2021 AFP Payments Fraud & Control Survey

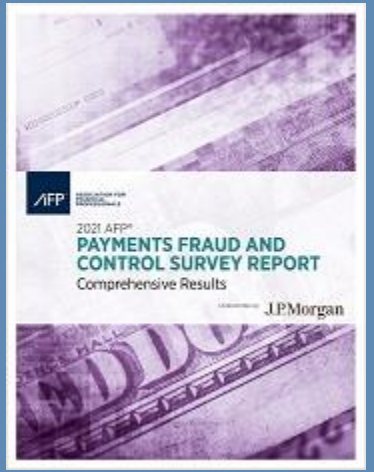
Companion Webinar

Thursday, May 13th 3:00PM EST

- **Tom Hunt,** Director of Treasury Services, AFP
- **Frank D'Amadeo,** Director, Assistant Treasurer, Treasury, Con Edison
- **Lisa Kerr,** VP, Global Risk Management and Business Continuity, Henry Schein, Inc.
- **Steven Bernstein,** Manager, N.A. Payables Product Support Specialists, J.P. Morgan
- **Sue Dean,** Head of Product Delivery for Commercial Banking and Wholesale Payments, J.P. Morgan

About the Survey

- **Generated 532 responses from treasury practitioners**
- **Examined the Following:**
  - Overall Fraud Levels
  - BEC Scams
  - Payments Controls



AFP thanks J.P. Morgan for underwriting

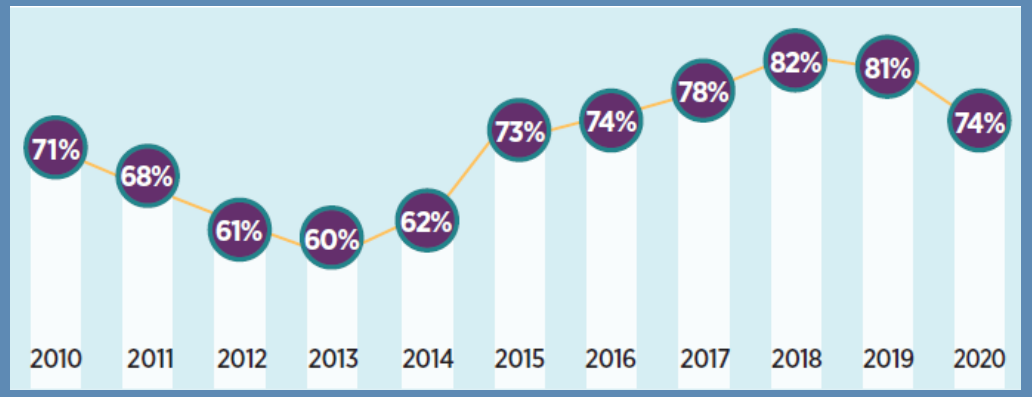
Agenda

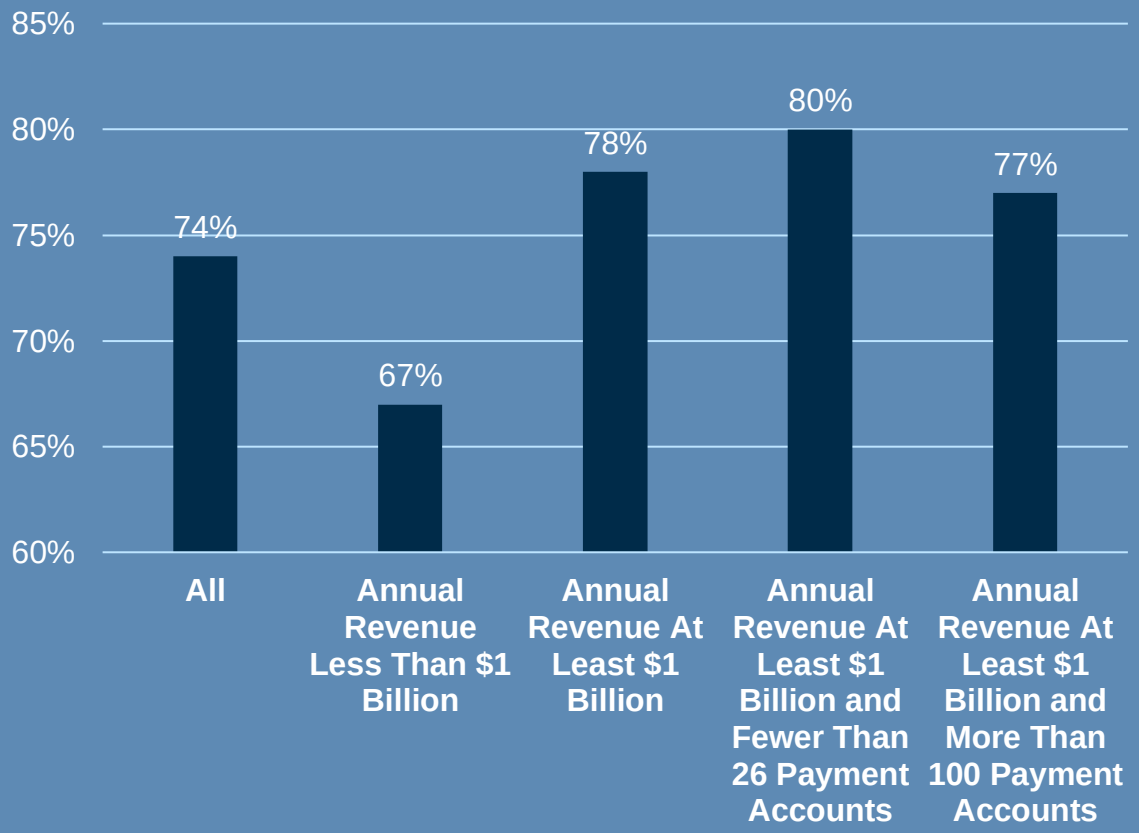
- Survey Highlights and Industry Trends
- BEC Fraud Focus
- Best Practices to Combat Fraud
- Q&A

Survey Highlights & Industry Trends

Fraud at High levels, but Decreased

Percent of Organizations Subject to Attempted and/or Actual Payments Fraud in 2020
(Percent of Organizations)

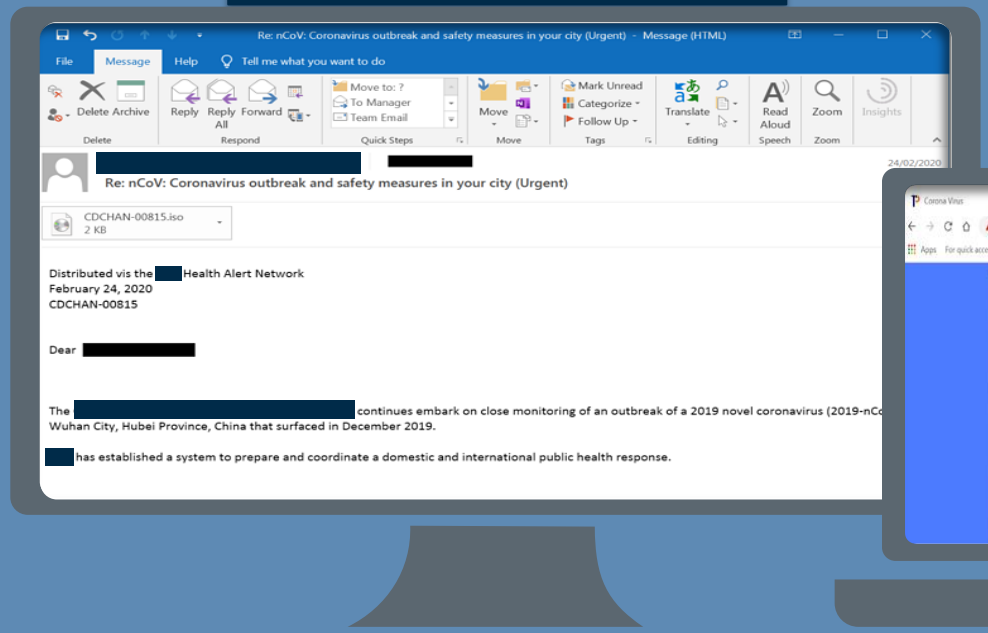




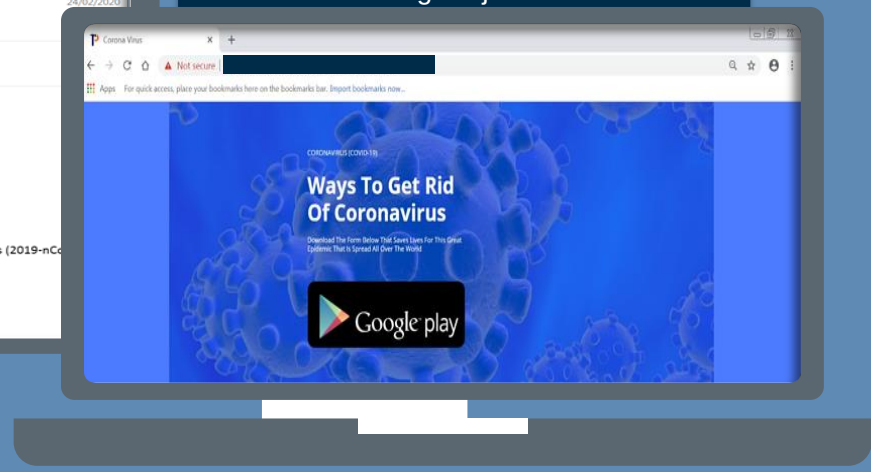
In uncertain times, bad actors will look to be opportunistic and take advantage of disruptions to normal business operations

