ASSOCIATION FOR FINANCIAL PROFESSIONALS

2023 AFP®

PAYMENTS FRAUD AND CONTROL SURVEY REPORT

KEY HIGHLIGHTS

Underwritten by: J.P.Morgan

2023 AFP®

PAYMENTS FRAUD AND CONTROL SURVEY REPORT

KEY HIGHLIGHTS

This summary report includes highlights from the comprehensive 2023 AFP® Payments Fraud and Control Survey Report. The complete report comprising all findings and detailed analysis is exclusively available to AFP members.

Learn more about AFP membership.

Underwritten by:

J.P.Morgan

We're proud to share the results from the 2023 AFP Payments Fraud and Control survey. As a sponsor of the survey for the last 15 years, J.P. Morgan is committed to helping organizations protect themselves from payments fraud.

The latest survey shows that payments fraud is still a serious threat for every organization. Instances of digital fraud are frequent across various fronts, with multiple schemes aimed at relaxed controls.

Here are some highlights from the survey:

- The share of businesses that reported commercial card fraud has increased by 10 percentage points since 2021.
- The share of businesses that reported ACH Credit fraud has increased by six percentage points over the same time frame.
- Fraudsters continue to impersonate employees and vendors through sophisticated business email compromise schemes that are the root cause of most reported fraud cases.
- Checks are the payment method most vulnerable to fraud—a trend that has remained consistent since the first AFP survey.
- Still, three out of four organizations that use checks plan to keep using checks.

J.P. Morgan offers products and services that can help you manage your fraud risk in connection with checks, wires, and ACH. We hope this report keeps you informed on the latest challenges and encourages you to remain vigilant as ever.

With best regards,

Sue Dean

Head of Solutions, Commercial Banking

J.P. Morgan

Max Neukirchen

Global Head of Payments & Commerce Solutions

J.P. Morgan

Alec Grant

Head of Client Fraud Prevention, & Recoveries, Commercial Banking,

J.P. Morgan

Ryan Schmiedl

Global Head of Trust & Safety, Payments,

J.P. Morgan

J.P.Morgan

TOPICS COVERED IN THE COMPREHENSIVE 2023 AFP® PAYMENTS FRAUD AND CONTROL SURVEY REPORT

PAYMENTS FRAUD ACTIVITY

- Payments Fraud Trends
- Payment Methods Impacted by Payments Fraud
- Corporate/Commercial Card Fraud
- Losses Incurred Due to Payments Fraud Attempts/Attacks
- Detecting Payments Fraud Activity
- Recouping of Funds
- Origination of Attempted/Actual Payments Fraud

BUSINESS EMAIL COMPROMISE (BEC)

- About Business Email Compromise
- Business Email Compromise Trends
- Financial Impact of Business Email Compromise
- Financial Losses Incurred Due to Business Email Compromise
- Targets of Business Email Compromise Scams
- Departments Most Susceptible to Business Email Compromise Fraud

PAYMENTS FRAUD CONTROLS

- Business Email Compromise Controls
- Check Fraud Controls
- ACH Fraud Controls
- Implementing Risks to curb Fraud via Faster Payments
- Beneficiary Validation
- Fraud Review
- Measures to Improve Controls

INTRODUCTION

As 2021 came to a close, organizations were slowly returning to some level of normalcy as the severity of the impact of COVID-19 began to diminish. However, the spread of the highly contagious Omicron variant upended those plans during the first few months of 2022. Once that threat subsided, business leaders were quick to focus on ramping up operations. But there were challenges, including a sudden and severe shortage of personnel in the workforce and a tight job market. Organizations found it difficult to fill open positions. Employees had the upper hand, and they were being swayed by higher compensation and benefits from other employers. A consequence was that people were resigning from their jobs in droves, resulting in a global phenomenon known as the "Great Resignation."

In February of 2022, Russia attacked Ukraine. Sanctions imposed on Russia by many western countries resulted in a very tense global situation. This created instability and fuel prices rose precipitously. Inflation rates rose to the highest levels in decades, and the cost of groceries, rent, fuel and other household items were skyrocketing. As a consequence, the Federal Reserve took action to control the rising inflation by increasing interest rates 7 times in 2022; it is anticipated there will be more rate increases in 2023.

