Internal Controls and Fraud Prevention – Protecting what is most important to you

October 16, 2023

Dennis Locke, Finance Director, City of Spartanburg

Brent Weaver, Relationship Manager, Wells Fargo Bank

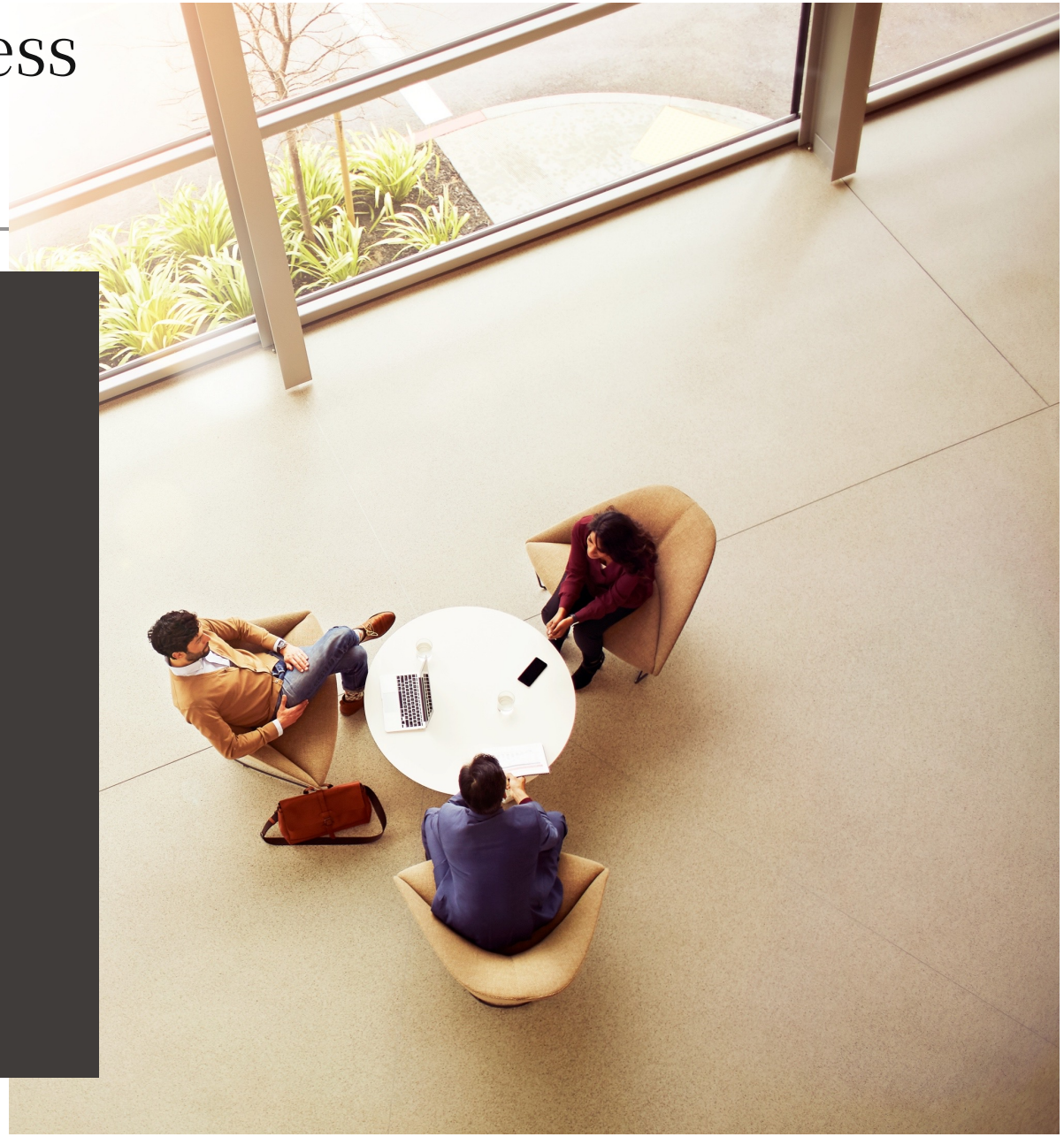
Internal Controls

- Municipal Checklist For Internal Controls

- General Controls
- Controls over Financial Records
- Controls over Cash
- Controls over Purchasing & Disbursements
- Controls over Information Systems

