Payments Fraud Trends & Prevention

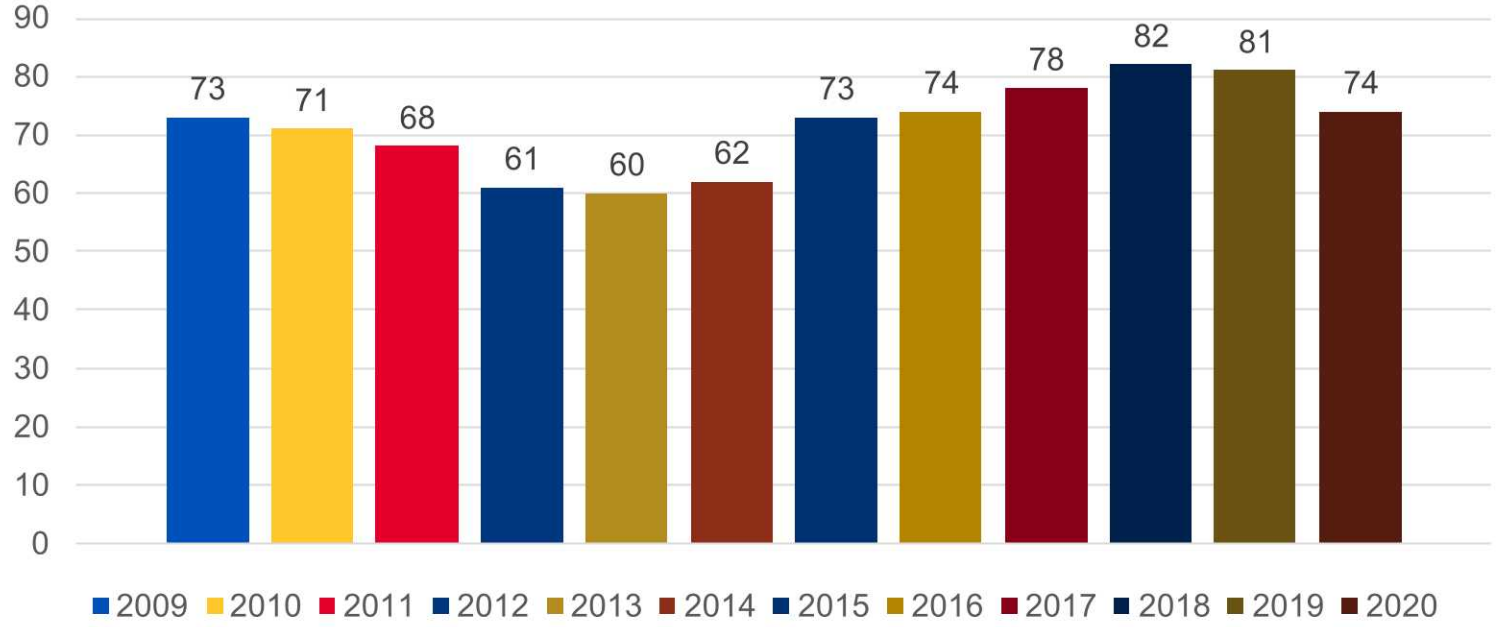
Lee Hicks, Vice President

Sr. Treasury Management Consultant

2021 AFP Payments Fraud and Control *Survey Results*

BANNER BANK

Percentage of organizations that experienced attempted and/or actual payments fraud 2009 - 2020



2021 AFP Payments Fraud and Control *Survey Results*

BANNER BANK

74% of responding organizations reported being targets of payments fraud in 2020.

Checks continue as the most targeted form of payment

Business Email Compromise (BEC) a key source of fraud in 2019 and 2020

Overall, due to the pandemic, a drop in business transactions resulted in a decrease in fraud

Employee education AND adoption of preventative measures are key to avoiding business disruption and financial loss

Business Email Compromise (BEC)

Business Email Compromise

What is it?

"An email purporting to be from a known source making a legitimate request."

Emails from a compromised/hacked email account or a spoofed email address.

Ultimately intended to implant malware, collect valuable information and/or deceive its target into disbursing funds to a fraudulent bank account.