With rising interest rates, the fear of a recession loomed over the economy. Tech companies began mass layoffs creating a sense of uncertainty and fear that organizations in other industries might follow suit. To address challenges in the work environment, many companies offered employees hybrid work arrangements, requiring that employees come into their offices only a few times a week or month. Some organizations mandated that employees return to offices, but that was – and continues to be – met with resistance. Other organizations chose to remain "virtual" permanently.

With the major threat of COVID-19 now abated, many businesses are functioning at pre-pandemic levels. During COVID-19, payment systems were put to the test of operating in an all-virtual environment. With minimal preparation, companies had to make and receive payments while operating in an environment drastically different from the usual norm. 2022 saw a large increase in brazen and successful attempts at stealing mail from post office boxes: i.e., the blue boxes typically found on street corners. Perpetrators of these crimes replicated keys to mailboxes and stole mail. Mail was then opened, and payments containing checks (government, business, personal, etc.) were washed and check amounts and names of payees altered. These checks were then endorsed and deposited into accounts with a short life. FinCen recently issued a warning to financial institutions about this type of fraud[1]. This type of fraud is low-tech (being paper based) and low cost, and so is an attractive method for fraudsters. Postal Inspectors are overworked with cases of this type of fraud, and perpetrators are able to get away with few repercussions. To address this trend, treasury and finance professionals worked on equipping their organizations to tackle the risk of fraud in this new scenario. Stringent controls were put in place to curb fraud attacks on payment systems. This appears to have been effective in curbing instances of widespread payments

[1] FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail | FinCEN.gov

INTRODUCTION (Continued)

fraud. Additionally, the use of checks, a common target of perpetrators, has declined considerably, preventing fraudsters from doing further harm using checks as a means to perpetrate fraud.

Every year since 2005, the Association for Financial Professionals® (AFP) has conducted its *Payments Fraud Survey*. The surveys examine the nature of fraud attacks on business-to-business transactions, the payment methods impacted, and the strategies organizations are adopting to protect themselves from those committing payments fraud. Continuing this research, AFP conducted the 19th Annual *Payments Fraud and Control Survey* in January 2023. The survey generated 471 responses from corporate practitioners from organizations of varying sizes representing a broad range of industries. Results presented in this report reflect data for 2022. Survey respondent demographics are available at the end of this report.

AFP thanks J.P. Morgan for its continued underwriting support of the *AFP Payments Fraud and Control Survey* series. Both questionnaire design and the final report, along with its content and conclusions, are the sole responsibility of AFP's Research Department.

"Attempted fraud was discovered by our supplier setup team calling an established vendor and confirming they had not changed banks, as per the email we received."

KEY FINDINGS

Overall, attempted or actual payments fraud in 2022 was lower compared to that in recent years.

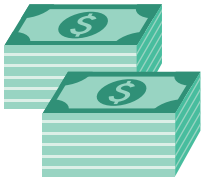
Sixty-five percent of respondents indicate that their organizations were victims of either attempted or actual fraud activity in 2022 – the smallest percentage since 2014.

Instances of fraud via digital payment methods have risen since 2021.

Commercial card fraud increased by 10 percentage points in 2022, fraud via ACH credits was up by 6 percentage points and fraud via virtual cards also increased by 6 percentage points during the same time frame.

Twenty-seven percent of organizations were able to successfully recover at least 75 percent of funds lost due to payments fraud in 2022, while 44 percent were unsuccessful in doing so.

Over half of organizations with annual revenue of less than $1 billion were unable to recover funds lost due to payments fraud attacks.



Business Email Compromise (BEC) scams are still highly prevalent and are the root cause of payments fraud at a majority of organizations. Seventy-one percent of companies were victims of payments fraud via email in 2022.

Larger organizations with annual revenue of at least $1 billion were more susceptible to BEC scams, while those companies with less than $1 billion in annual revenue were more susceptible to fraud committed by individuals outside their organizations.

Payment methods used during BEC attempts included wires, cited by 45 percent of respondents (the highest percentage in the past five years) and ACH debits.