Fraud Prevention/Awareness Agenda

- Current fraud landscape
- New and evolving threats
- Business email compromise
- Account takeover
- Critical strategies your organization needs for fraud protection
- Tips for creating a strong password
- 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]

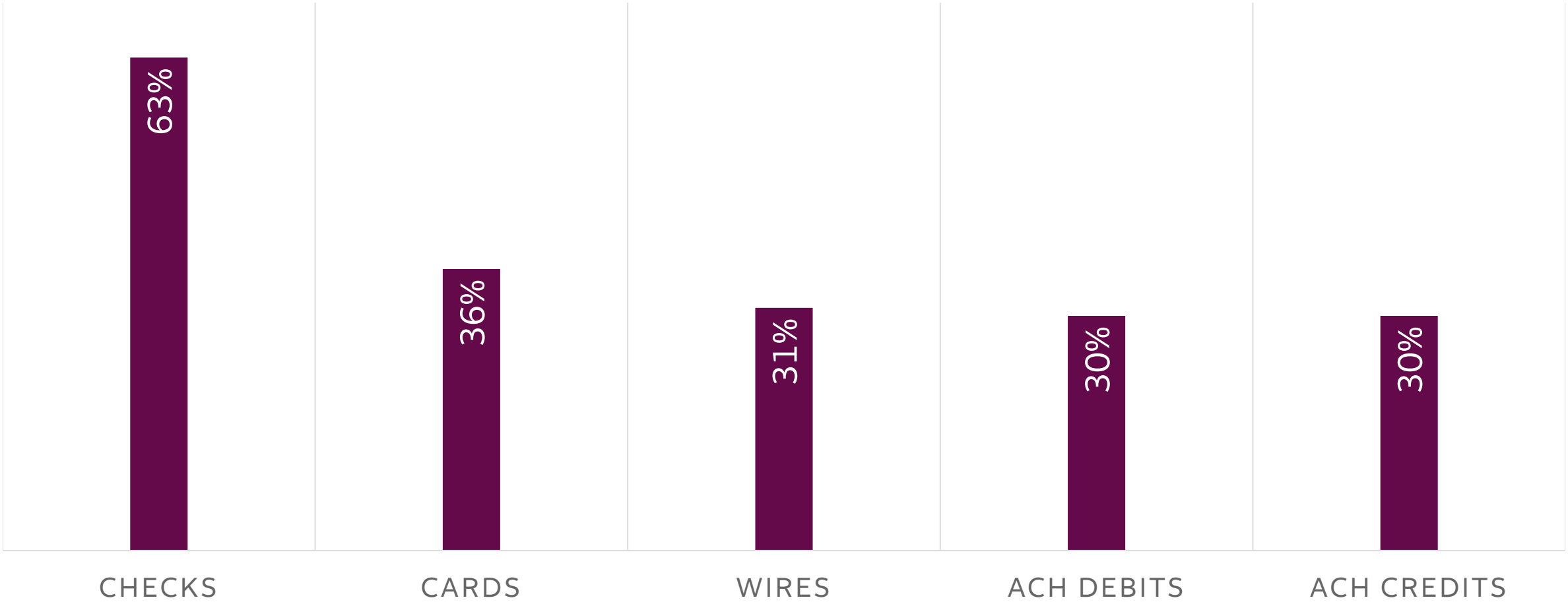
73% of organizations who experienced BEC, did so through a **spoofed email**[2]

$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

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.