We have seen attempts by these actors to leverage the COVID-19 situation to target individuals and organizations through advanced social engineering (email, phone, text) and the use of fake websites

Example of Covid-19 Phishing email



A fake website that actually downloads a banking Trojan virus



J.P.Morgan

This activity adds to an already-growing threat landscape that has seen continued attacks

ASSOCIATION FOR FINANCIAL PROFESSIONALS

Key statistics

74% of companies were targets of payment fraud in 2020 – down from a record high **82%** in 2018[1]

The percentage of organizations experiencing business email compromise (BEC) has risen from **75%** in 2019 to **76%** in 2020[1]

34% of companies experienced a financial loss as a result of these email scams in 2020- a slight decrease from **38%** in 2019.[1]

34% of organizations report fraudsters accessed ACH credits using BEC in 2020, a slight decrease from **37%** reported in 2019[1]

COVID-19 related web domain registrations are up **750%** since the beginning of 2020[2]

Note: [1] 2021 AFP Payments Fraud and Control Survey Report; [2] Internal J.P. Morgan data

J.P.Morgan

…and new tactics

ASSOCIATION FOR FINANCIAL PROFESSIONALS

Recent trends

Impersonation of authoritative academic or governmental organizations requesting personal data, soliciting donations to “charities”, or directing targets to fake websites with additional information on health statistics

Increased abuse of a company’s own brands to target that company’s employees with the above strategies

Emails or phone calls inquiring about organizational working arrangements, such as percentage of staff or types of roles working remotely – this information can then be used in future attacks

Other sources of payments fraud include third parties or outsourcers such as vendors (experienced by 19 percent of organizations[1]

Bad actors leveraging social media channels asking for personal information or directing targets to malicious websites

Use of email to deliver financial malware continues to be a dominant attack method with 65% of threat groups using spear-phishing to compromise their victim’s networks and 1 in 412 emails containing malware[2]

Over 66% of companies are adopting stronger internal controls that prohibit initiation of payments based on emails or other, less secure messaging systems[1]

J.P.Morgan

Note: [1] 2021 AFP Payments Fraud and Control Survey Report; [2] 2019 Symantec Internet Security Threat Report; [3] Internal J.P. Morgan data

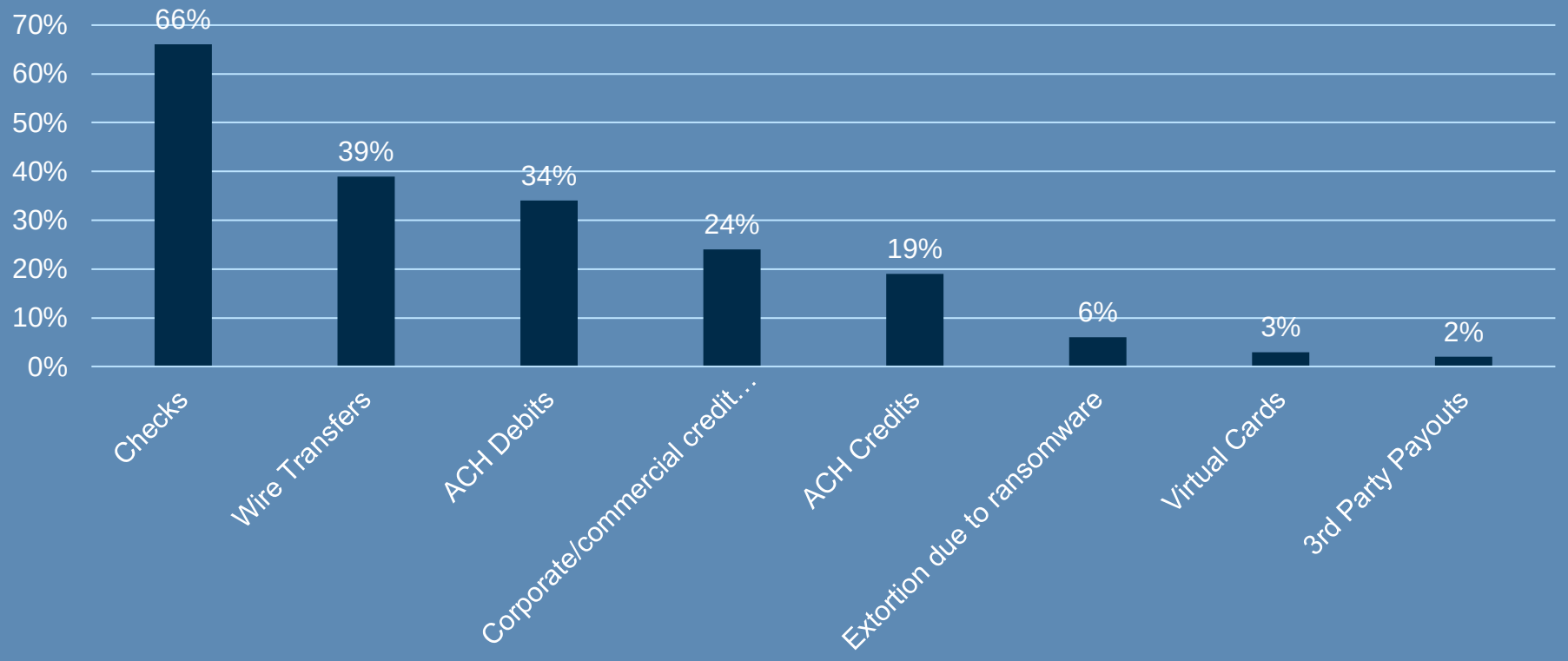
Polling Question #1

Did your organization see more attempts of Fraud last year across all payment types?