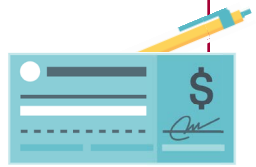
Fraudsters are increasingly targeting ACH debits when attempting scams via email.

Nearly 80 percent of organizations are most likely to seek assistance from their banking partners for guidance regarding the steps to take to minimize the impact of payments fraud.

Sixty-nine percent inform the security/compliance team at their organizations.

Checks continue to be the payment method most vulnerable to fraud.

Sixty-three percent of respondents report that their organizations faced fraud activity via checks. Three-fourths of organizations currently using checks do not plan to discontinue issuing checks.



PAYMENTS FRAUD ACTIVITY IN 2022

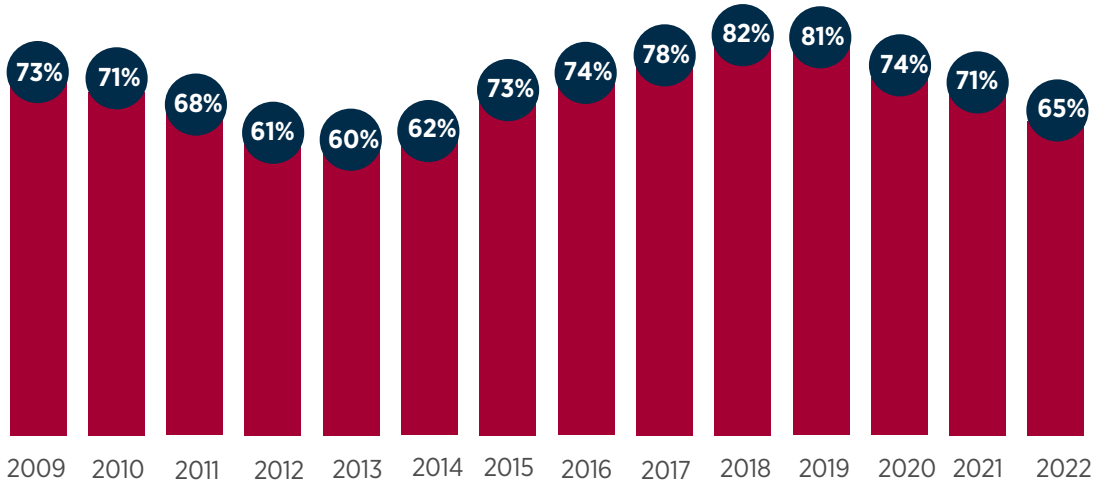
Fewer Organizations Report Being Targets of a Payments Fraud Attack in 2022

From 2009-2013, organizations experienced a decline in payments fraud activity. Sixty percent of respondents reported instances of fraud at their organizations in 2013. Then the pendulum swung the other way and there was an uptick in fraud activity between 2014-2018. In 2018 and 2019 payments fraud activity was widespread with over 80 percent of organizations falling prey to the tactics of fraudsters.

Since then, there has been a decrease in the percentage of treasury professionals reporting that their organizations had been targets of a fraud attack. Fortunately, this downward trend activity continued in 2022; 65 percent of organizations were victims of either attempted or actual fraud activity – the smallest percentage since 2014. Although this figure is lower than fraud reported in recent years, it is still a significant share with two out of three companies continuing to be victims of fraud attacks.