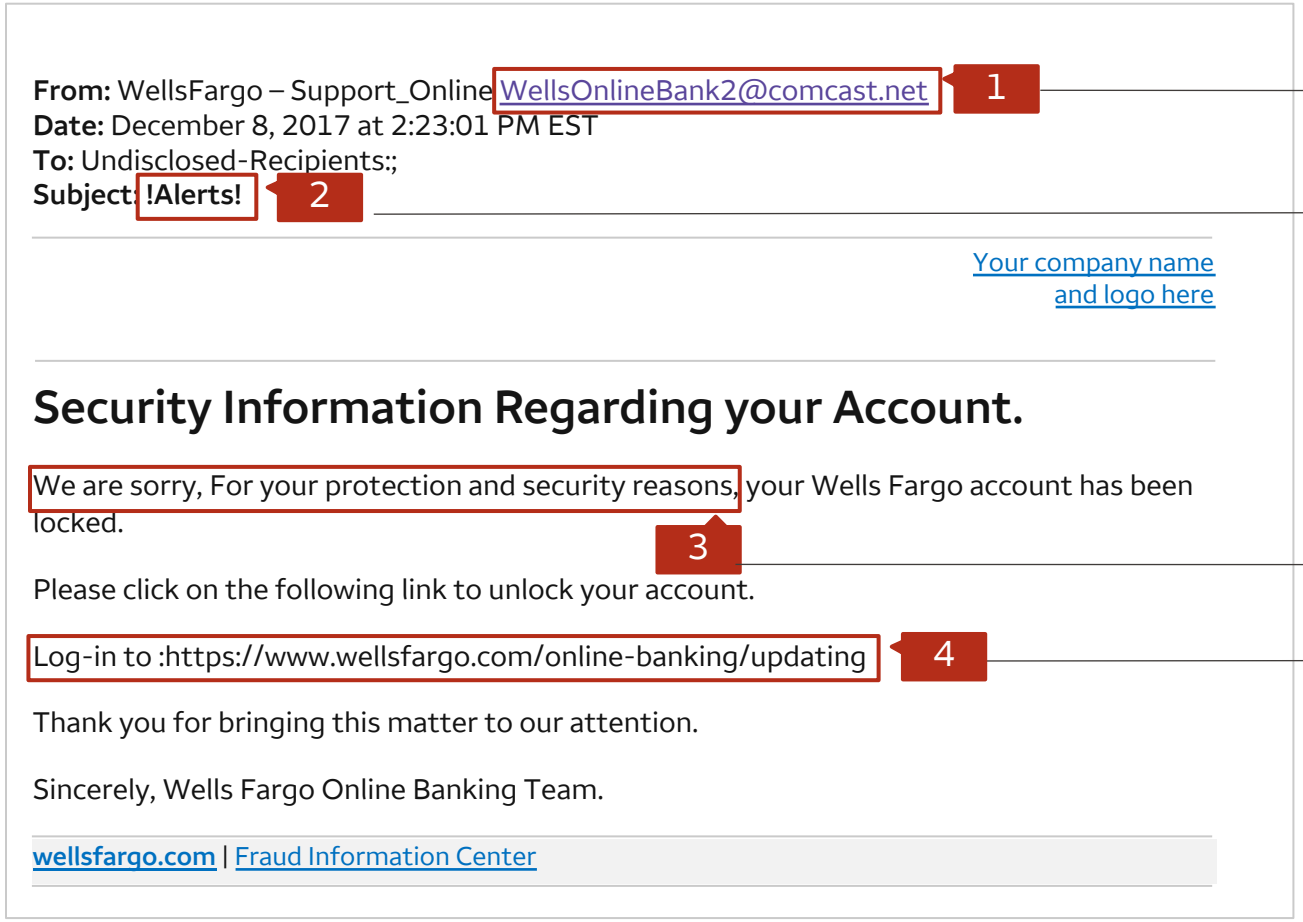
A
T
O

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

Your company name and logo here

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

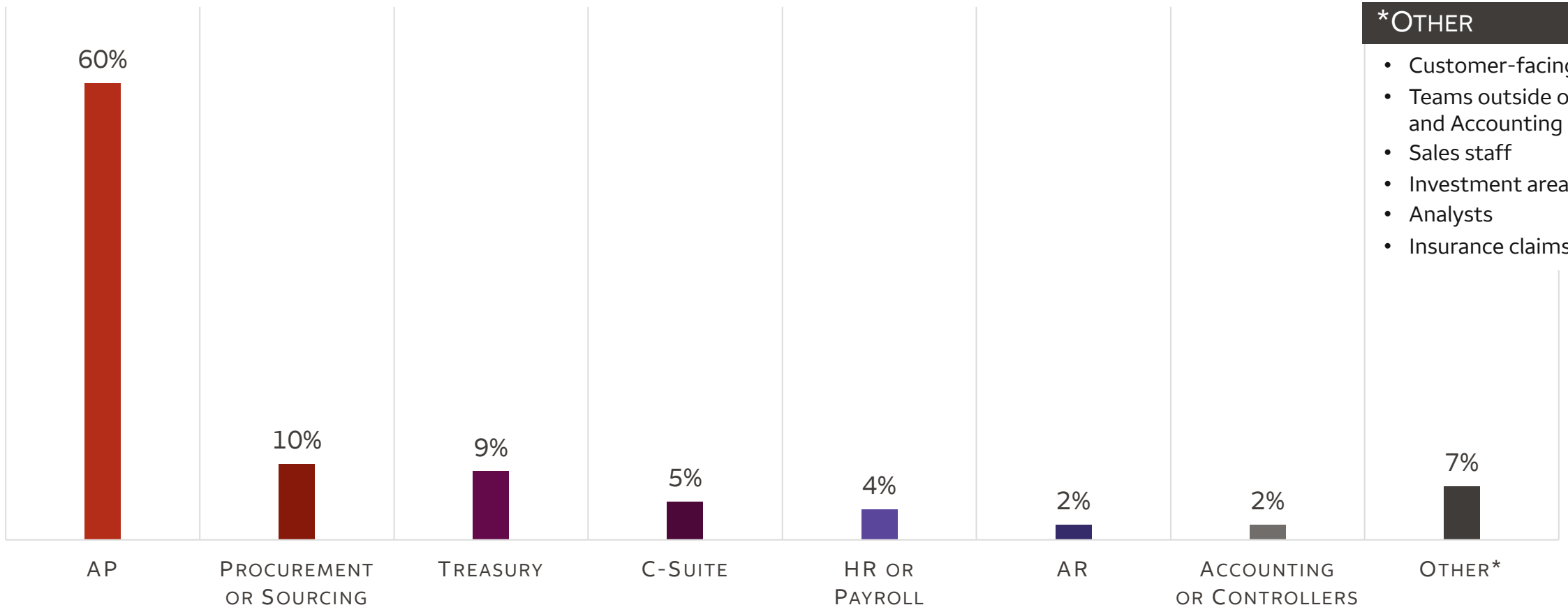
- Attempts **appear legitimate** at first

