SUMMIT 2022

ALABAMA ASSOCIATION FOR FINANCIAL PROFESSIONALS

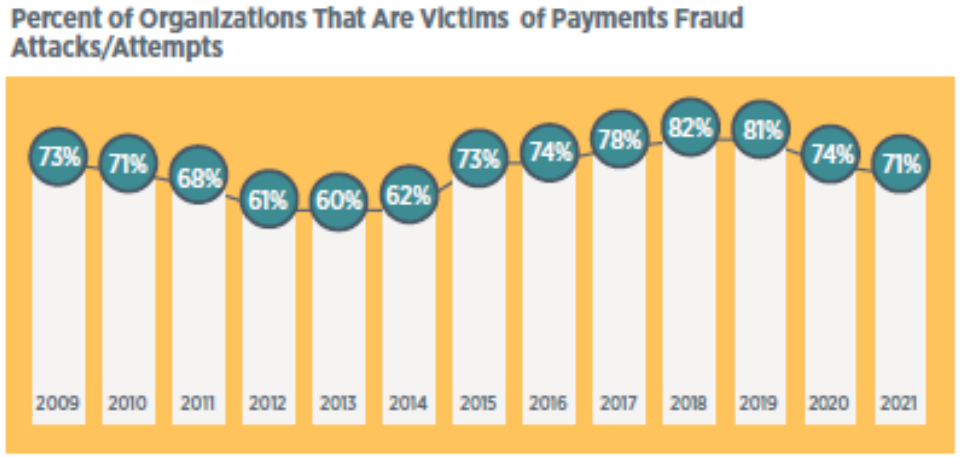
FRAUD PREVENTION PANEL

Payments, Cybersecurity & Other Scary Stuff

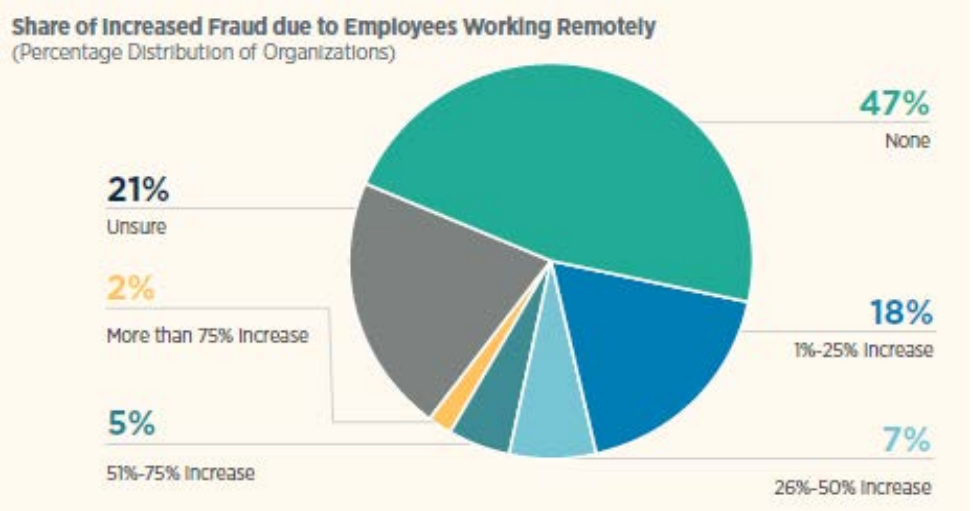
2022 AFP® Payments Fraud and Control Report

