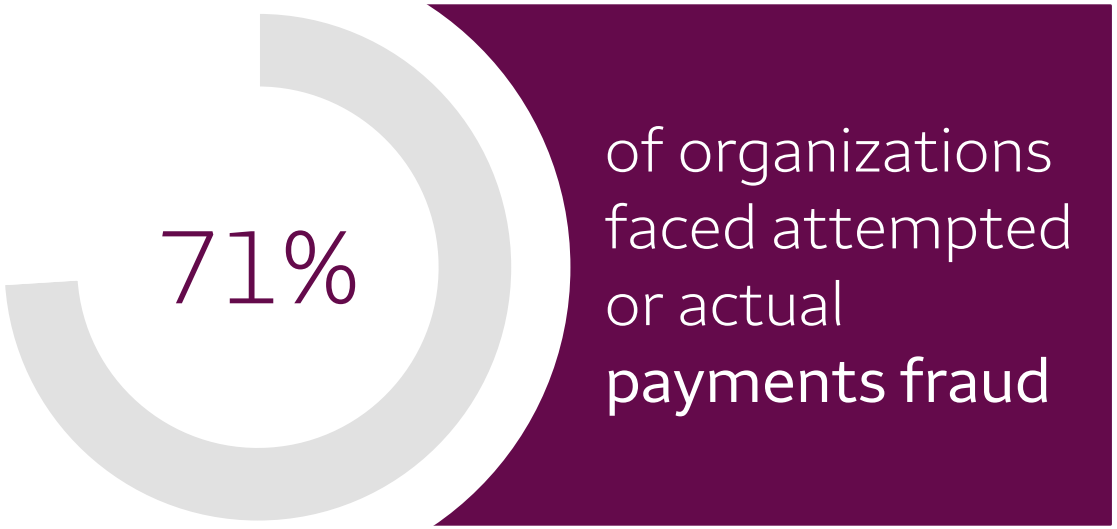
- Current fraud landscape
- New and evolving threats
- Business email compromise
- Account takeover
- Critical strategies your organization needs for fraud protection
- Fraud education resources



Payment fraud continues to be a significant business risk

It only takes **one incident** for your organization to be compromised

2021 fraud statistics



of organizations faced attempted or actual **payments fraud**

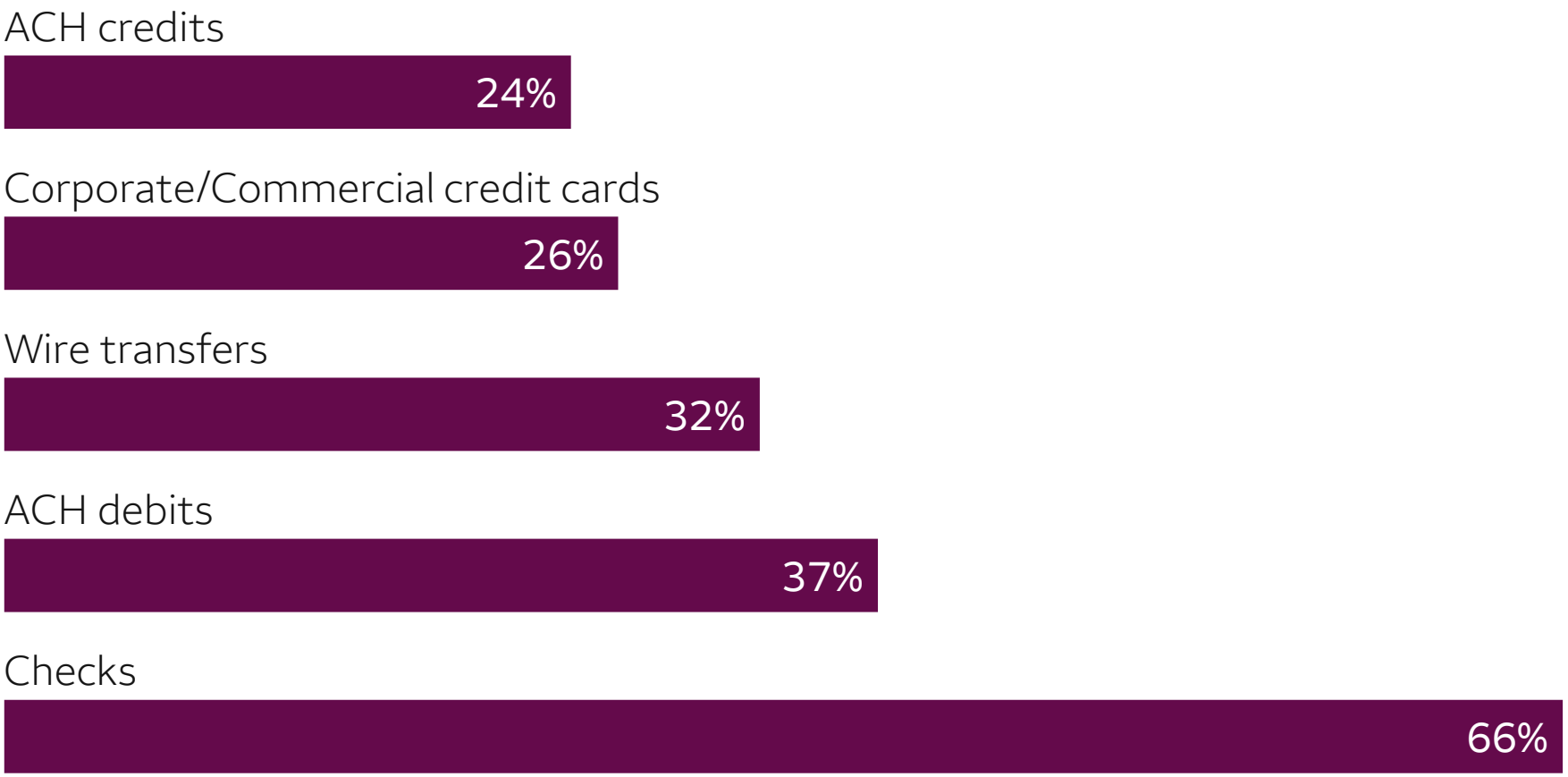
Companies of **all sizes** and **across all industries** are at risk

