WELLS FARGO

Treasury Management

Fraud insights and prevention

September 23, 2021

Lynn Nieves, SVP, Treasury Management Consultant
Jackie Kobialko, SVP, Treasury Management Consultant
Peter Pulos, SVP, Treasury Management Sales Manager

© 2021 Wells Fargo & Company. All rights reserved.
Deposit products are offered through Wells Fargo Bank, N.A., Member FDIC. Wells Fargo Bank, N.A. is a banking affiliate of Wells Fargo & Company.

Today's presenters

Lynn Nieves, MBA, CTP
Senior Vice President
Treasury Management Consultant
Global Treasury Management
Government Banking

Lynn has been in Treasury Management serving Government entities for over 25 years, with the last 13 at Wells Fargo, covering West Central and Northern Florida. She is a graduate of the University of Central Florida where she received her Bachelors and Masters degrees.

Jackie Kobialko
Senior Vice President
Treasury Management Consultant
Global Treasury Management
Government Banking

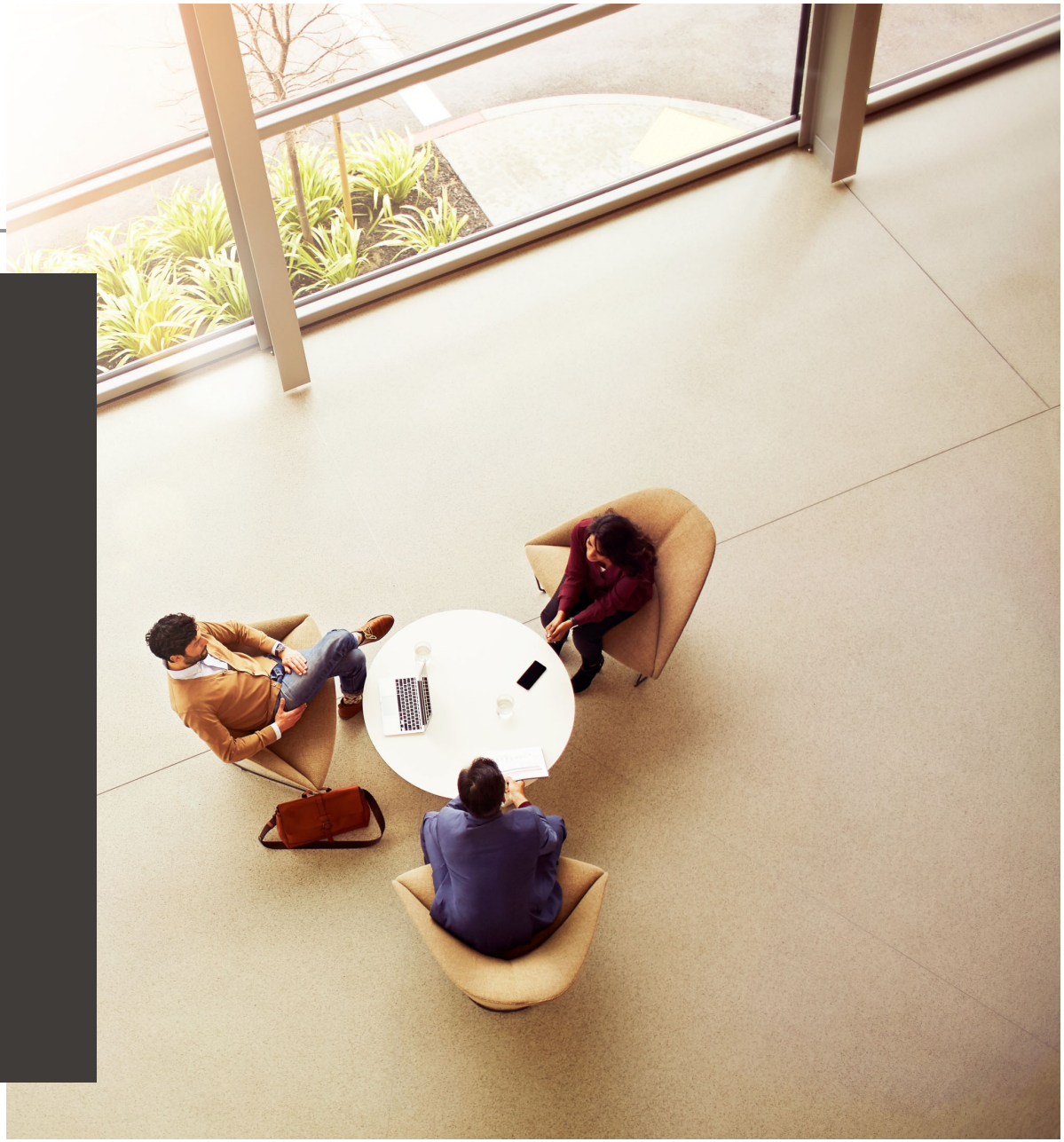
Jackie has been in the Governmental Finance industry for 28 years, with the last 16 at Wells Fargo and 14 of those years dedicated to Treasury Management in the Government Banking segment, covering the eastern and southern coastal areas of the State of Florida.