Highlights

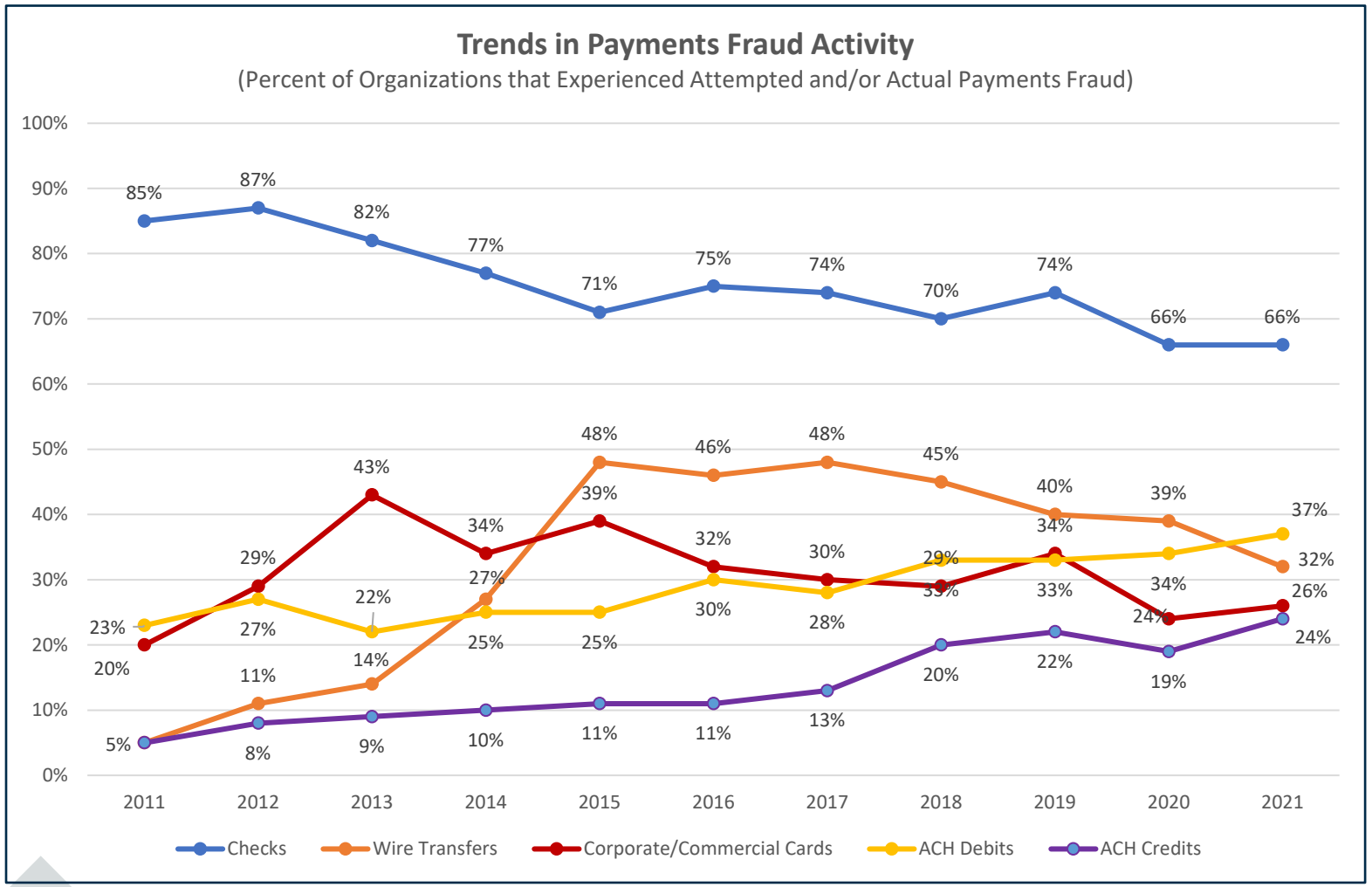
Payment Fraud and Control Survey Highlights



- Overall attacks have decreased
- Steady decline since 2018, but remains an issue
- 63% report “About the Same”
- 29% report “More”
- Remote work considered a factor for 32%



Payment Fraud and Control Survey Highlights



What examples of Payment Fraud attempts have you observed in your industry and/or experienced?

Payment Fraud Attempts

- **Business Email Compromise**

68% of companies experienced BEC (2022 AFP survey)

Targets employees with access to company finances

Directs employee to release funds to bank accounts thought to belong to trusted partners

Iterations Over Time:

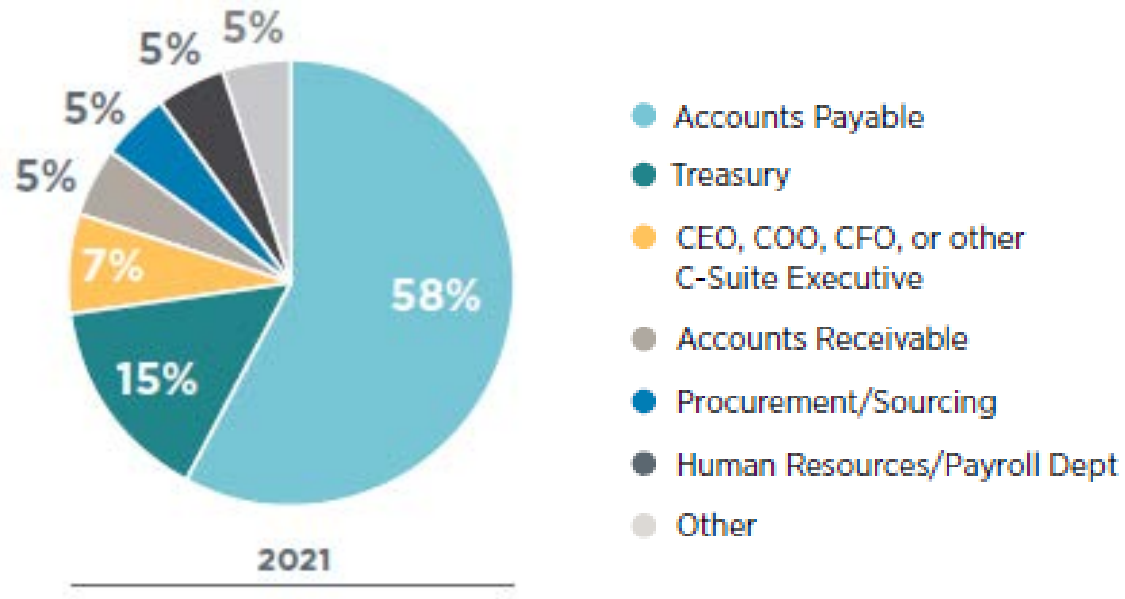
Executive email intrusion: criminal impersonates senior executive requesting payment or order to purchase gift cards

Vendor email intrusion: criminal impersonates vendor requesting the company to change payment remittance information

Employee email intrusion: criminal impersonates an employee requesting the vendor to send payment account information or requesting the company change employee's direct deposit information

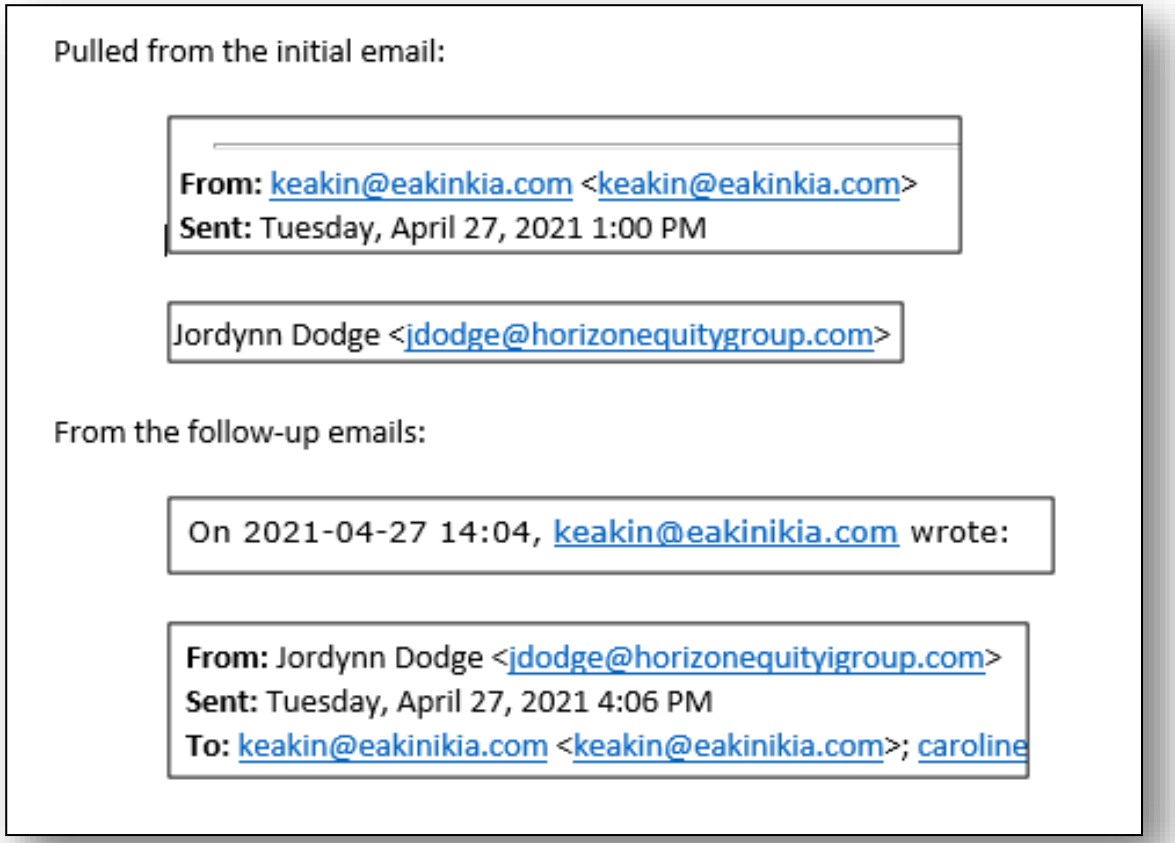
Departments Most Vulnerable to Being Targeted by BEC Fraud (Percentage Distribution of Organizations**)**