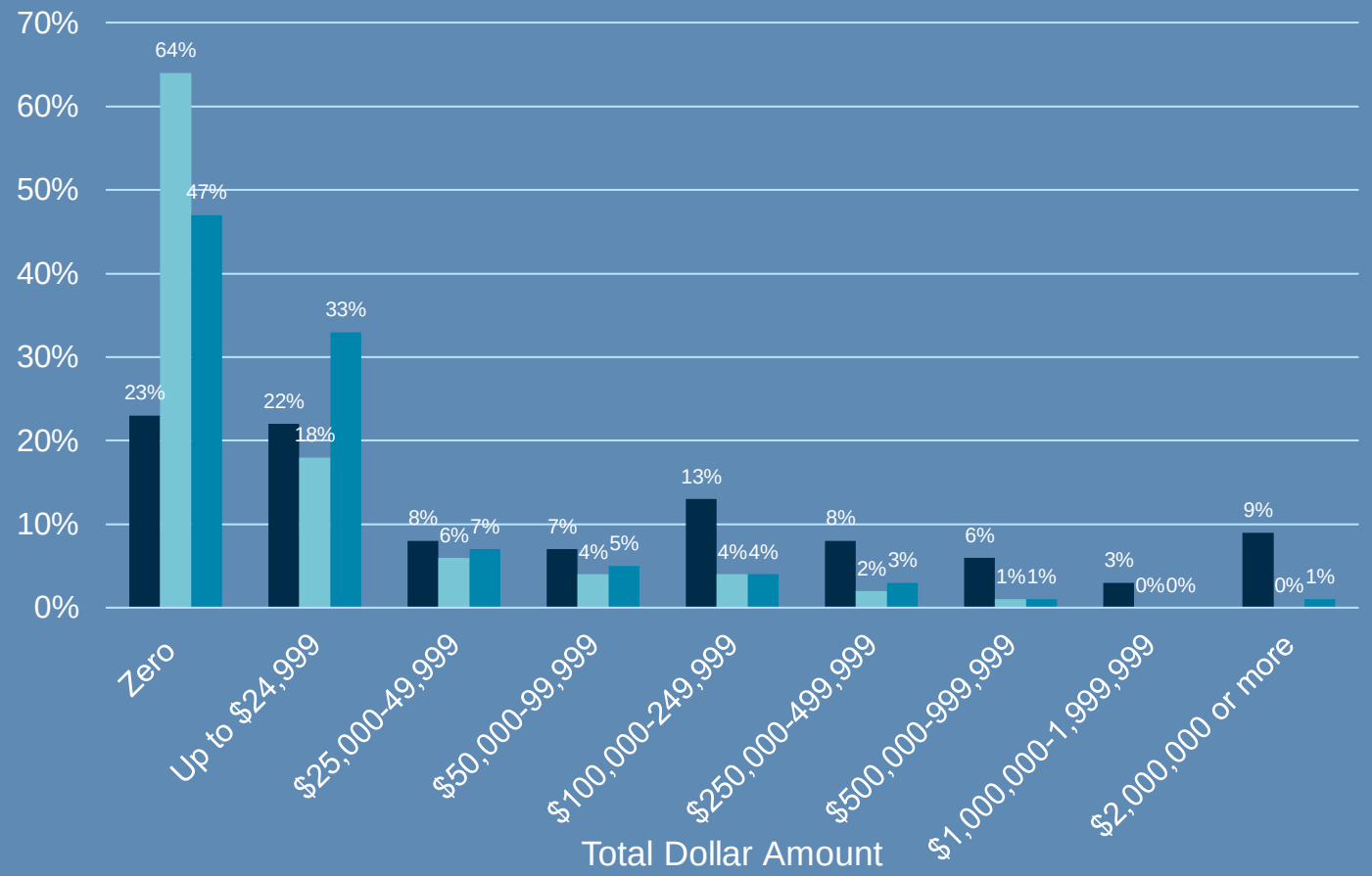
1. Yes
2. No
3. About the same

Checks and Wires are Still the Main Targets

Payment Methods that Were Targets of Attempted and/or Actual Payments Fraud in 2020
(Percent of Organizations)

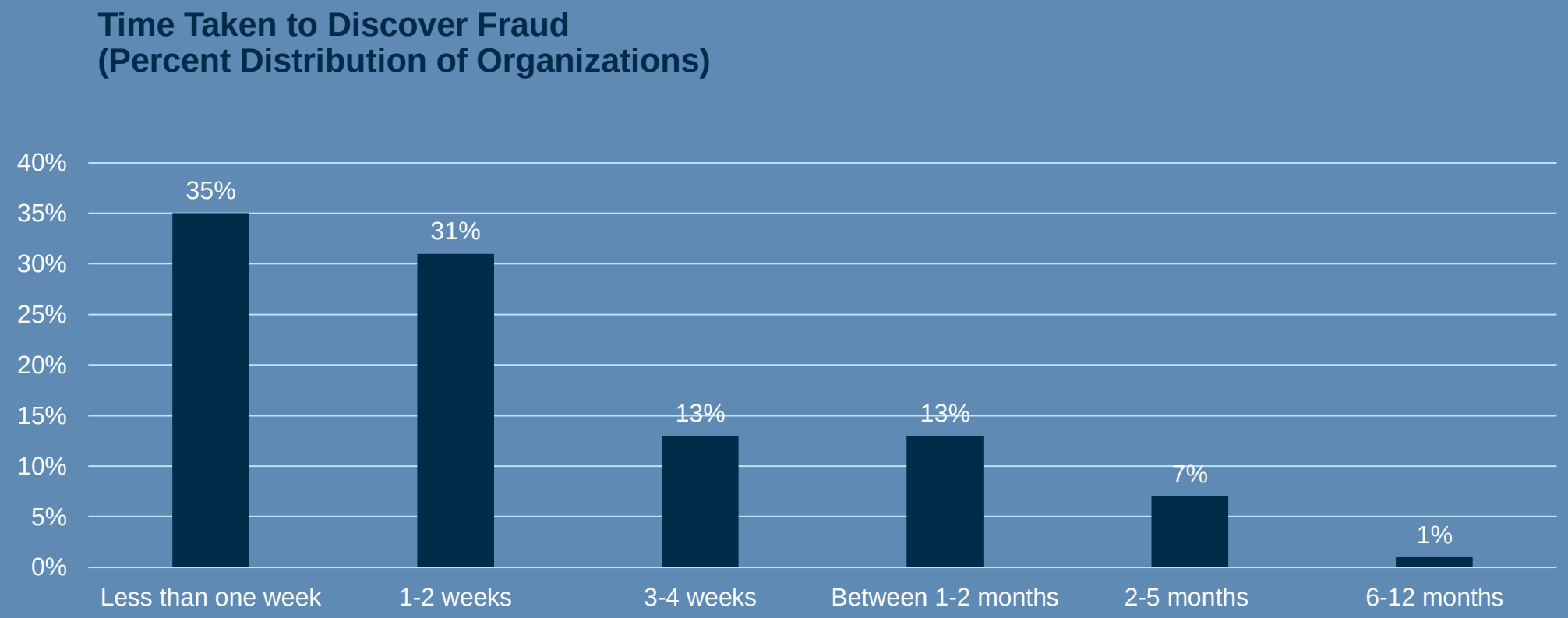


Actual Financial Losses from Payments Fraud Not Extensive



- Potential Financial Loss from Attempted and/or Actual Payments Fraud in 2020
- Actual Direct Financial Loss From Payments Fraud in 2020
- Costs to Manage/Defend/Cleanup from Attempted and/or Actual Payments Fraud in 2020

Less than a Week to Fraud Discovery



BEC Fraud Focus

BEC In Perspective: Still Big Business

ASSOCIATION FOR FINANCIAL PROFESSIONALS

2020 Crime Types *Continued*

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,866,642,107	Overpayment	$51,039,922
Confidence Fraud/Romance	$600,249,821	Ransomware	**$29,157,405
Investment	$336,469,000	Health Care Related	$29,042,515
Non-Payment/Non-Delivery	$265,011,249	Civil Matter	$24,915,958
Identity Theft	$219,484,699	Misrepresentation	$19,707,242
Spoofing	$216,513,728	Malware/Scareware/Virus	$6,904,054
Real Estate/Rental	$213,196,082	Harassment/Threats Violence	$6,547,449
Personal Data Breach	$194,473,055	IPR/Copyright/Counterfeit	$5,910,617
Tech Support	$146,477,709	Charity	$4,428,766
Credit Card Fraud	$129,820,792	Gambling	$3,961,508
Corporate Data Breach	$128,916,648	Re-shipping	$3,095,265
Government Impersonation	$109,938,030	Crimes Against Children	$660,044
Other	$101,523,082	Denial of Service/TDos	$512,127
Advanced Fee	$83,215,405	Hacktivist	$50
Extortion	$70,935,939	Terrorism	$0
Employment	$62,314,015		
Lottery/Sweepstakes/Inheritance	$61,111,319		
Phishing/Vishing/Smishing/Pharming	$54,241,075		

Source: FBI Internet Crime Complaint Center 2020 Internet Crime Report

BEC Goes Crypto

"In 2020, the IC3 observed an increase in the number of BEC/EAC complaints related to the use of identity theft and funds being converted to cryptocurrency.

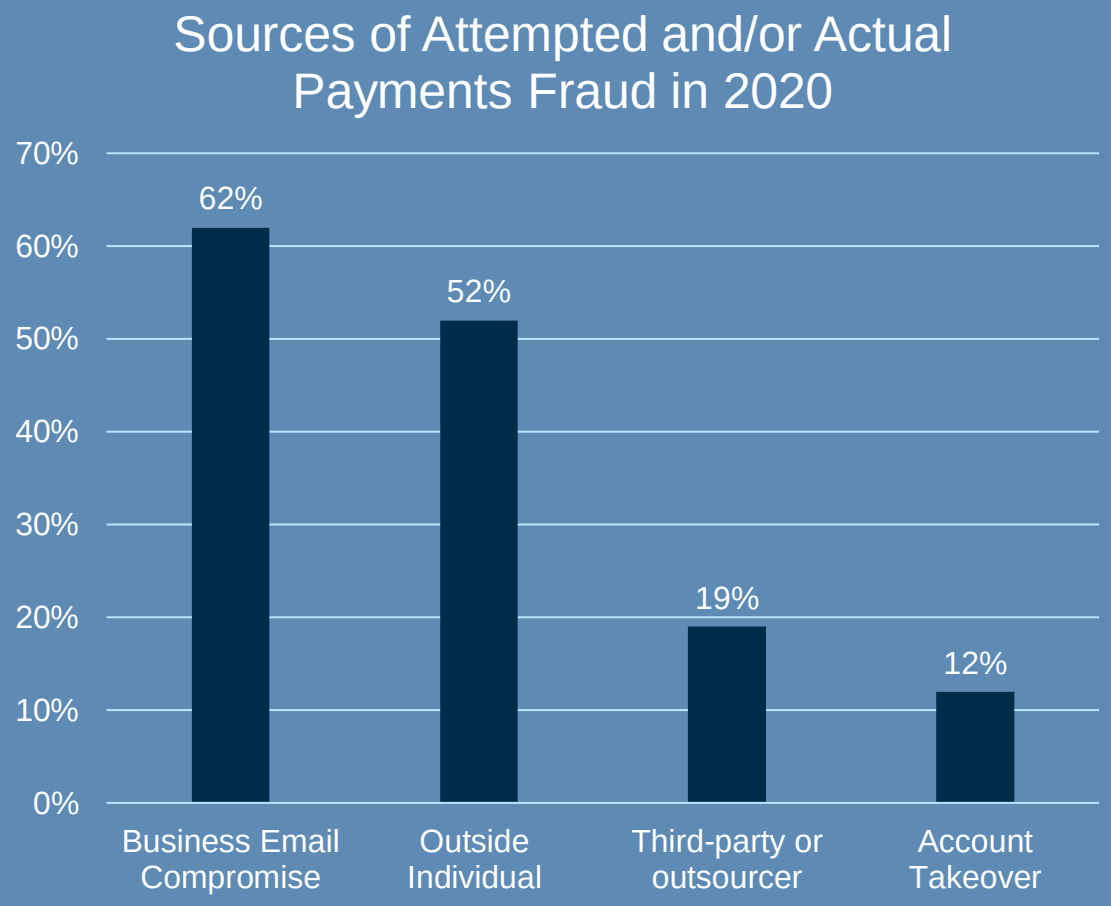
In these variations, we saw an initial victim being scammed in non-BEC/EAC situations to include Extortion, Tech Support, Romance scams, etc., that involved a victim providing a form of ID to a bad actor.

