Global Treasury Management

WELLS FARGO

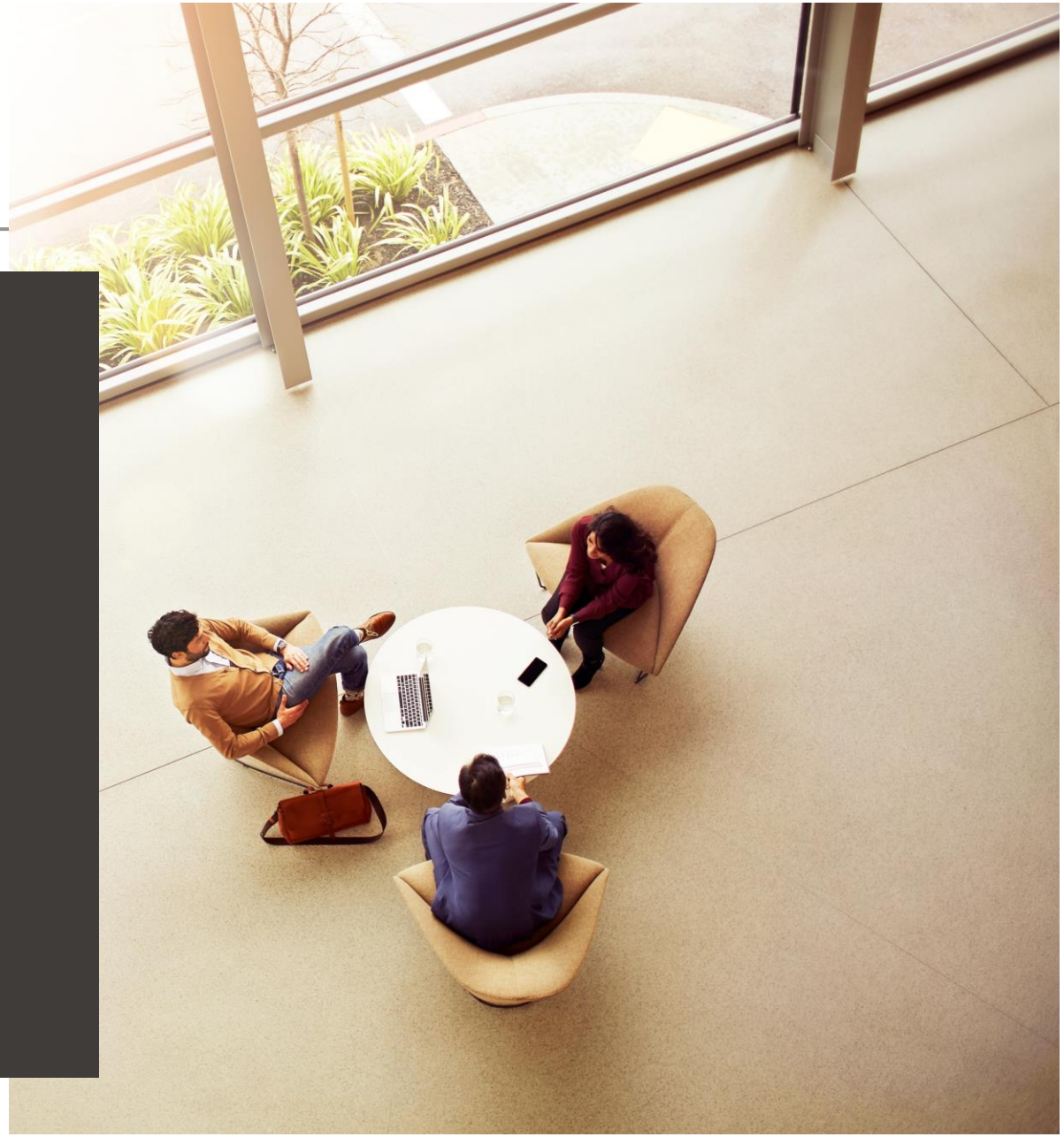
Cyber payments fraud and risk

December 2023

Anil Khilnani
Fraud Education & Awareness

Agenda

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



What are you doing to reduce your exposure?