Peter Pulos
Senior Vice President
Regional Manager
Global Treasury Management
Government Banking

Pete has the responsibility of guiding a team of treasury management consulting professionals within the Governmental sector throughout the Southeast region of the United States, along with Texas and Colorado. He assures a smooth consultative approach in treasury management product solutions and enhancements.

Agenda

- Threats in the world of fraud
- Business email compromise
- Account takeover
- Critical strategies your organization needs for fraud protection
- Fraud education resources

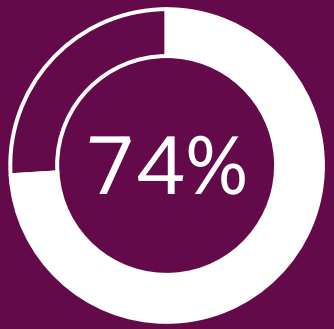


Threats in
the world of fraud

Payment fraud is growing at a record pace

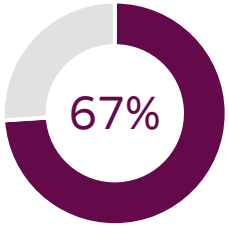
It only takes one incident for your organization to be compromised

2020 fraud statistics

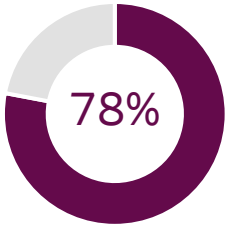


of organizations faced attempted or actual **payments fraud**

Companies of **all sizes** are at risk



annual revenue less than $1B



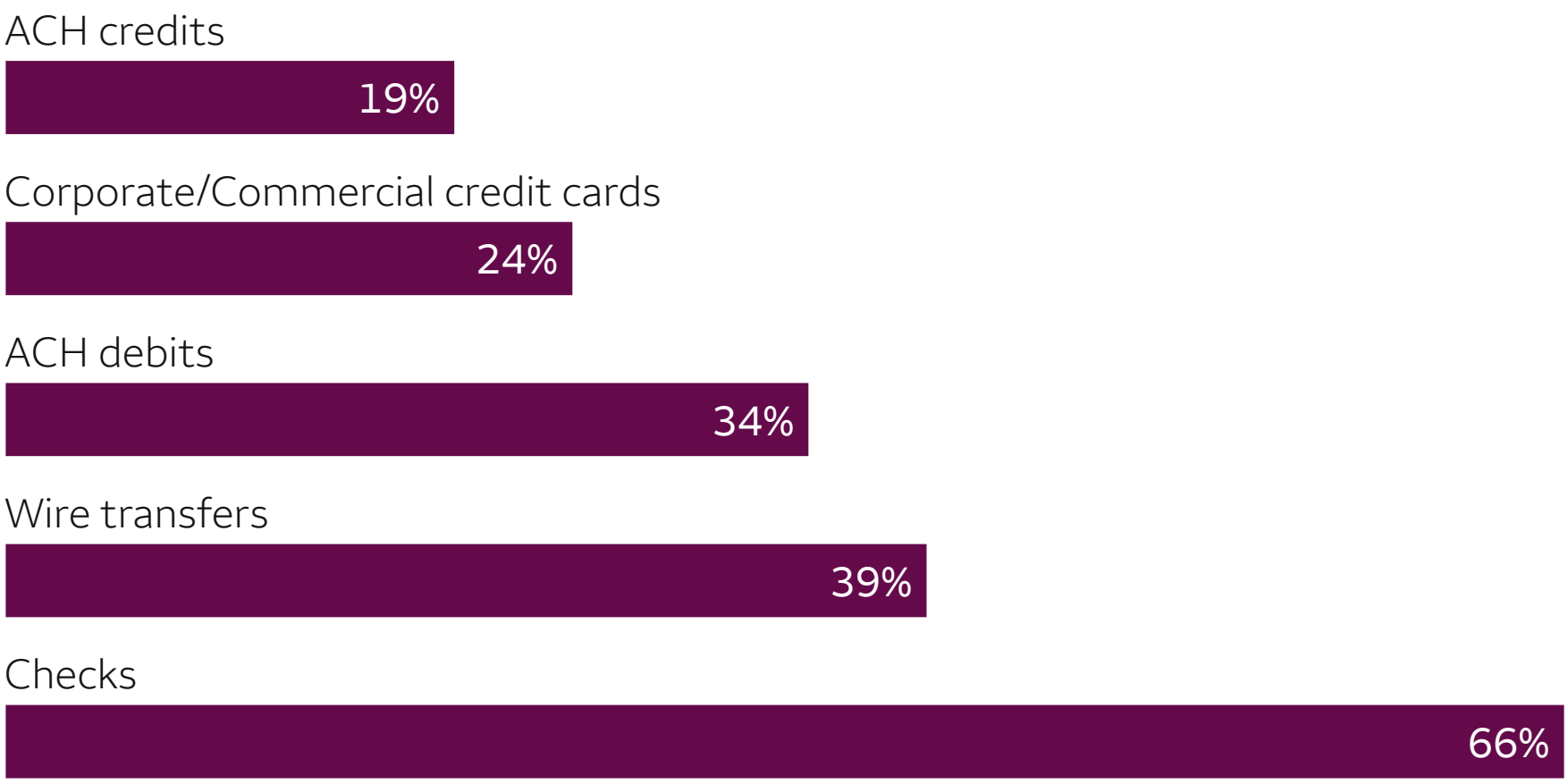
annual revenue at least $1B

What are you doing to reduce your exposure?

Source: Association for Financial Professionals, 2021 AFP Payments Fraud and Control Survey

Are your payments a target for fraud?

Organizations that experienced fraud in 2020 by payment type



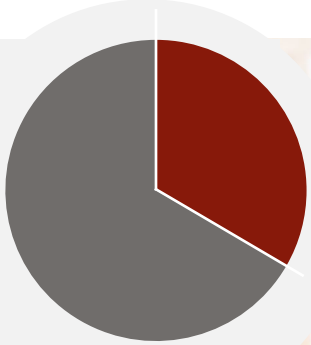
Source: Association for Financial Professionals, 2021 AFP Payments Fraud and Control Survey