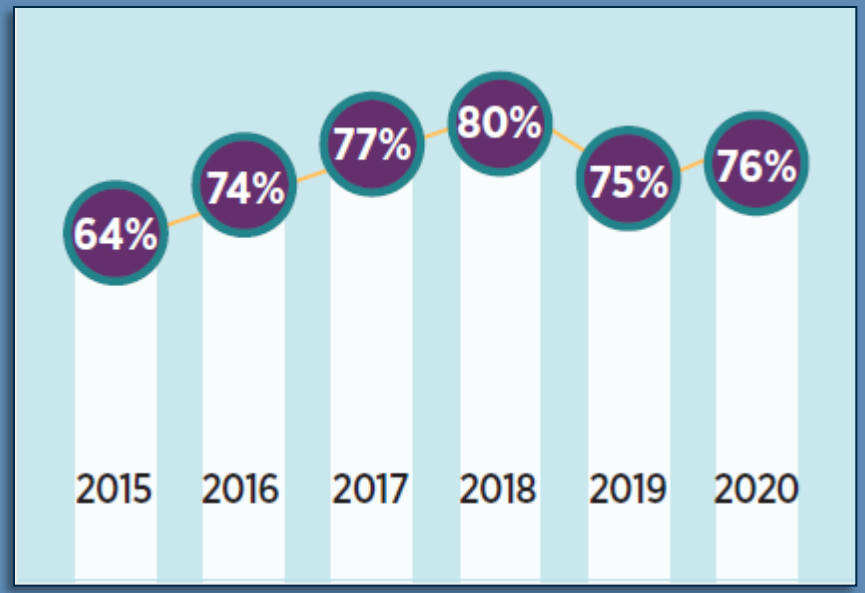
That identifying information was then used to establish a bank account to receive stolen BEC/EAC funds and then transferred to a cryptocurrency account"

Source: FBI Internet Crime Complaint Center 2020 Internet Crime Report

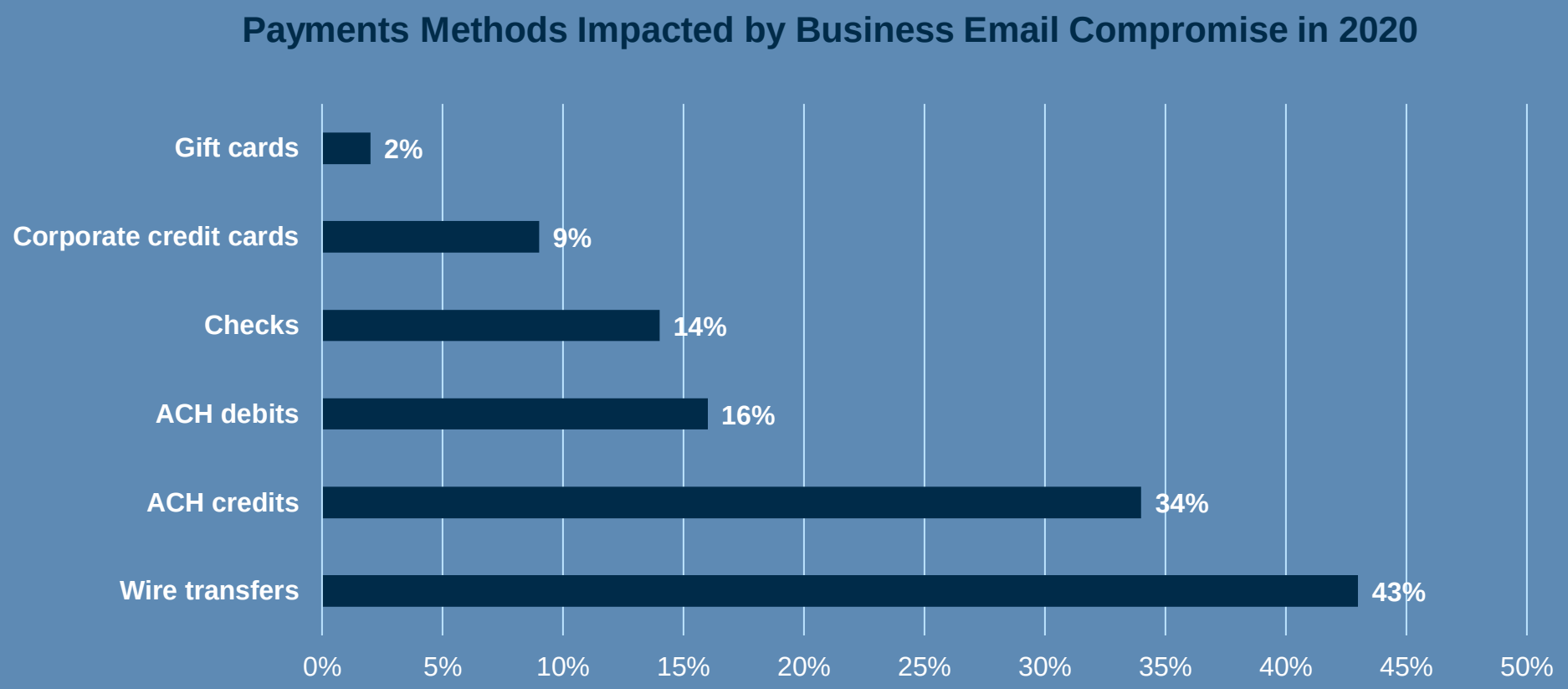
Internet Crime Complaint Center (IC3) | Business Email Compromise The $26 Billion Scam 2020_IC3Report.pdf