4 of 5 organizations indicated fraud **threat level increased in 2022**[1]

#1 complaint reported to FBI's IC3 in 2022 was **phishing** (300,497 complaints) [4]

9 of 10 companies experienced a data breach caused by an **end-user mistake on email**[3]

71% of organizations targets of **Business Email Compromise** (BEC) in 2022[2]

73% of organizations who experienced BEC, did so through a **spoofed email**[2]

$2.74 billion in **losses from BEC** in 2022[4]

1. 2023 Strategic Treasurer/Bottomline Treasury Fraud & Controls Report
2. Association for Financial Professionals, 2023 AFP® Payments Fraud and Control Report
3. Tessian Research, 2022 State of Email Security Report
4. 2022 Internet Crime Complaint Center Internet Crime Annual Report

Top 5 security trends

For the next 10 years

1

Zero trust security

Emerging as a more secure model for companies to control remote access

> **"Never trust, always verify"**

Reducing reliance on passwords for authentication

2

Vendor security

44% of companies experienced a significant data breach through a third-party vendor

On average, a median size company contracts with approximately **5,000 third-party vendors**

3

Cyber skills gap

Cybersecurity workforce **needs to grow 65%** to be effective in defending critical assets as there are 400k open cybersecurity positions in the U.S.

4

Cyber attacks

In 2021, cybercrime caused **$6 trillion in damages**[a] (about $18,000 per person in the U.S.) and is **projected to grow 15% annually to $10.5 trillion by 2025**[b]

Attacks increased **600%** during the pandemic[c]