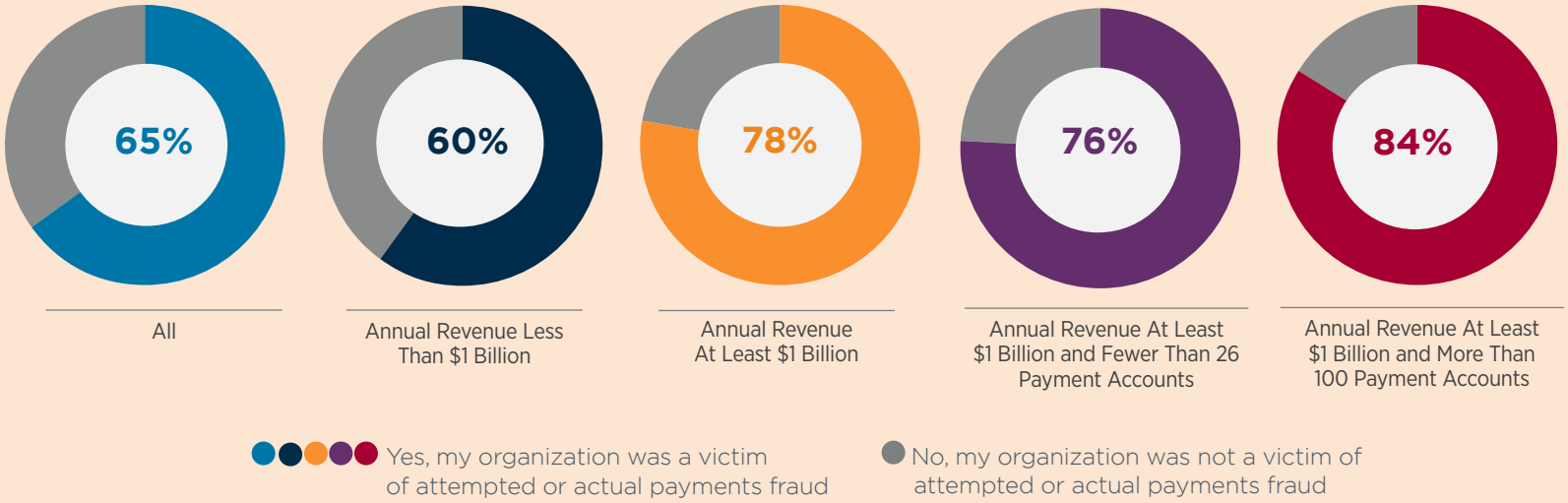
A greater share of survey respondents from larger organizations and those with more payment accounts – i.e., those with annual revenue of at least $1 billion and with more than 100 payment accounts – reports their firms experienced payments fraud in 2022 compared with the share of respondents from other organizations. Eighty-four percent of these organizations were targets of payments fraud. Fewer smaller organizations – those with annual revenue less than $1 billion – were targets of payments fraud in 2022 than were larger organizations (with annual revenue of at least $1 billion): 60 percent compared to 78 percent, respectively. Fraudsters were more inclined to target larger organizations, exposing deficiencies around process controls using social engineering.

Percent of Organizations That Were Victims of Payments Fraud Attacks/Attempts



PAYMENTS FRAUD ACTIVITY IN 2022

Prevalence of Attempted/Actual Payments Fraud in 2022
(Percentage Distribution of Organizations)