Your approach matters

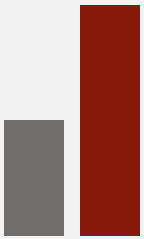
In 2020, nearly

1/3 of fraud

reported was from a lack of internal controls



Small businesses fraud risks are



2-4x higher

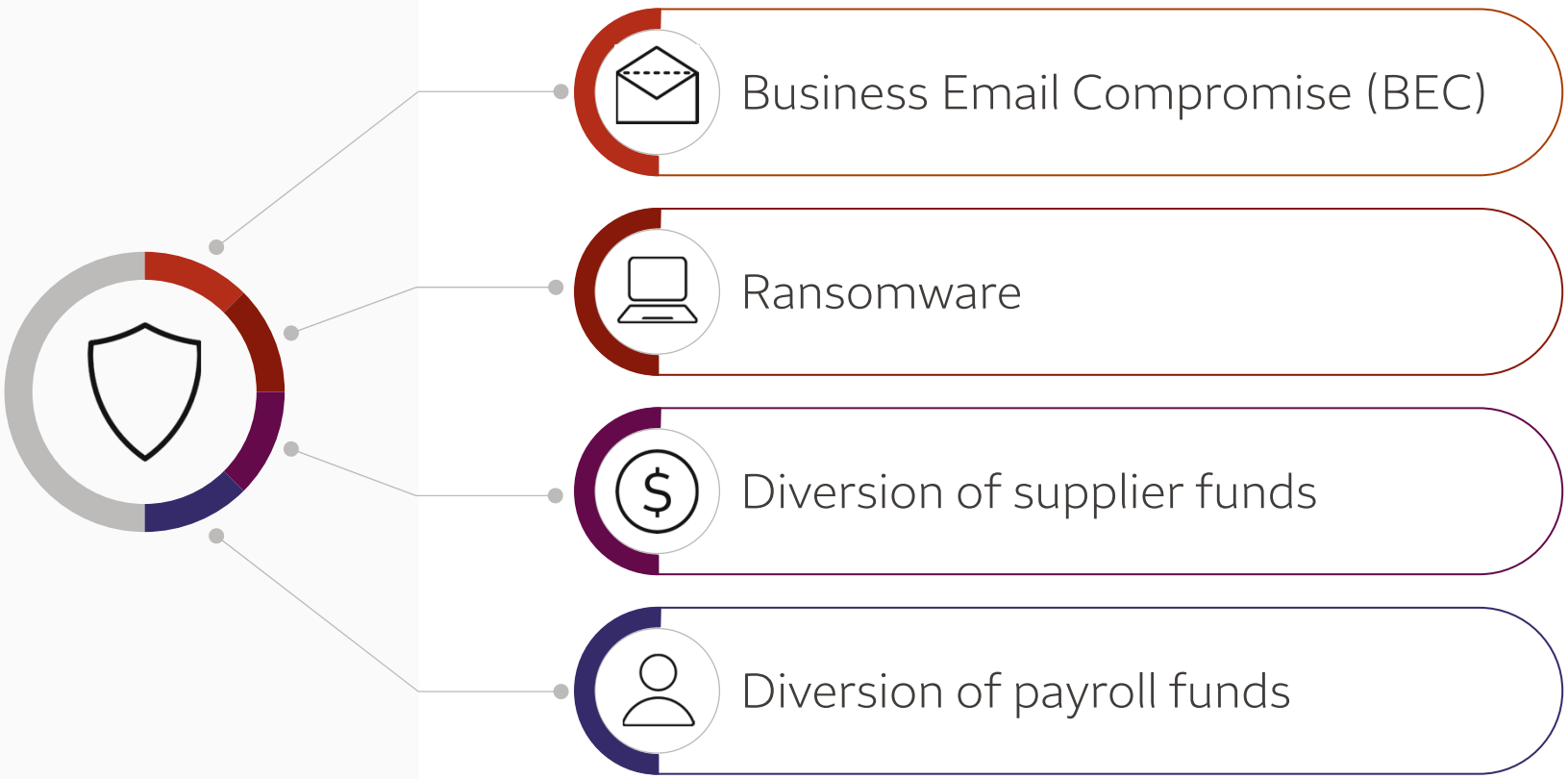
for billing, payroll, and payment tampering

Source: Association of Certified Fraud Examiners (ACFE)
Report to the Nations® 2020 Global Study on Occupational Fraud and Abuse

Your fraud strategy can help reduce your risk

Fraud attacks: the schemes that **stand out**

What is trending?



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, creating and adding fake employees to payroll, and stealing sensitive customer information.