2022 AFP® Payments Fraud and Control Survey Report:



Payment Fraud Attempts

- **Business Email Compromise - Example**



Pulled from the initial email:

From: keakin@eakinkia.com <keakin@eakinkia.com>
Sent: Tuesday, April 27, 2021 1:00 PM

Jordynn Dodge <jdodge@horizonequitygroup.com>

From the follow-up emails:

On 2021-04-27 14:04, keakin@eakinikia.com wrote:

From: Jordynn Dodge <jdodge@horizonequityigroup.com>
Sent: Tuesday, April 27, 2021 4:06 PM
To: keakin@eakinikia.com <keakin@eakinikia.com>; caroline

Can you spot the differences?

Payment Fraud Attempts

- **Phishing Scheme**
  - How it works
  - Example: Shipped $58,000 materials from Alabama to Fort Worth, TX
- **Ransomware**
  - How it works
  - Example: $125,000 payment; $250,000 remediation; month of downtime; Distribution company
- **Email Hack**
  - How it works
  - Examples:
    1. $750,000 wire for property
    2. Quarterly payout
- **Vulnerabilities in Applications & Brute Force Attacks**
  - How it works
  - Examples:
    1. Fraudster infiltrating system
    2. App(s) not updated

What are some success stories you can share?

Success Stories Against Payment Fraud Attacks

- **Ransomware Attack**
  - What happened
- **Email Relay**
  - What happened
- **Security Awareness Training**
  - What happened
- **Pindrop Software**
  - What happened

What can be done to mitigate or prevent payment fraud attempts from hurting businesses?

Tactics & Tools to be Prepared Against Fraud Attacks

- **Backup and Disaster Recovery**
- **Multi-factor Authentication & Additional Internal Controls**
- **Security Awareness Training**
- **Pindrop Software**
- **GIACT, an account validation database**
- **Endpoint Detection & Response**
- **Security Incident & Event Management**
- **Security Continuity Planning**
  - Business Continuity Plans
  - Disaster Recovery Plans
  - Incident Response Plans

Any additional words of advice?

Appendix

Select Items from Dark Web Price Index 2022

PRODUCT	PRICE
Credit card details, account balance up to 5,000	$120
Stolen online banking logins, minimum 2,000 on account	$65
USA hacked credit card details with CVV	$17
50 Hacked PayPal account logins	$150
USA verified Local Bitcoins account	$120
Hacked Gmail account	$65
LinkedIn company page followers x 1000	$10
US driver's license	$150
10 million USA email addresses	$120
Malware, USA high-quality, per 1,000 installs	$1,700
DDOS (Distributed Denial of Service) attack - Unprotected website, 10-50k requests per second, 1 hour	$10

Source: PrivacyAffairs.com
Prices valid as of June 2022

Call Back Control

If you receive an email requesting a change to the account number for payments:

STOP – **DO NOT** process the request received via email

CALL – Call the "sender" using a legitimate phone number known to you. **DO NOT** reply to the email, and **DO NOT** call the number listed in the email

CONFIRM – Verify that the real vendor or employee did, in fact request the change

Resources & Website Information

Federal Government	Internet Crime Complaint Center	**https://www.ic3.gov**
	Federal Bureau of Investigation	**https://www.fbi.gov**
	Cybersecurity & Infrastructure Security Agency	**https://www.CISA.gov**
	Federal Trade Commission	**https://www.ftc.gov**
	National Security Agency	**https://www.nsa.gov**
	CISA, Homeland Security & Secret Service	**https://www.stopransomware.gov**