Types of imposter fraud

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

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

Critical strategies for strengthening your defenses

01

Consider **your needs**

One size does not always fit all

Integrate your security measures to reflect your organization's priorities

02

Consider **your actions**

Be prepared and ready

Have an actionable plan in place to respond in case of a fraud attack

03

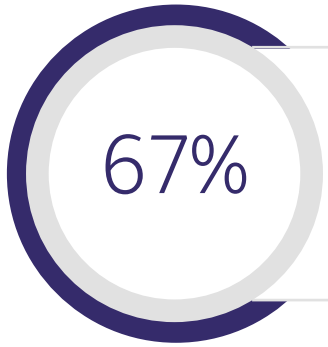
Consider **your options**

Small but mighty

Simple processes can be some of your most powerful safeguards

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

Suspect payment fraud? Here's what to do next.

Fraud action items

If you suspect fraud with an electronic payment you've sent, immediately notify the following:

- Your dedicated client service officer
- Global Treasury Management Service at **1-800-AT-WELLS** (1-800-289-3557)
- Your relationship manager

Note: Fraud recovery efforts are extremely time-sensitive and are not guaranteed – the faster you let us know, the better your chances of recovery.

You should also file a report with one or more of the following resources for assistance with the fraud:

- FBI Internet Crime Complaint Center website (ic3.gov)
- Local FBI field office
- Local police department

Suggestions

- Notify your own IT and risk management teams of the incident – so they can take any necessary remediation measures – including identifying other compromised users within your organization.
- Review all recent payments to find other potential fraudulent transactions that may have been processed.
- Analyze the incident to identify any potential gaps in your processes – to determine if additional internal fraud controls or employee training are needed.

Note: We encourage you to report all fraud attempts you experience to Wells Fargo – even attempts you were able to stop – that information can be helpful for us to prevent future fraud.

Fraud recovery process and updates

- Recovery time frames vary among banks and can take up to 90 business days or longer, depending on the Receiving Depository Financial Institution (RDFI).
- Your assistance with supplying all relevant information promptly, including any required documentation, helps expedite the recovery effort.
- Wells Fargo actively engages with RDFIs on all fraud recoveries. We're dependent on the RDFI and their investigation processes, including frequency of updates.
- As we receive information from the RDFI, we will relay it to you (if not restricted by privacy regulations).
- Your client service officer or your relationship manager are your primary points of contact for updates on fraud investigations and recoveries.

5 tips for creating a strong password

- Make it unique
- Go long
- Mix things up
- Be unpredictable
- Create a passphrase

Resources for additional fraud protection information

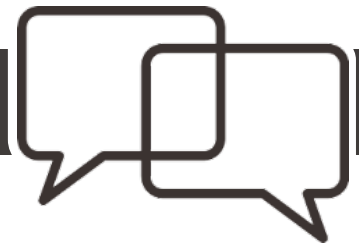
Wells Fargo websites

- 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