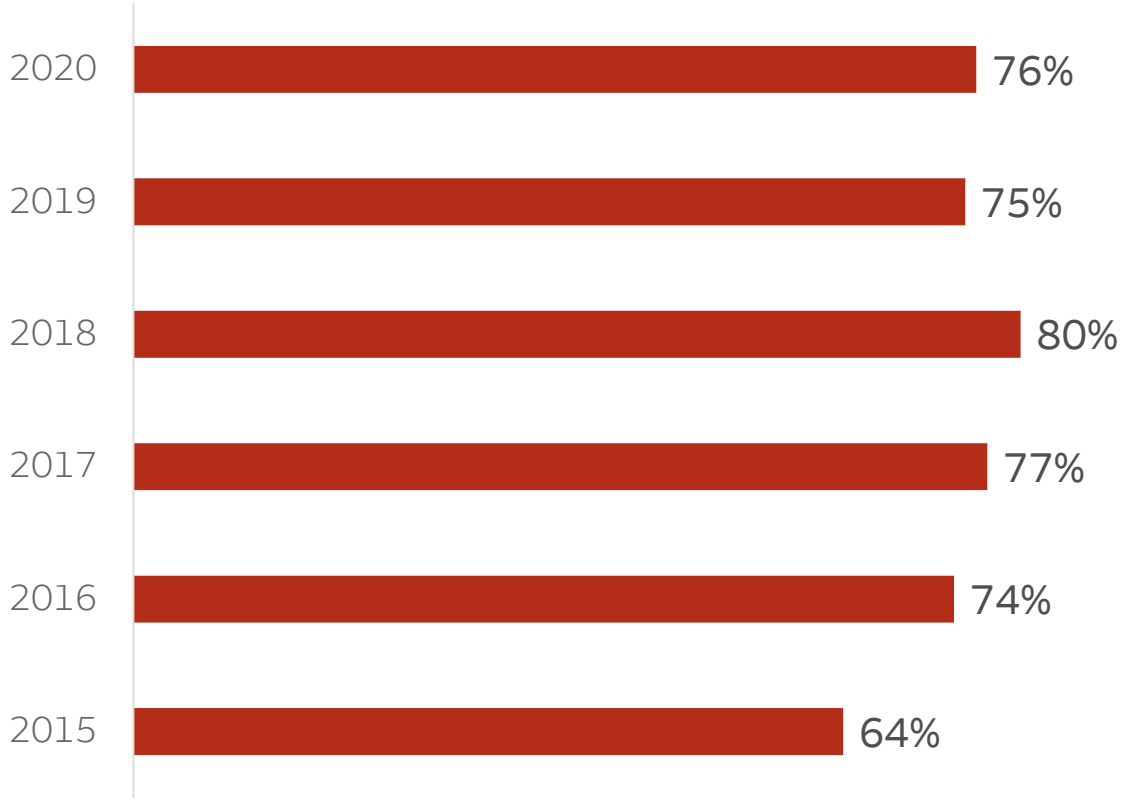
Business email compromise

Sophisticated fraudsters + time and patience = **significant losses**

- Attempts appear legitimate at first
- Attacks are timed during vulnerable organization transitions
- Keeping good data and records can help