Business Email Compromise





Wires and ACH Credit Highest Targets



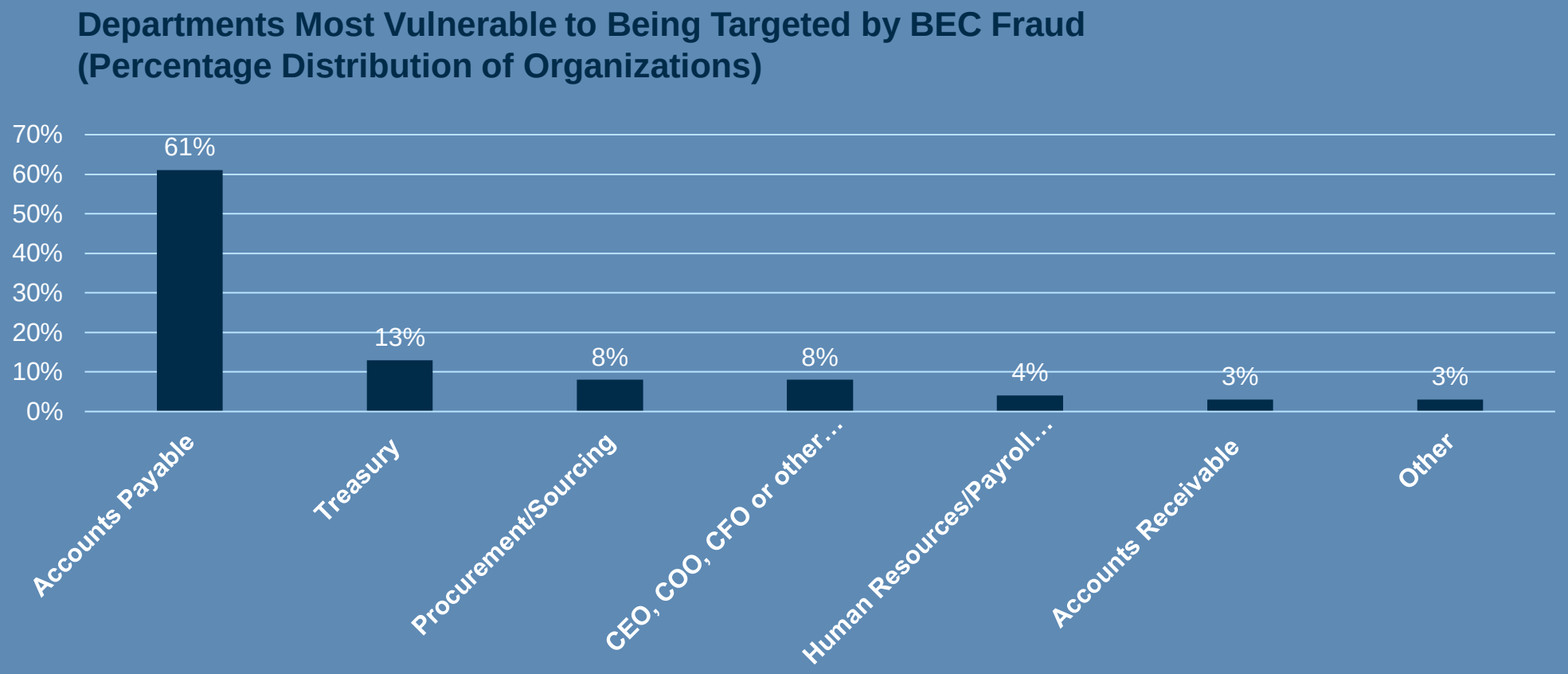
BEC Scams Result Primarily in No Losses

Estimated Total Dollar Loss to Organizations from BEC in 2020

(Percentage Distribution of Organizations that Experienced Payments Fraud via BEC)

	ALL	ANNUAL REVENUE LESS THAN $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION AND FEWER THAN 26 PAYMENT ACCOUNTS	ANNUAL REVENUE AT LEAST $1 BILLION AND MORE THAN 100 PAYMENT ACCOUNTS
No Loss	66%	69%	64%	68%	58%
Up to $24,999	14%	15%	14%	10%	19%
$25,000-49,999	7%	10%	6%	7%	5%
$50,000-99,999	4%	4%	4%	4%	5%
$100,000-249,999	4%	–	6%	6%	6%
$250,000 - $499,999	2%	1%	2%	1%	3%
$500,000 - $999,999	2%	1%	3%	3%	3%
$1,000,000 - $1,999,999	–	–	1%	1%	–
Over $2,000,000	–	–	1%	–	2%

Accounts Payable Most Vulnerable to BEC



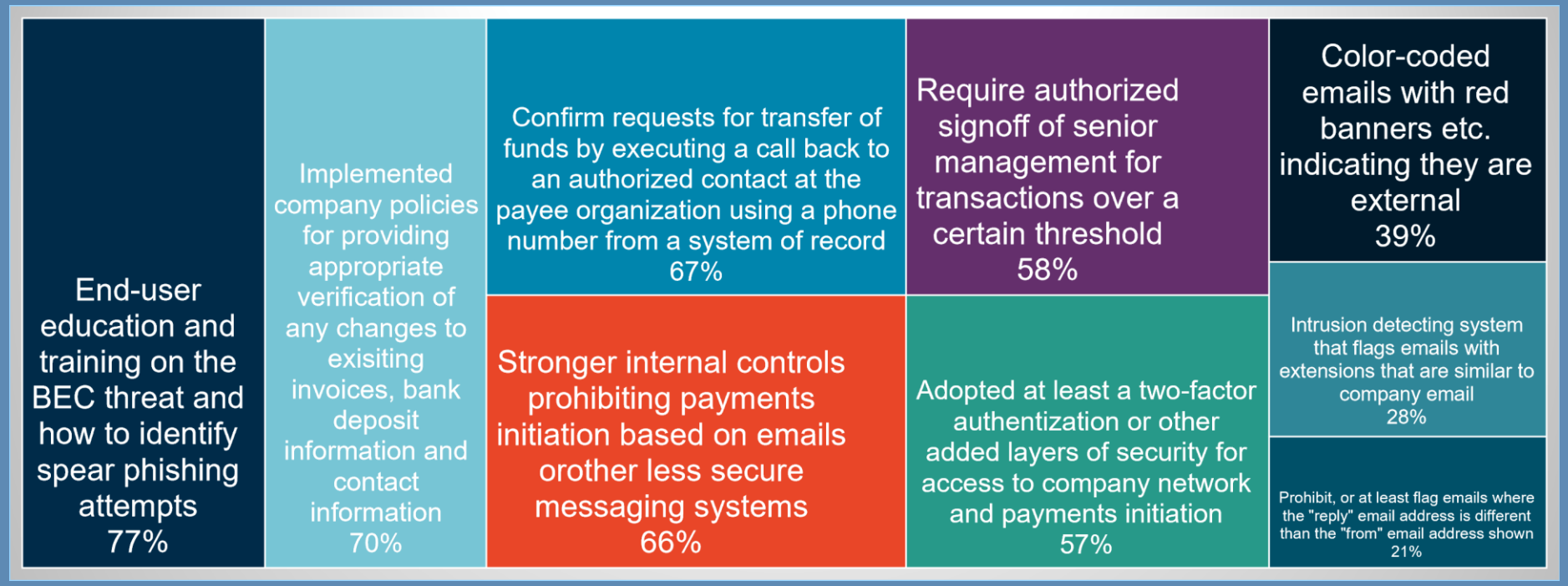
Polling Question #2

At your organization, does Treasury and A/P have the same policies and procedures in place with regards to moving money?

1. Yes
2. No
3. To some extent

Internal Controls In Place for BEC

Internal Controls Methods Implemented to Prevent BEC Fraud (Percent of Organizations)



Cybersecurity risks

ASSOCIATION FOR FINANCIAL PROFESSIONALS

	Business Email Compromise	Financial malware	Social Engineering
Definition	**Business Email Compromise (BEC)** is an electronic scam to obtain confidential, personal or financial information through email	**Malware** is malicious software, to include viruses, ransomware, and spyware, designed to cause damage to data and systems, or gain unauthorized access	**Social Engineering** refers to psychological manipulation of people into performing actions or divulging confidential information
	BEC scams accounted for **half of the cyber crimes losses**, of approximately of **$1.8bn** in 2020[1]	**Ransomware** costs are forecasted to reach a record **$20bn** by 2021[2]	**70%** to **90%** of All Malicious Breaches are Due to Social Engineering and Phishing Attacks[3]
Risk areas	■ Email Spoofing / Masking ■ Client Email Compromise ■ Vendor Email Compromise / Supply Chain ■ Lookalike Domain	■ Malware modifying legitimate payment instructions to a bad beneficiary ■ Redirection to a fake login page	■ Call from someone pretending to be a vendor ■ Client Received SMS message from a spoofed phone number
Best practices considerations	■ Consider available email security solutions to defend against lookalike domains ■ Enable controls to mark outside emails as external and ensure the process for reporting suspicious emails is clear and simple ■ Train employees on suspicious email trends and process to verify payment properly	■ Block access to suspicious websites ■ Scan email attachments upon message receipt ■ Ensure all software, antivirus and firmware is patched and updated ■ Regularly back up and secure data	■ Block access to suspicious websites ■ Scan email attachments upon message receipt ■ Ensure all software, antivirus and firmware is patched and updated ■ Regularly back up and secure data

J.P.Morgan

[1]FBI report 2020, 2PurpleSec Ransomeware statistics data report and trends, 3 KnowBe4

Cyber Insurance BEC Best Practices

“To ensure your company has protection against BECs, consider the following best practices when renewing insurance programs:

1.Check whether the insurance program includes coverage for social engineering fraud, invoice manipulation, and network security coverage. Does your company have this coverage in its policy forms? Is the insurer offering this coverage by endorsement for an additional premium?

1.Check the policy limits that would apply to those coverages. Binder letters might not disclose a sublimit on certain insuring agreements.

2.Consider how excess coverage will apply. If the primary policy has lower coverage limits for BEC losses, policyholders should explore whether excess policies will "drop down" to attach at the level of any sub-limits, to avoid coverage gaps.”

Source: 2020 edition of Corporate Policyholder Magazine, Barnes and Thornburg LLC

Polling Question #3

Does your organization have a Cyber Insurance or Crime Policy in place to cover losses from BEC?