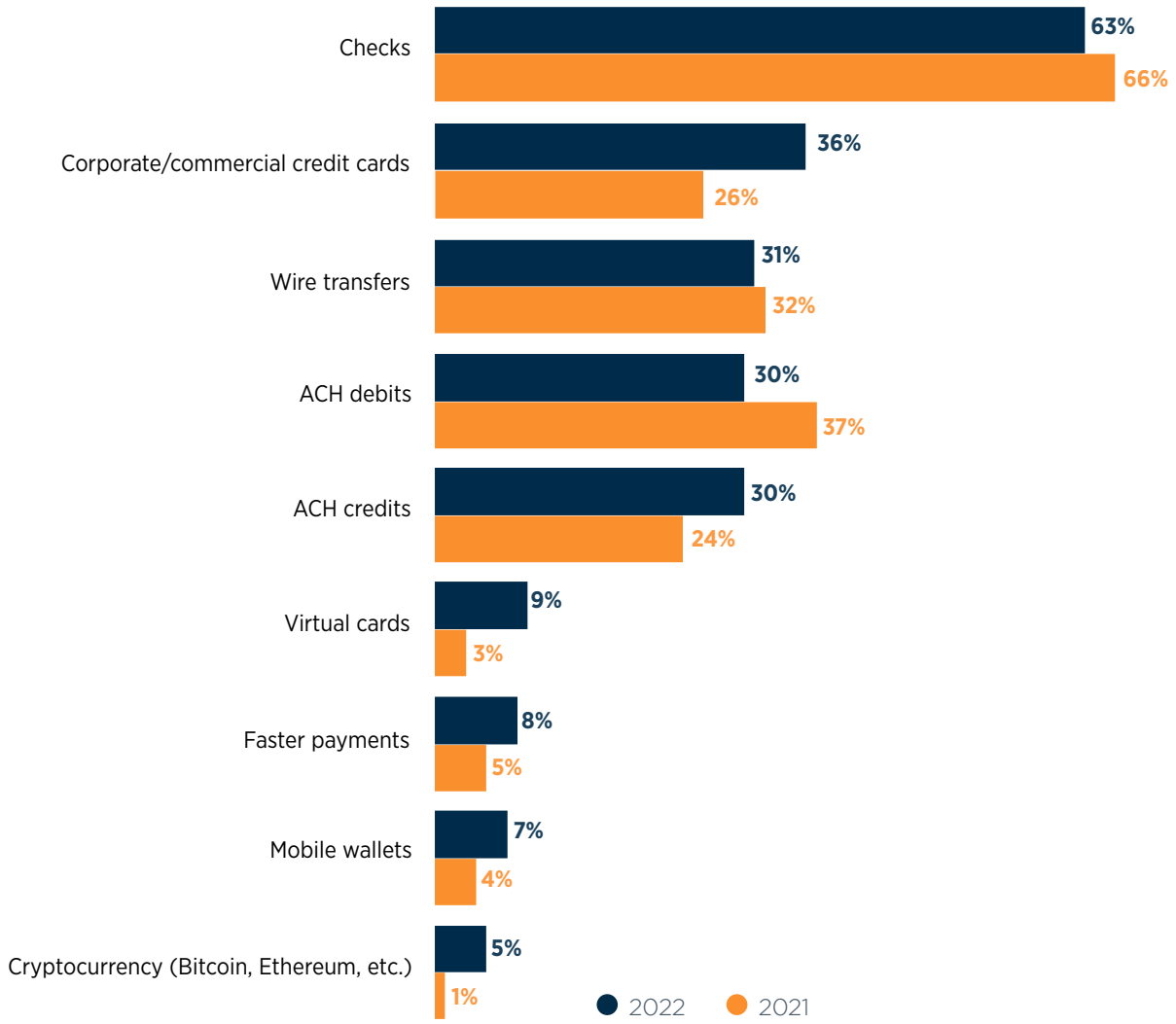
PAYMENT METHODS MOST VULNERABLE TO FRAUD

Checks Continue to be Most Vulnerable to Payments Fraud

In 2022, checks continued to be the payment method impacted most often by fraud activity; 63 percent of respondents report that their organizations faced some kind of check fraud activity, attempted or actual. Payments fraud via checks had been on the decline since 2010, with some intermittent upticks in between. Seventy percent of financial professionals reported that their organizations' check payments were subject to fraud attempts/attacks in 2018, while 74 percent reported the same for 2019. We then saw a decrease to 66 percent in 2020 and it remained unchanged in 2021.

"We had a washed check and relied on our bank to track down the errant payee."

Payment Methods Subject to Fraud by Type
(Percent of Organizations)



PAYMENT METHODS MOST VULNERABLE TO FRAUD

Contributing to the decline in check fraud is the fact that organizations are using fewer checks in their business-to-business (B2B) transactions and an increase in digital payments. According to the *2022 AFP® Electronic Payments Report*, 33 percent of organizations used checks for B2B payments in 2022, while in 2004 over 80 percent of companies used checks for similar transactions.

The share of organizations that were victims of fraud attacks via wire transfers has also been decreasing – from 48 percent in 2017 to 32 percent in 2021 and 31 percent in 2022. Companies are more efficient in detecting potential fraud and mitigating it appropriately. Results suggest a clear downward trend in wire fraud activity, indicating that the controls companies are putting in place to prevent wire fraud are effective. Fraudsters often use wires to infiltrate an organization's payment systems using email, and because in recent years companies have bolstered their efforts to control fraud via email – i.e., Business Email Compromise (BEC) – those efforts have contributed to a decrease in instances of wire fraud.