Organizations impacted by BEC

Percent of organizations experiencing actual BEC fraud



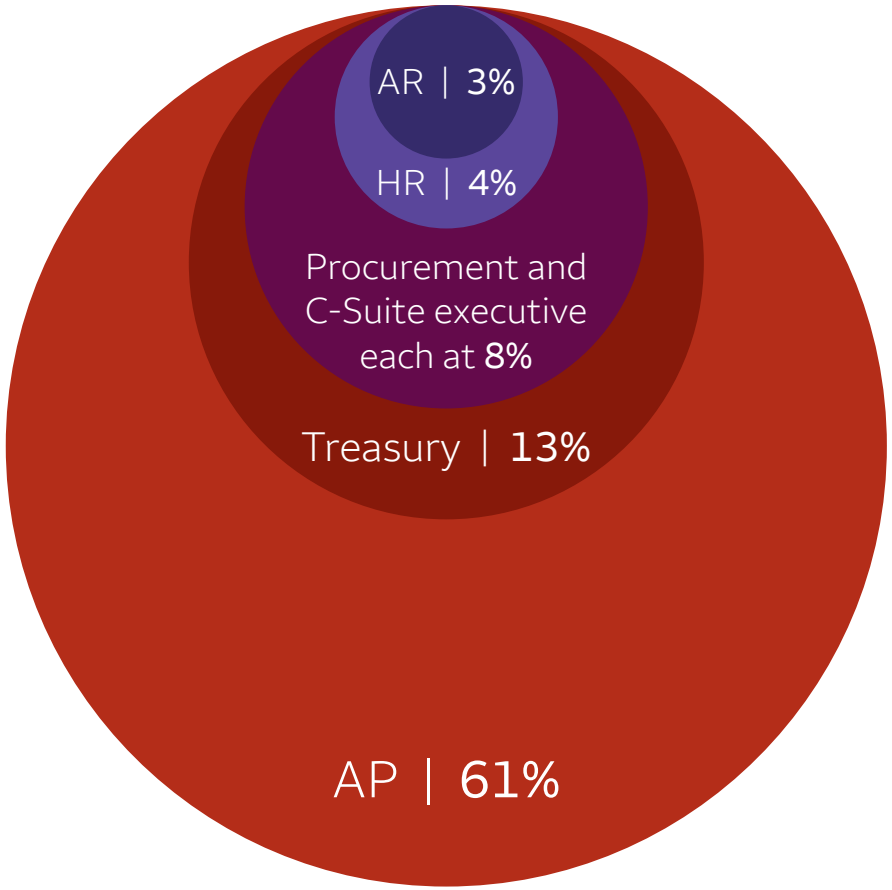
76%

of organizations were targeted by BEC in 2020

Source: Association for Financial Professionals, 2021 AFP Payments Fraud and Control Survey

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, 2021 AFP Payments Fraud and Control Survey