Fraud disguised as plausible activities:

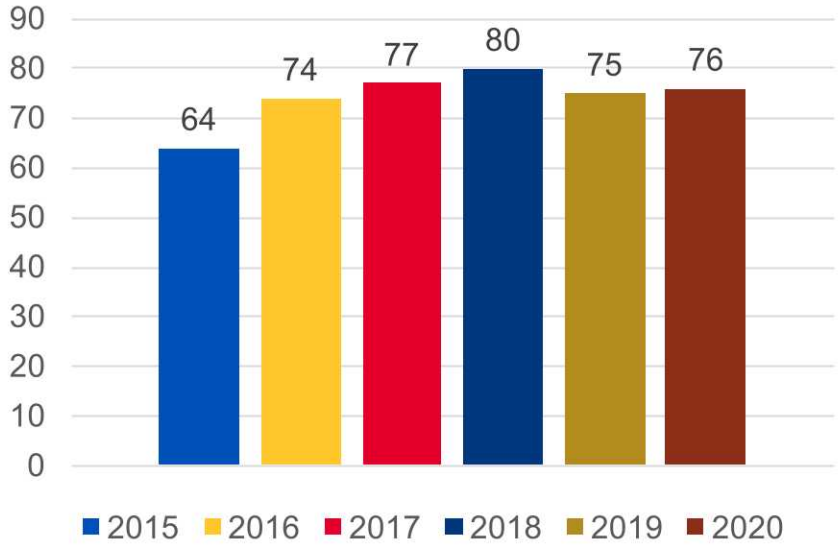
- A vendor your company regularly deals with emails you an invoice.
- Your customer wishes to pay you and initiates an email seeking your ACH or Wire instructions.
- A company owner instructs their bookkeeper to initiate a wire to a new supplier.

2021 AFP* Payments Fraud and Control Survey | www.AFPonline.org / Note: Definition acquired from The Federal Bureau of Investigation

Business Email Compromise

BANNER BANK

Percentage of Organizations that Experienced BEC



2020 Financial Impacts

Nation

- 19,369 claims reported to IC3 (FBI's Internet Crime Complaint Center)
- $1.8 billion in financial losses
- 34% of AFP survey respondents reported financial loss

Oregon

- 263 claimants
- $10,940,974 in losses

Washington

- 525 claimants
- $38,009,931 in losses

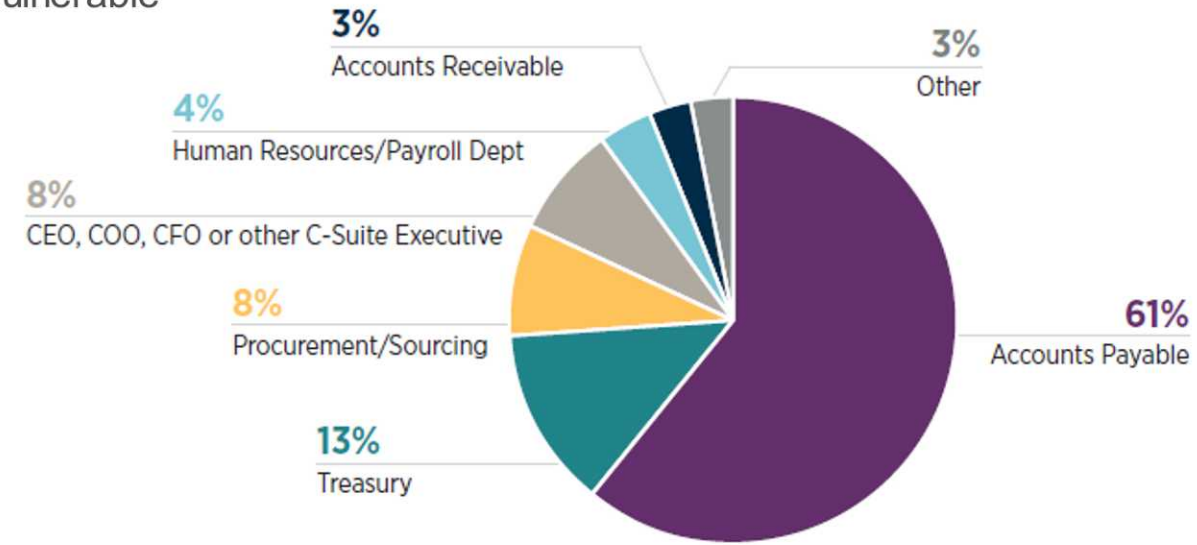
2021 AFP* Payments Fraud and Control Survey | www.AFPonline.org / IC3 2020 Internet Crime Report