The share of respondents reporting fraud via ACH debits decreased from 37 percent in 2021 to 30 percent in 2022. The percentage of fraud activity via ACH debits had been increasing gradually – from 33 percent in 2019 to 34 percent in 2020 and to 37 percent in 2021. Time will tell whether the recent decline is the beginning of a trend or not. Potential reasons for the decline possibly include businesses having stronger procedures and tools in place, including the use of debit filters, debit blocks, etc. Also, as more payments move to digital channels, the stronger processes around ACH debits might have helped to reduce the incidence of fraud.

Fraud via ACH credits rose 6 percentage points from 2021 to 30 percent in 2022. In 2019 fraud via ACH credits accounted for 22 percent of fraud activity, then decreased slightly to 19 percent in 2020 before rising again to 24 percent in 2021 and to 30 percent in 2022. As companies move from paper to digital payment methods, the origination point of ACH credits needs further review around processes, controls and procedures. Dual approvals and proper payment backup/detail protocols should parallel those for other payment channels such as wires, Real Time Payments and Same Day ACH. In addition, organizations should continually educate their employees on how to protect their payment systems from fraudsters.

Apart from fraud via checks, wire transfers and ACH credits, attacks via corporate/commercial credit cards, faster payments, virtual cards, cryptocurrency and mobile wallets have increased from 2021 to 2022. The percentage of organization that were victims of fraud attacks via corporate/commercial credit cards rose from 26 percent to 36 percent in 2022, fraud attacks via faster payments increased from 5 percent to 8 percent and fraud attacks via cryptocurrency rose from one percent to five percent.

ASSISTANCE SOUGHT WHEN REPORTING PAYMENTS FRAUD

Banking Partners Often Sought Out for Assistance in Process to Report Payments Fraud

When looking to report payments fraud, 79 percent of respondents indicate their organizations are most likely to seek assistance from their banking partners to receive guidance about the steps to take to minimize the impact from such fraud. Since banking partners are increasingly being sought out for guidance, practitioners should ensure that when selecting banking partners those partners have experience in dealing with payments fraud and so will be able to help organizations when the need arises. If changing banks, it is a good practice for a company to incorporate a "fraud checkup" into the RFP as a requirement including requesting demos of fraud solutions for each payment type, how exceptions are handled, timing to action exceptions, and setting defaults to "not pay" if deadlines are missed. Sixty-nine percent of respondents report they would inform the security/compliance team at their organizations; this action is taken more frequently at larger organizations with annual revenue of at least $1 billion (74 percent) than at those firms with annual revenue of less than $1 billion (59 percent). Other steps being taken when reporting fraud are:

- File report with police (local, state, or federal) (cited by 38 percent of respondents)
- Inform law enforcement agencies (e.g., FBI) (35 percent)
- Inform the Federal Trade Commission (FTC) (6 percent)

ASSISTANCE SOUGHT WHEN REPORTING PAYMENTS FRAUD

Process Used to Report Payments Fraud in 2022
(Percent of Organizations)

	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
Seek assistance from our banking partner	79%	73%	84%	87%	78%
Inform internal security/compliance team	69%	59%	74%	72%	78%
File report with police (local, state or federal)	38%	30%	45%	44%	41%
Inform law enforcement agencies (e.g., FBI)	35%	30%	43%	44%	41%
Inform the Federal Trade Commission (FTC)	6%	6%	6%	7%	7%
Other • File police report in targeted country (when outside of the U.S.) • File a claim with Postmaster General's office • Depends on the fraud • File a Suspicious Activity Report (SAR)	4%	6%	3%	1%	4%

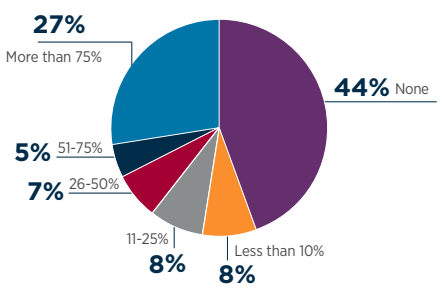
RECOUPING OF FUNDS

A Majority of Organizations Recoup Less than 10 percent of Funds Stolen Due to Fraud