5

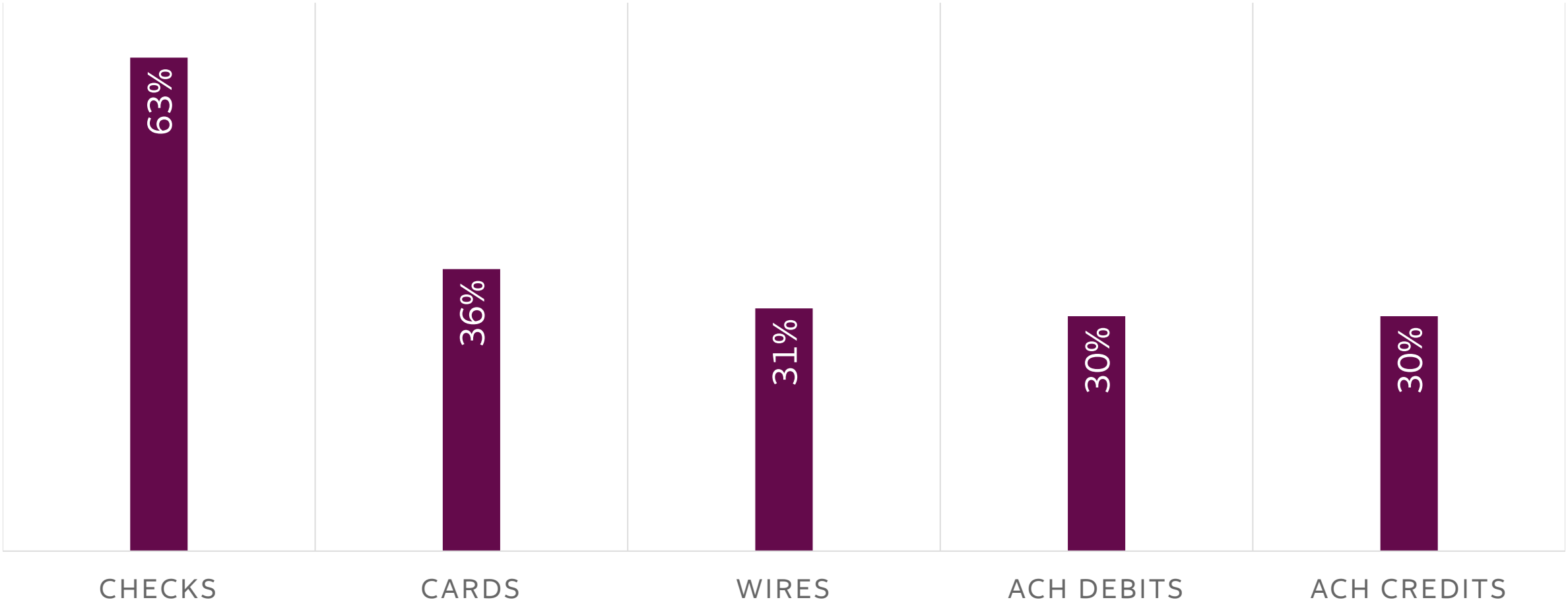
AI-driven threats

AI technology (e.g., ChatGPT) being **used to automate individual interactions** and other cyber fraud attacks at a **cheap and scalable** rate, which could increase the size, scale and speed of cyber threats

1. 7 Facts About the Zero Trust Security Model (redriver.com)
2. Can closing the cybersecurity skills gap change the world? | World Economic Forum (weforum.org)
3. Cyber attacks:
   a) 119 Impressive Cybersecurity Statistics: 2021/2022 Data & Market Analysis - Financesonline.com
   b) Cybercrime To Cost The World $10.5 Trillion Annually By 2025 (cybersecurityventures.com)
   c) https://www.businessinsider.com/top-un-official-warned-of-cybercrime-spike-during-pandemic-2020-5

Are your payments a target for fraud?

Percent of organizations that experienced fraud in 2022 by payment type



Source: Association for Financial Professionals, 2023 AFP® Payments Fraud and Control Reports

Current threat landscape

Key fraud threats impacting wholesale customer-facing digital channels

B
E
C

Business email compromise (BEC) aka imposter fraud

Fraudsters impersonate a vendor, company executive, or another trusted trading partner — ultimately tricking you into making the payment to them.