What are you doing to reduce your exposure?

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

Are your payments a target for fraud?

Organizations that experienced fraud in 2021 by payment type



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

Current threat landscape

Key fraud threats impacting Wholesale customer-facing digital channels

B
E
C

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.

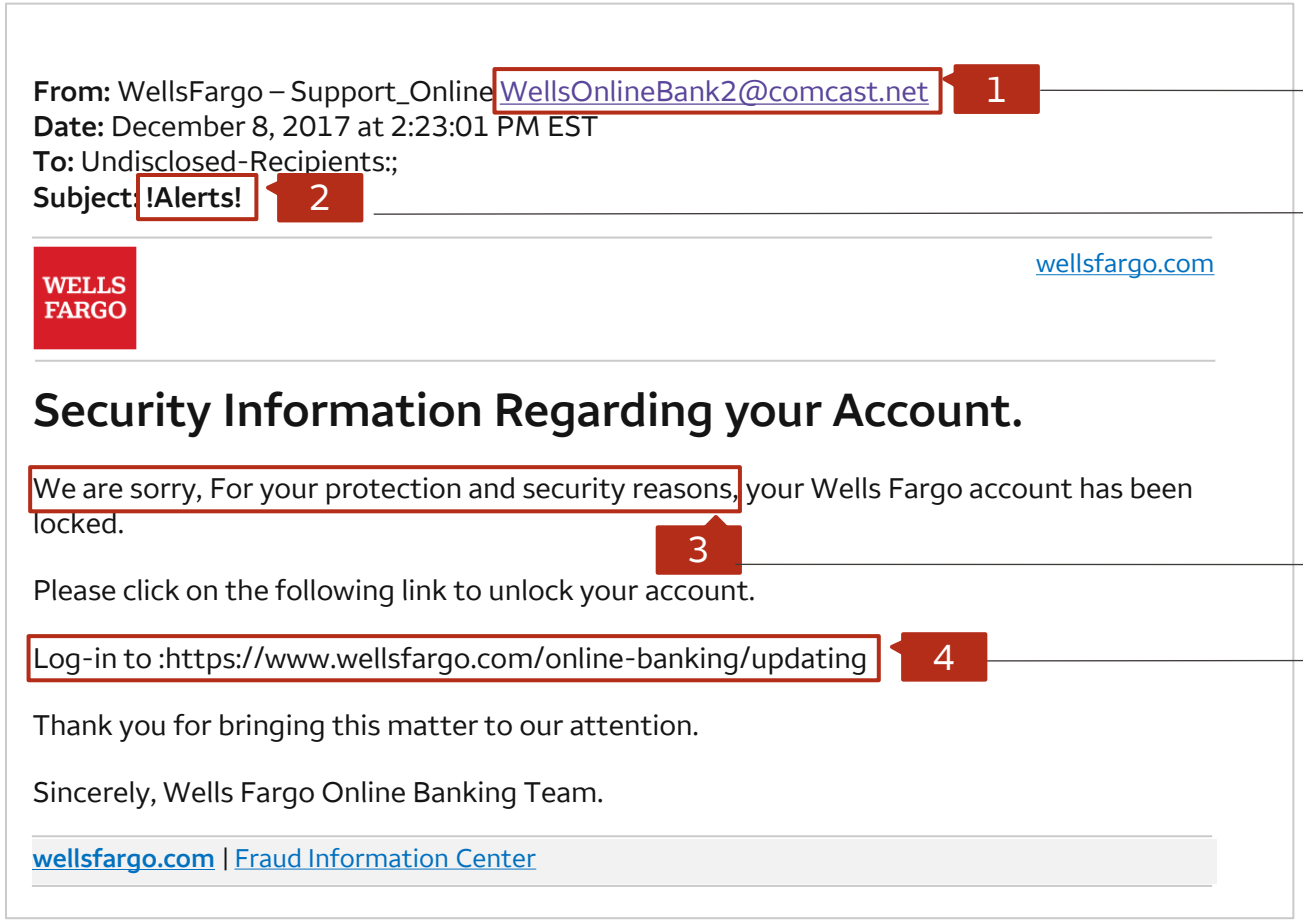
A
T
O

Online Account Takeover (ATO)

Thieves gain access to make unauthorized transactions, including transferring funds, or stealing sensitive customer information.

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.



From: WellsFargo – Support_Online WellsOnlineBank2@comcast.net 1
Date: December 8, 2017 at 2:23:01 PM EST