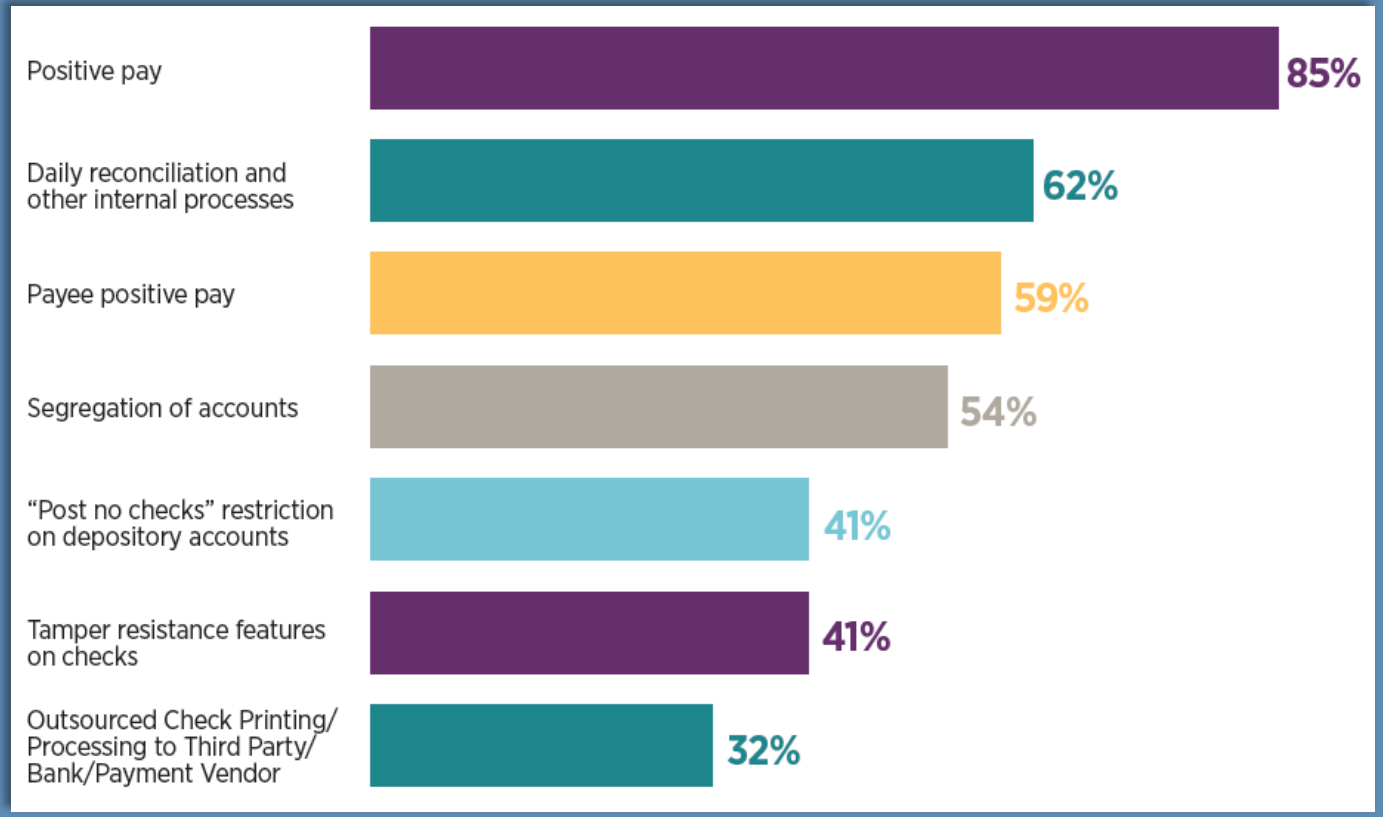
1. Yes
2. No
3. I don't know, but I'm going to find out

Best Practices to Mitigate Fraud

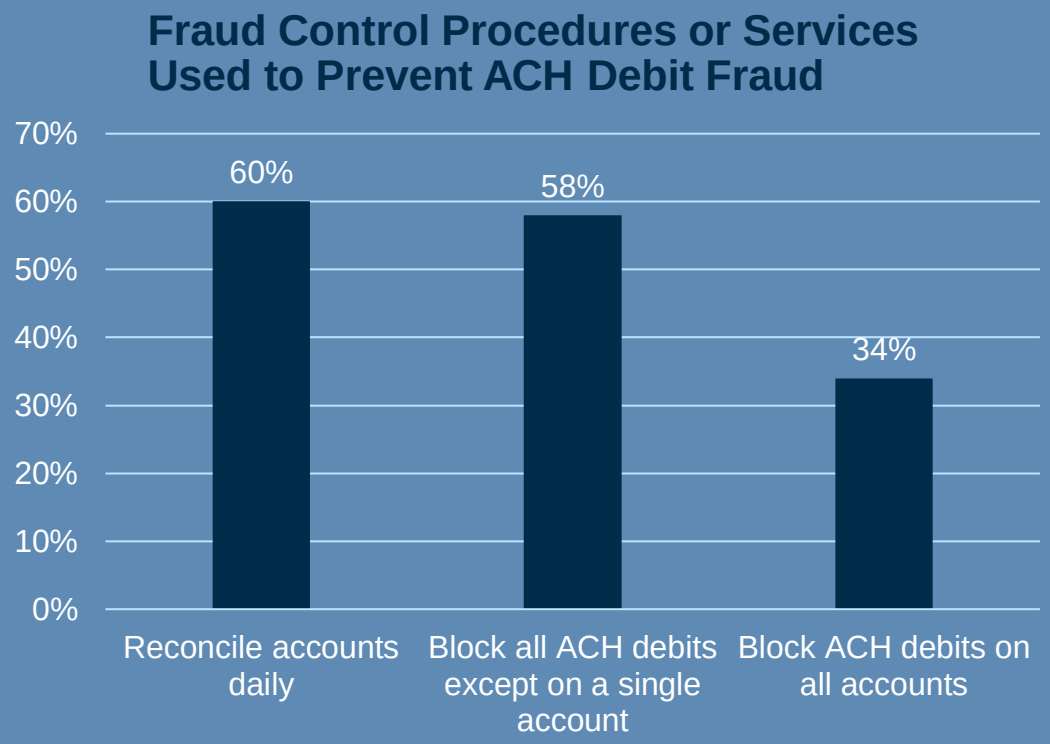
Products and Tools to Help Prevent Check Fraud

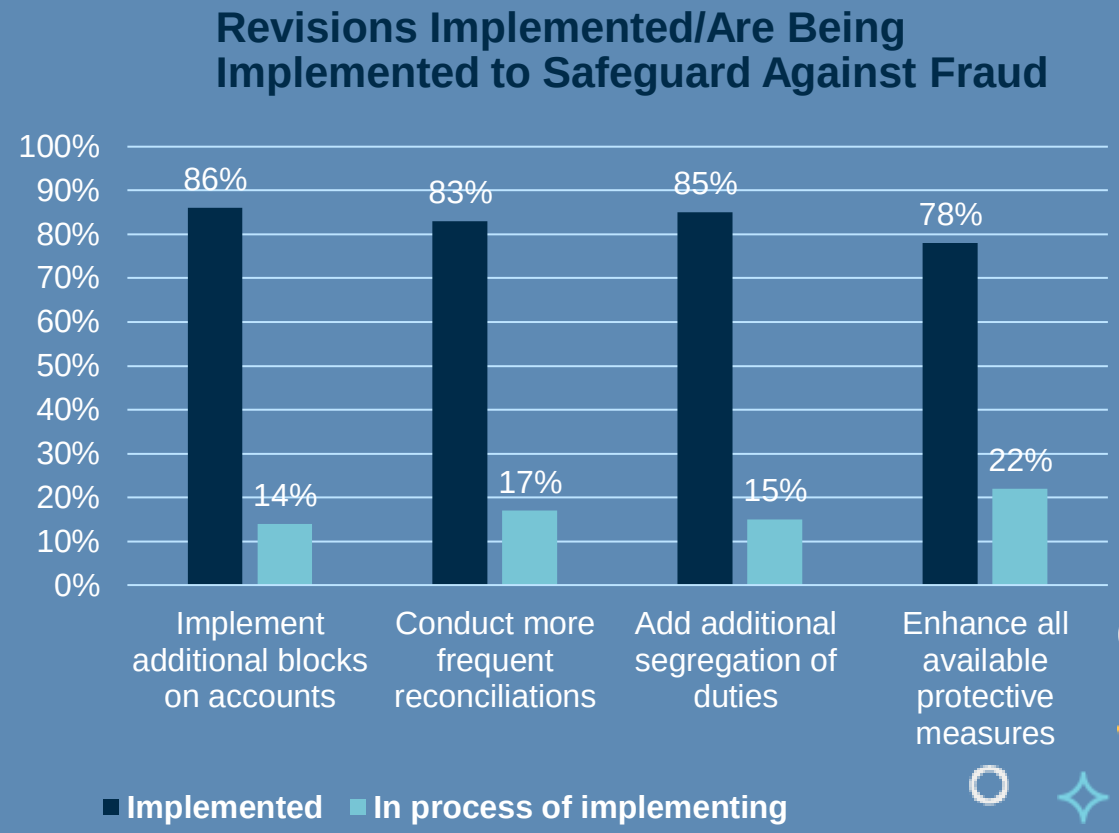
Fraud Control Procedures and Services Used to Protect Against Check Fraud