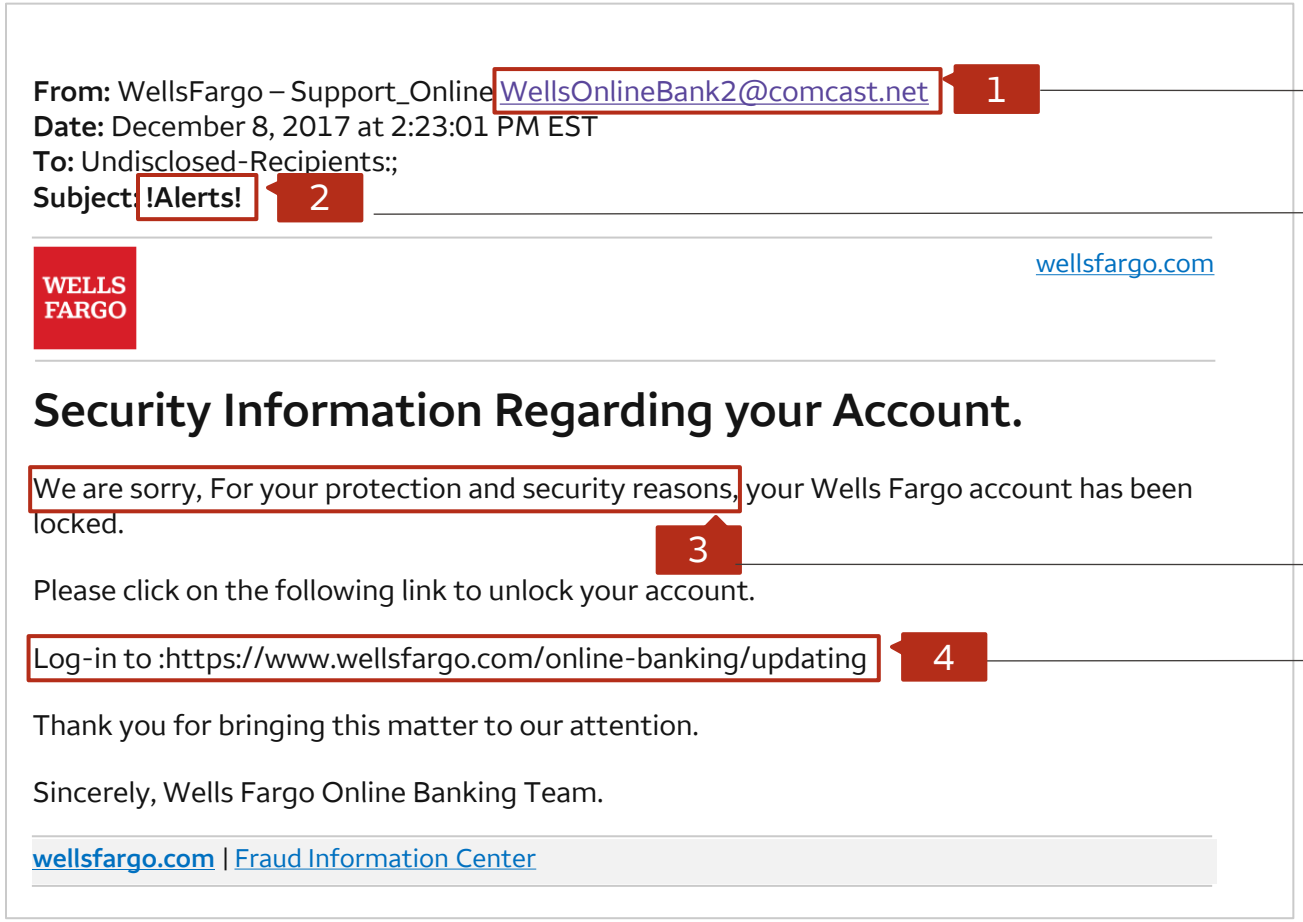
A
T
O

Online account takeover (ATO)

Thieves gain access to make unauthorized transactions by stealing banking portal log-in credentials.

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

This is an example email only

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

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

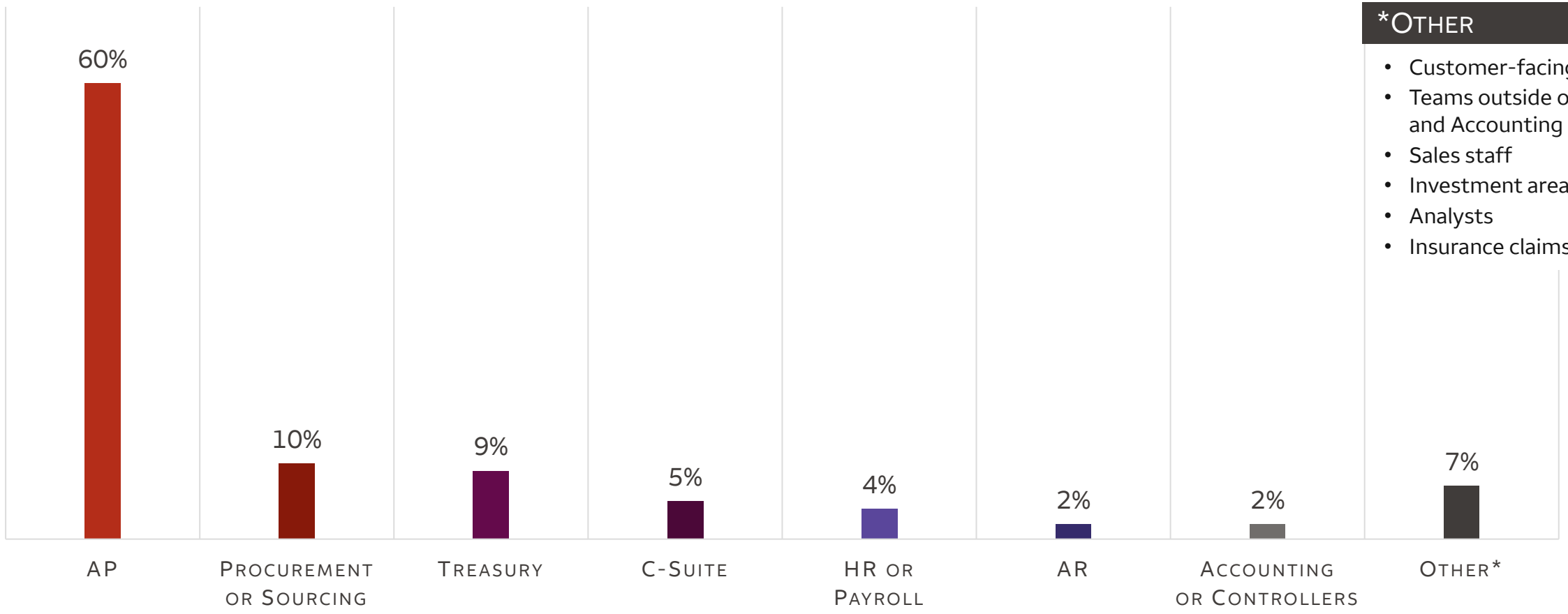
- Attempts **appear legitimate** at first