To: Undisclosed-Recipients:;
Subject: !Alerts! 2

WELLS FARGO

wellsfargo.com

Security Information Regarding your Account.

We are sorry, For your protection and security reasons, your Wells Fargo account has been locked. 3

Please click on the following link to unlock your account.

Log-in to :https://www.wellsfargo.com/online-banking/updating 4

Thank you for bringing this matter to our attention.

Sincerely, Wells Fargo Online Banking Team.

wellsfargo.com | Fraud Information Center

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

This is an example email only

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**

Organizations impacted by BEC

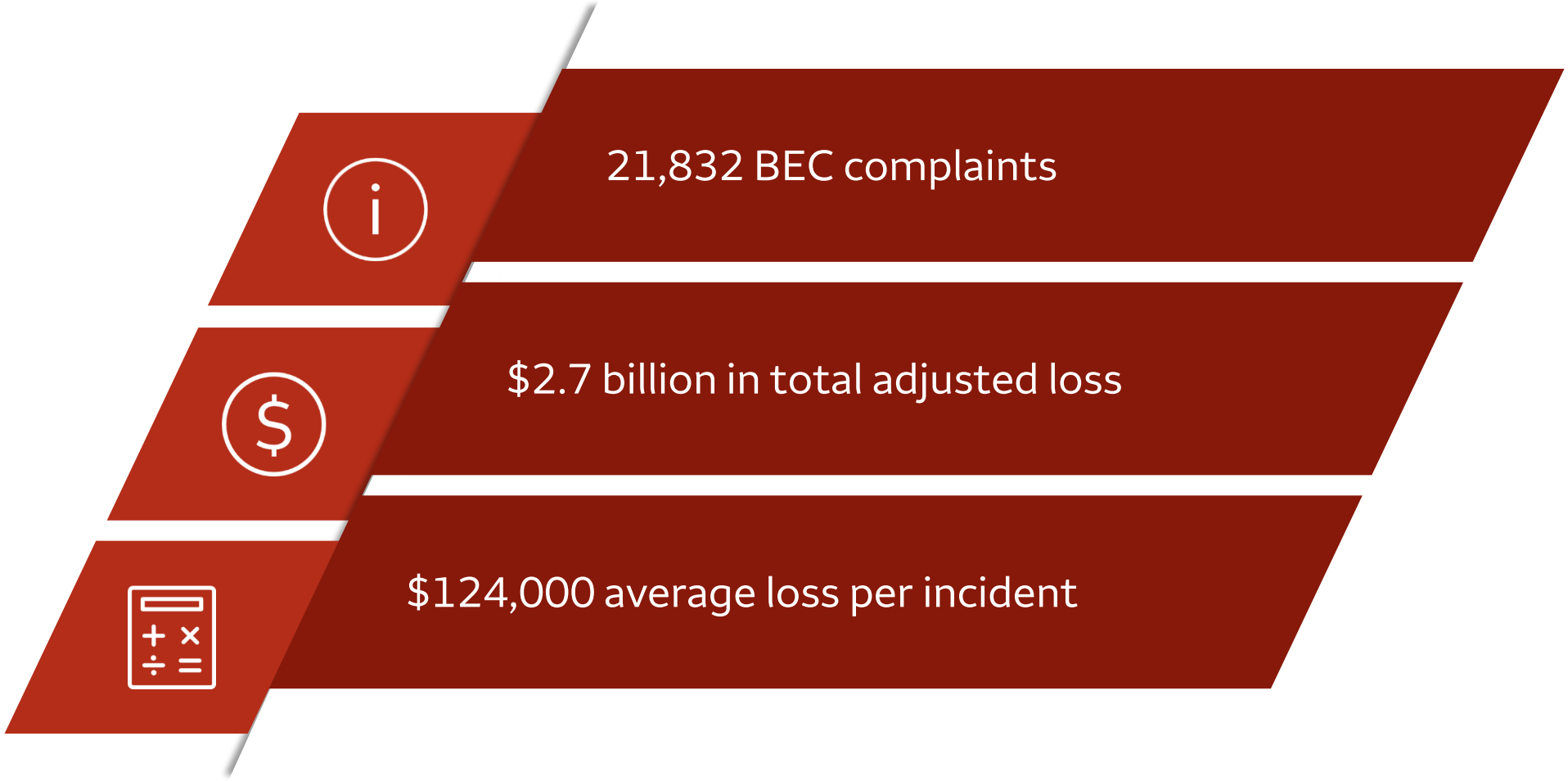
Percent of organizations experiencing actual BEC fraud