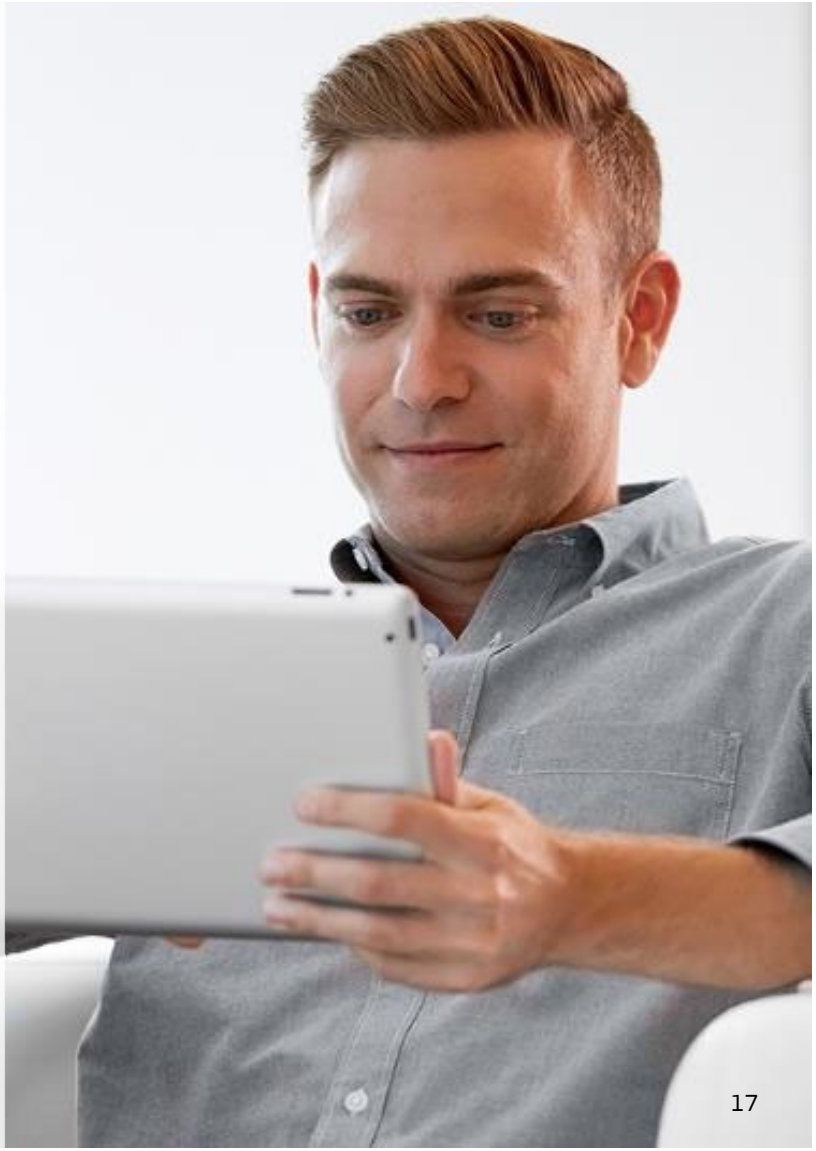
Account takeover

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**

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**



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

Steps to help protect against ATO fraud

Best practices

- 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
- Be wary of unsolicited phone calls concerning unreported system issues. Immediately contact your Wells Fargo bank representative
- Use notification and alert services to receive text or email notifications regarding electronic debits from your accounts

Implement dual custody

- Requires two users, on different devices, to initiate and approve online payments, payment instruction changes and administrative changes
- Verify payment changes with requestor before initiating a request
- Review payment details, and note changes from the information you have on file
- Confirm any changes are verified before approving a payment – Approvers must verify both the payment and payment instructions

Practical strategies to explore

Focus areas for potentially lowering fraud risk

Steps your organization can use to help mitigate the risk

Verbally authenticate all requests

- Requests for payment and payment instruction changes
- Use contact information on file to verify; never use contact information provided in the request

Vendor/trading partner awareness

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

Educate your entire staff

- Alert management and supply chain personnel to the threat
- Instruct all staff, especially AP staff, to question unusual payment or account requests received by email — even from executives
- Review processes and retrain your employees

Create the right atmosphere

Establish rules and outline responsibilities

Potential code of conduct items

- Be responsible