Business Email Compromise

Targets within an Organization

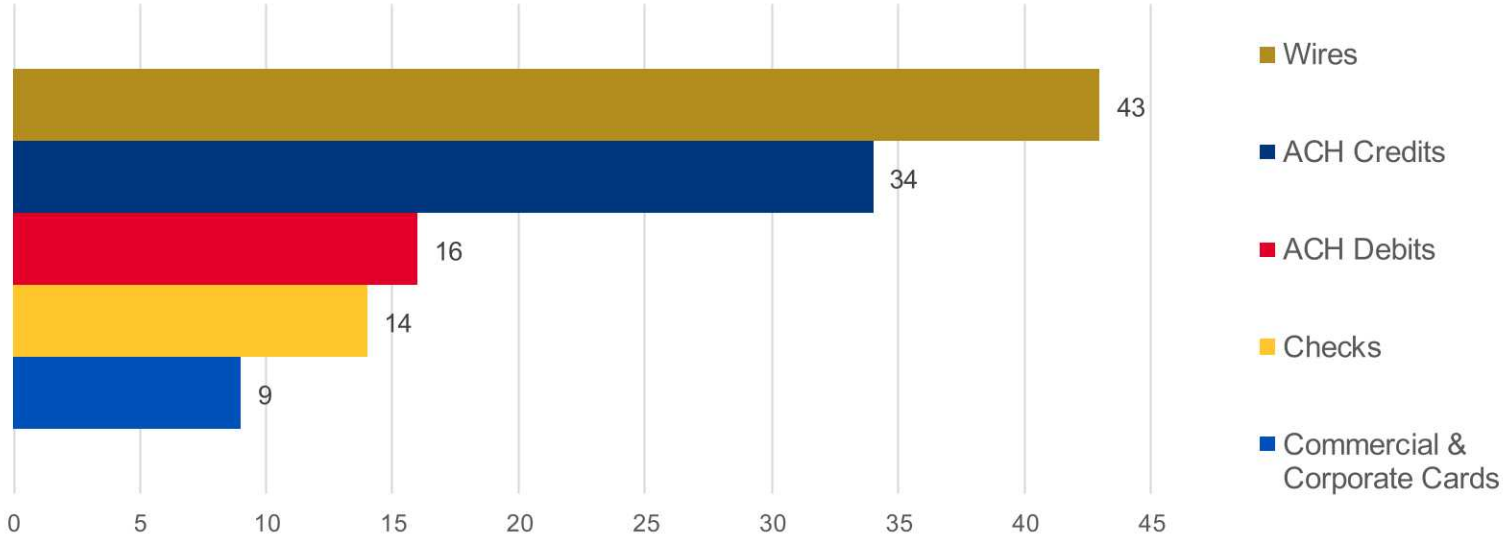
- Accounts Payable most vulnerable
- Treasury
- Procurement/Sourcing
- Executives
- HR/Payroll
- Accounts Receivable

Departments Most Vulnerable to BEC Fraud



2021 AFP Payments Fraud and Control *Survey Results*

Payment Methods Impacted by Business Email Compromise



BANNER BANK

Preventative Measures

Fraud Prevention

BANNER BANK

Reconcile accounts daily, Checks and ACH debits

Use Check and ACH Positive Pay

Rely on ACH initiation for payroll and B2B payments, reduce reliance on checks

Utilize dual user controls for ACH & Wires; one user to initiate, another to approve

NEVER initiate an ACH or wire transfer solely based on emailed instructions or an inbound call.

Phone verify (w/ *known* numbers) ALL emails requesting funds transfers and/or ANY changes to existing beneficiary account details.

Fraud Prevention

BANNER BANK

Educate your staff. Employees are the first and last line of defense. Ensure they understand they are top target of hackers.

Prevent social engineering by exercising restraint publishing employee information on company websites or social media.

Be skeptical of requests from strangers to join LinkedIn or other social networking sites.

Scrutinize all emails. Do not open unsolicited emails or click on embedded links/attachments. Notify IT.

Be wary of "internal" emails or from a "trusted source" i.e. an executive requesting secrecy or applying pressure to act with urgency

Immediately report criminal activity to your bank, local authorities and the FBI's IC3 division: https://www.ic3.gov/default.aspx

AFP Payments Security Guide Trust, But Verify: How to Stop Business Email Compromise Attacks

Top Recommendations to Prevent Fraud

#1 TIP: Educate and train your staff. ★
They are your greatest asset & weakest link!

ALSO:

- Create formal policy and procedures
- Reconcile your accounts *daily*
- Utilize Check & ACH Positive Pay
- Initiate payments via ACH when and where possible (reduce check usage)
- Implement dual-user controls for all ACH & Wire Payments
- Phone verify ALL new and/or updated payment requests
- Contact your bank and authorities immediately if you doubt any transaction or experience fraud

Resources

- Banner Bank:
https://www.bannerbank.com/financial-resources/security

- Federal Trade Commission
Start with Security: A Guide for Business | Federal Trade Commission (ftc.gov)

- Federal Bureau of Investigation
https://www.fbi.gov/investigate/cyber

- Internet Crime Complaint Center
https://www.ic3.gov/default.aspx

Questions & Answers

Important Information About This Presentation

The material appearing in this presentation, and the accompanying oral commentary, if any, by Banner Bank representatives, is for informational purposes only. Every business has unique cyber security issues and requirements that must be individually assessed.

This material does not provide legal advice. The information presented is not intended to be a substitute for professional or cyber security services. Banner Bank and its employees disclaim liability for the contents of this material and any accompanying oral presentation. The material and commentary is presented "as-is" and without warranty that it is entirely up to date or error free.

BANNER BANK

Thank you for your time.