(Percent of Organizations that Experienced At Least One Attempt of Check Fraud)



Tools to Mitigate ACH Fraud

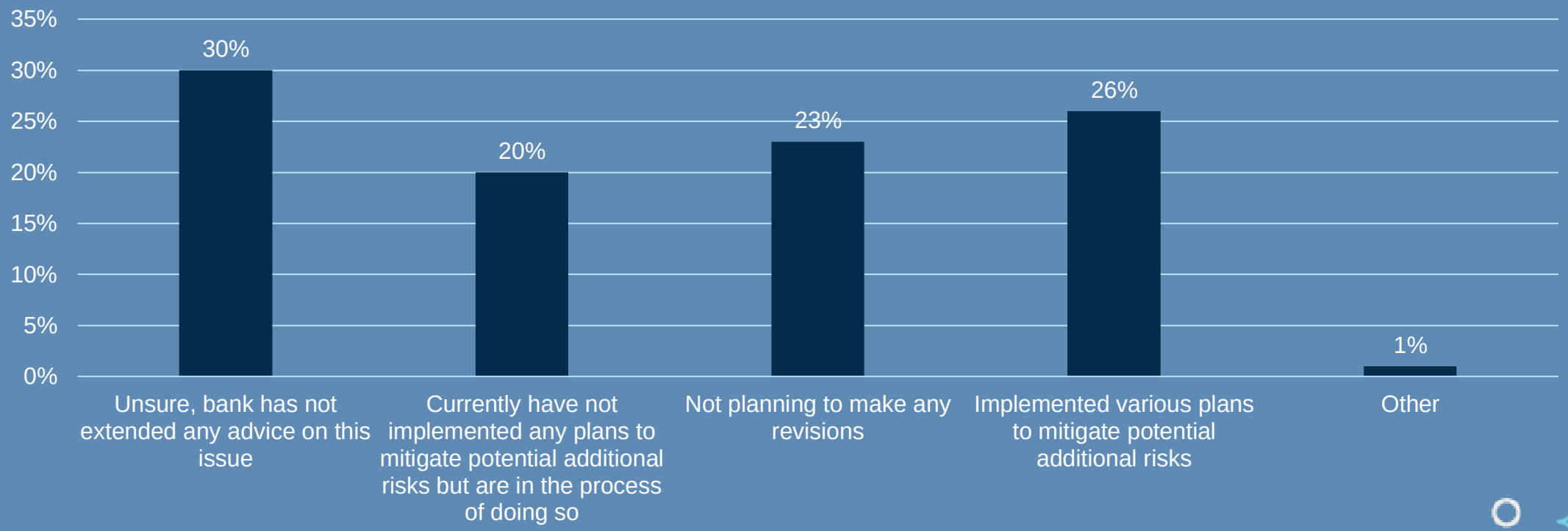




Same Day ACH Limits Increasing, Be Prepared

Organizations' Preparedness to Mitigate Potential Additional Risks with Same-Day ACH for Both Credit and Debit Transactions

(Percentage Distribution of Organizations that Experienced At Least One Attempt of Ach Fraud)



Payment Security

DON'T let unauthorized and potentially costly ACH Transactions impact your accounts

Payment Verification

- Authentication and validation of beneficiary detailed prior to payment release.
- Validation of new or updated beneficiary account details.

Enhanced security

- Mitigate fraud by controlling who has access to your accounts
- Control who can post ACH debits and credits to your account
- Return unauthorized debit and credit transactions posted to your account

Greater savings

- Spend less time reconciling and investigating your transactions
- Avoid unintended returns of authorized ACH transactions

More flexibility

- Configure features to meet the level of protection you need
- Option for dual control to block profile setups and changes, user decisions and returns

J.P.Morgan

Payment Verification

Minimizing fraudulent payments, returns, and exceptions by validating account ownership and account status prior to transaction initiation

Account Verification

Account Owner Authentication

Provides answers real-time at point of transaction:

- Does the account exist (open/active)?
- What is the account's associated risk?
- Is the person authorized to transact on this account?
- What is the likelihood of the item being returned?
- Is the account a non-DDA Account?

Account Validation Best Practices

- **Confirm** that the account exists (open/closed), and whether it is a new account or in a negative status
- **Verify** if the account is a non-DDA account
- **Understand** the account's associated risk & likelihood of the item being returned
- **Validate** that this person is authorized to transact on the account
- **Identify** if lost or stolen checks have been reported on the account
- **Process Payment** once account is validated and the account is in good standing

Choose the right solution for your business—ACH Security Services

ASSOCIATION FOR FINANCIAL PROFESSIONALS

Block or decision BEFORE posting

Transaction Blocking

Automatically block unauthorized ACH debit and credit transactions from posting

TIP: Ideal for when no debits or credits should post

How it works:

- Received ACH debits and credits that match block settings are returned automatically without posting
- No option to review and decision unauthorized ACH activity prior to blocking or posting, which may result in unintended returns and potential related missed payment deadlines and penalties

ACH Positive Pay

Get notified of blocked transactions, change decisions to pay and add allowable IDs for future transaction

TIP: Ideal for ensuring all received ACH debits and credits are authorized, preventing unintended returns and postings

How it works:

- Received ACH debits or credits generate alerts
- Choose to change the Pending Return or Pay decision applied based on the blocking profile

Review and decision AFTER posting

Transaction Review

Review and confirm transactions posted the prior banking day for more proactive management of activity

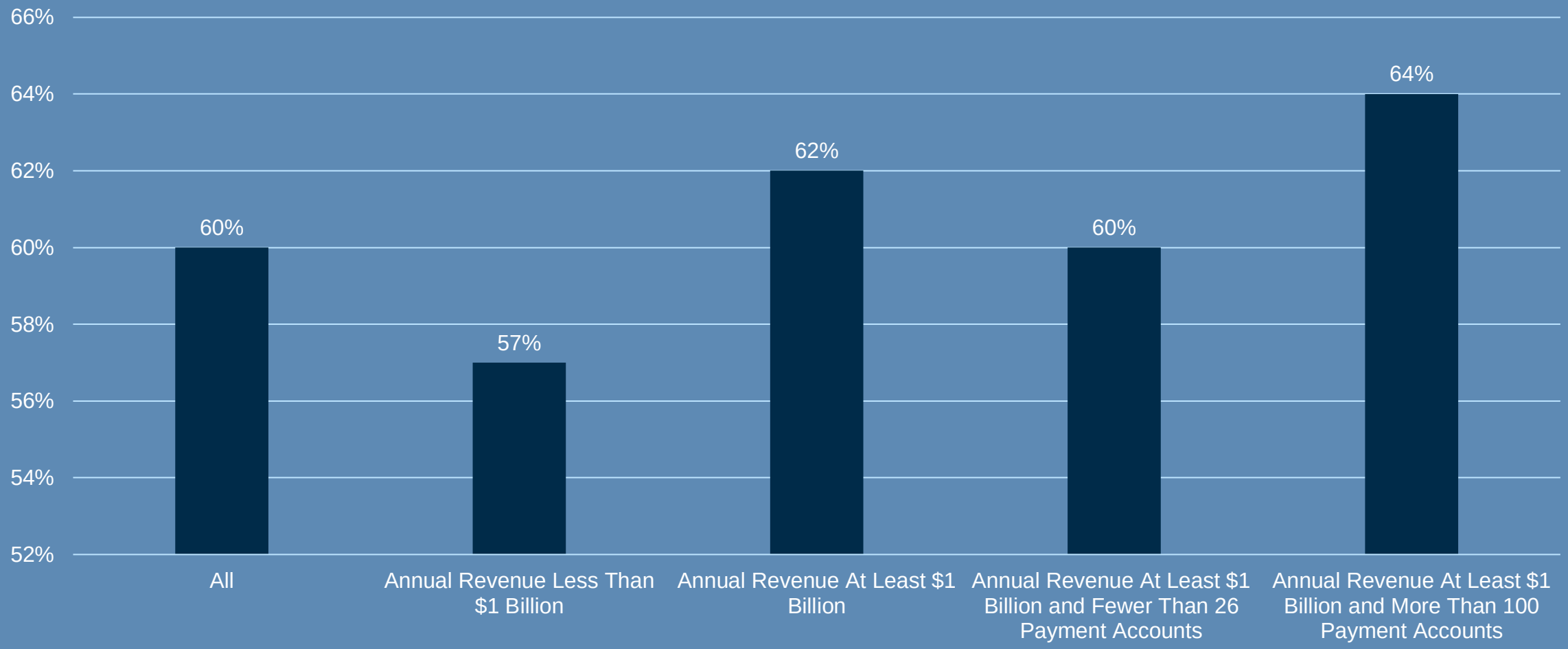
TIP: Ideal for when viewing and returning received ACH activity are necessary and when reviewing and returning the banking day after posting are not a concern