- Be accurate
- Be honest
- Encourage accountability
- Report activities that don’t seem right
- Protect confidential information

Empower your employees

Fostering the right environment promotes continued success

- Create an atmosphere that promotes trust and truthfulness
- Encourage feedback, new ideas, and candid communication
- Learn and grow with each other

Focus on education and training

According to the 2021 AFP® Payments Fraud and Control Survey

76%

Of organizations were targeted by BEC in 2020

77%

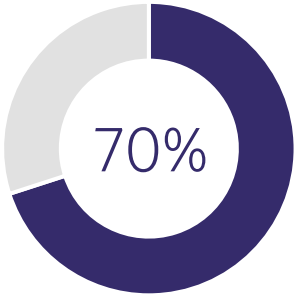
Of organizations educate on identifying BEC threats

Educate on the systems and processes in place to minimize risk

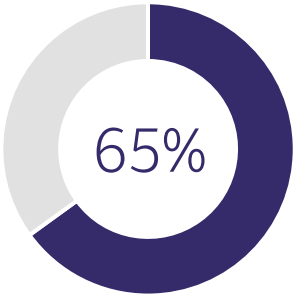
Practical payment and financial controls

74% of organizations were targets of payment scams in 2020

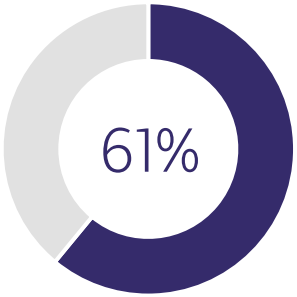
Internal measures being leveraged include:



Policies to verify changes



Confirming transfer requests



Stronger internal controls

Source: Association for Financial Professionals, 2021 AFP® Payments Fraud and Control Survey

Make fraud detection and planning part of your business' DNA

Review

and update your plan regularly

Document

your strategies for detecting fraud, including who is responsible for each task

Monitor

Knowing someone is paying attention and monitoring activity acts as a deterrent

Resources for more fraud protection information

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

Fraud checklists

- Double your protection with dual custody checklist
  https://global.wf.com/hub_infographic/double-protection-dual-custody-tm-12171/
- Triumph over account takeover checklist
  https://global.wf.com/hub_infographic/triumph-over-takeover-tm-12170/

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.

Treasury
Management

WELLS
FARGO

Thank you