Types of imposter fraud

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

Departments most vulnerable to BEC fraud

Percentage of organizations impacted **by department targeted in 2022**



***Other**

- Customer-facing teams
- Teams outside of Finance and Accounting
- Sales staff
- Investment area
- Analysts
- Insurance claims

Source: Association for Financial Professionals, 2023 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
your accounts

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

Account takeover (ATO)

Theft of confidential information to access online accounts directly

Fraudsters typically leverage **social engineering** and **malware** to execute an account takeover incident

Social engineering

For example, **phishing**, manipulates you into divulging confidential information

Malware

Malicious software installed on your computer without your consent or knowledge and 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 they're from a trusted sender

Do

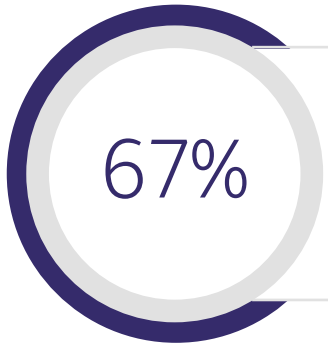
- **Use notification and alert services** to receive text or email notifications regarding electronic debits from your accounts
- Implement **dual custody**
- Use **multi-factor authentication**, or at least two-factor authentication, for access to your company networks and for payments initiation
- 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

Education and awareness to help mitigate the risk

The **data**



of companies **require annual security training** for employees involved in payments.[1]

Employees must be right **100%** of the time, while threat actors need to be right **only once** – and they know this.[2]

The **actions**

Educate your entire staff

- **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

1. 2023 Treasury Perspectives Survey Report, Strategic Treasurer
2. Abnormal Security H1 2023 Email Threat Report

Resources for additional fraud protection information

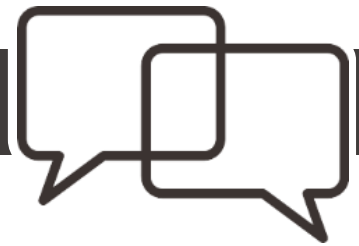
Wells Fargo websites

- Treasury Insights
  https://www.wellsfargo.com/com/insights/treasury-insights/
- Wellsfargo.com Fraud & Security 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

Global Treasury Management

WELLS FARGO

Thank you

Anil Khilnani
Vice President, Fraud Education & Awareness
Global Treasury Management Fraud Prevention