- Received debits/credits that post to the account the prior banking day are reviewed based on profile filters
- Return decisions generate an ACH return. Pay decisions will have no impact since they are posted the prior day

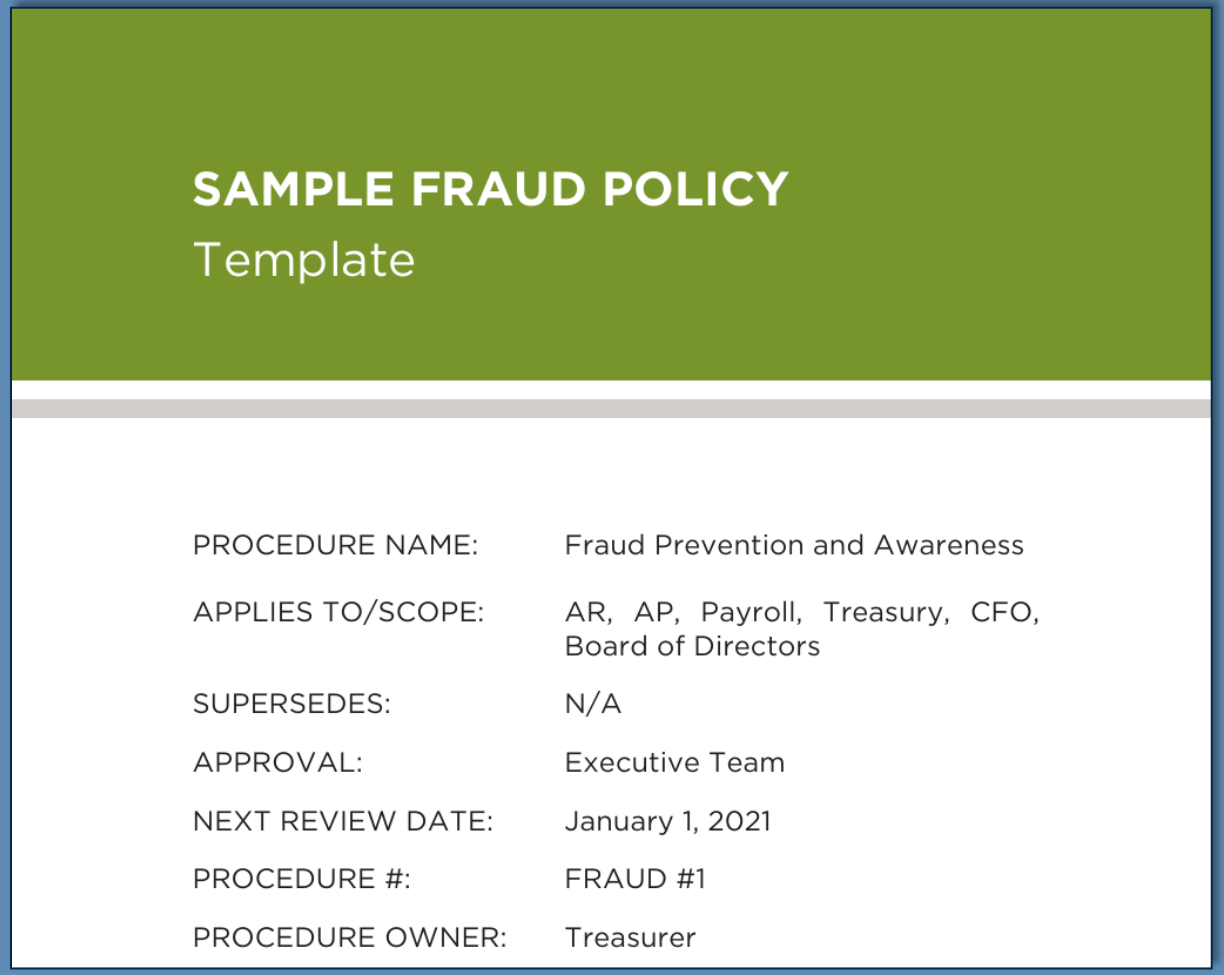
J.P.Morgan

Percentage of Organizations That Have a Fraud Policy

(Percentage Distribution of Organizations)



AFP Fraud Policy Template



SAMPLE FRAUD POLICY
Template

PROCEDURE NAME:	Fraud Prevention and Awareness
APPLIES TO/SCOPE:	AR, AP, Payroll, Treasury, CFO, Board of Directors
SUPERSEDES:	N/A
APPROVAL:	Executive Team
NEXT REVIEW DATE:	January 1, 2021
PROCEDURE #:	FRAUD #1
PROCEDURE OWNER:	Treasurer

AFP Members Can Access Here:

https://bit.ly/2WEhSEb

Best practices – General

ASSOCIATION FOR FINANCIAL PROFESSIONALS

Tips to better protect your firm

1 Conduct an independent assessment	Engage an experienced engineering firm that understands the technical risks and complexities of enterprise architecture to do a complete technical independent assessment of your firm's infrastructure. Make sure to engage a company that has more technical expertise than a general consulting firm. You should know where your vulnerabilities are at all times
2 Engage government and law enforcement	Ensure you have a clear engagement model with the government including law enforcement. Who are you going to call? Which agency and under what circumstances? Have the relationship established up front and the engagement documented in a run book
3 Join an industry forum	Join an applicable industry-based information sharing forum ("ISAC") to share and receive important threat information
4 Simulate an internal attack	Create a Red Team and have them attack your systems using the same techniques the bad guys do. Not once a year, all the time. Also consider establishing a program to harvest credentials and account numbers that might be in the underground related to your bank—to detect compromises you may not otherwise be aware of
5 Deploy mandatory employee training and testing	Malicious email is the #1 way bad guys get into organizations. Establish a baseline training program for all employees that is mandatory and focuses on the specific actions employees need to take to protect the firm. Once you have trained your employees, actively test them.
6 Know your third party vendors	Understand your third party environment and upgrade your contract provisions and ensure they are following the same standards you are striving for in your own environments
7 Exercises and drills	Run simulations and drills to assess your capability. Use a combination of table top scenario exercises and live inject of events into your Security Operations Centres to see how it responds. Learn lessons and repeat. Include colleagues from the business in addition to technologists in the table top exercises
8 Know how money leaves the organization	Look at all of the ways money leaves your institution. Figure out what controls and thresholds you can put in to protect money movement assuming bad guys get around your other controls. Examples: wire limits, country destinations, new beneficiaries
9 Implement controls for maximum effect	Consider using resources such as Positive Pay, Reverse Positive Pay, ACH Debit Blocking, and ACH Transaction Review to provide early warning of potential fraudulent activity, allowing for faster intervention and increased likelihood of stopping transactions and recovering funds
10 Protect your computers	Consider physical or logical network segmentation for funds transfer related computers; employ the concept of 'least privilege" to limit the use of administrator privileges; and consider limiting the processes and services that can be run on funds transfer related computers (e.g. no email or Internet browser applications).

J.P.Morgan

Questions

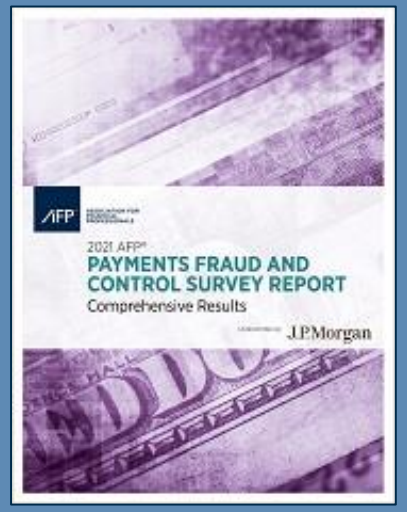
Contacts:

Tom Hunt, CTP
AFP
Director, Treasury Services
thunt@afponline.org

Sue Dean
Head of Product Delivery for Commercial Banking and Wholesale Payments
J.P. Morgan Commercial Banking
Susan.J.Dean@jpmorgan.com

Steven Bernstein
Manager, N.A. Payables Product Support Specialists
Commercial Banking, J.P. Morgan
Steven.Bernstein@jpmchase.com

https://bit.ly/3y5ipk3



https://bit.ly/2WEhSEb