of organizations were targeted by BEC in 2021

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

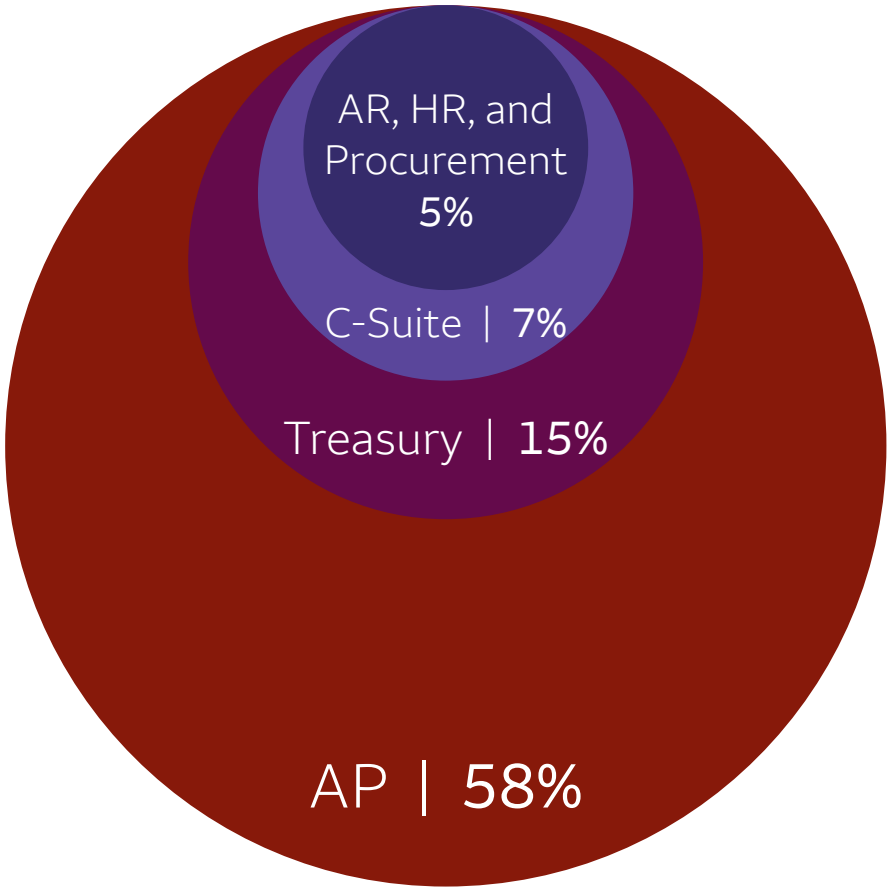
The cost of BEC

According to the FBI Internet Crime Complaint Report for 2022



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, 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 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

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

Caution

- Be wary of **unsolicited phone calls** concerning unreported system issues – Immediately contact your Wells Fargo bank representative

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

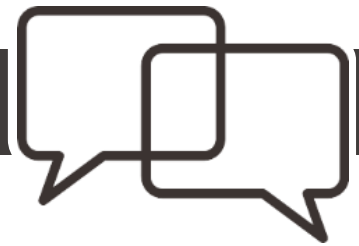
Wells Fargo fraud websites for additional fraud assets

- 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/

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.



Q&A

WELLS FARGO

Treasury Management

Thank you

Anil Khilnani
Fraud Education & Awareness
Global Treasury Management Fraud Prevention

anil.khilnani@wellsfargo.com