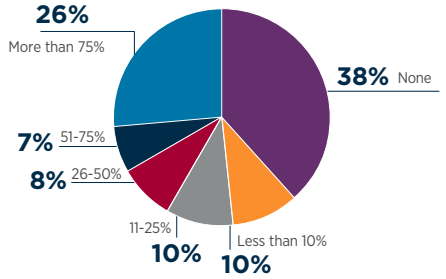
Forty-four percent of respondents indicate that after a successful fraud attempt, their organizations were unable to recover the funds lost due to the fraud. At the other end of the spectrum, 27 percent were able to recoup 75 percent of the funds lost. Larger organizations with annual revenue of at least $1 billion and more than 100 payment accounts have greater success in recovering funds lost; 41 percent of these companies were successful in regaining more than 75 percent of the funds lost due to a fraud attack and only 19 percent were unsuccessful in recouping funds. Organizations with greater revenue and with a larger volume of payment accounts are better equipped to detect fraud early. They implement systems that allow for uncovering the origins of the fraud and thus minimize the financial impact of a fraud attack.

Recoup of Funds After a Successful Fraud Attempt
(Percentage Distribution of Organizations that Experienced Fraud)

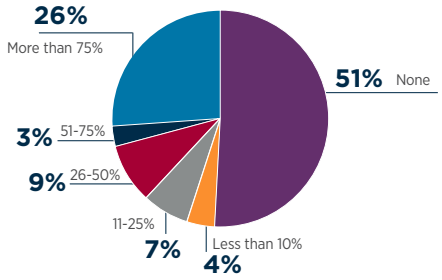
All



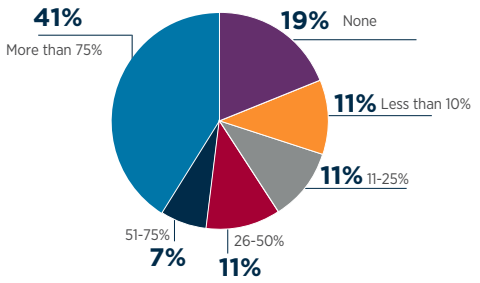
Annual Revenue At Least $1 Billion



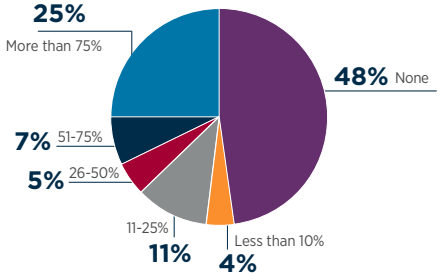
Annual Revenue Less than $1 Billion



Annual Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts



Annual Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts



ORIGINATION OF PAYMENTS FRAUD

Majority of Payments Fraud Originate from an Individual (External to Organization) and Business Email Compromise

The most-common source of payments fraud in 2022 was an external source or individual (e.g., forged check, stolen card); 54 percent of financial professionals report that payments fraud at their companies was the result of actions by an individual outside the organization. This is a slight uptick from the 51 percent reported last year (for 2021).

Fifty-three percent of fraud was a result of Business Email Compromise (BEC). In 2019, 61 percent of respondents cited BEC as a source of fraud; in 2020 the share inched upward to 62 percent. Although BEC continued to be the chief reason organizations were experiencing fraud in 2021, the share of respondents that cited BEC as a reason for payments fraud at their companies that year decreased slightly from previous years (55 percent). The percentage also decreased slightly to 53 percent in 2022, and BEC was the second most cited source of payments fraud. Larger organizations with annual revenue of at least $1 billion and with more than 100 payments accounts were more susceptible to BEC scams in 2022, while companies with less than $1 billion in annual revenue were more susceptible to fraud committed by outside individuals.

Other sources of payments fraud included vendor imposter (37 percent) and bad actor who takes over an account (20 percent) – i.e., account takeovers via hacked system, phishing, spyware or malware.

A larger share of companies with annual revenue of less than $1 billion were targeted by an outside individual (58 percent) than were those organizations with annual revenue of at least $1 billion (52 percent).

Those respondents indicating that note that an insider committed fraud at their organizations (3 percent) suggest that these individuals worked in Accounts Payable, Retail, Sales or Bookkeeping departments.

Sources of Attempted/Actual Payments Fraud Attempts in 2022
(Percent of Organizations)

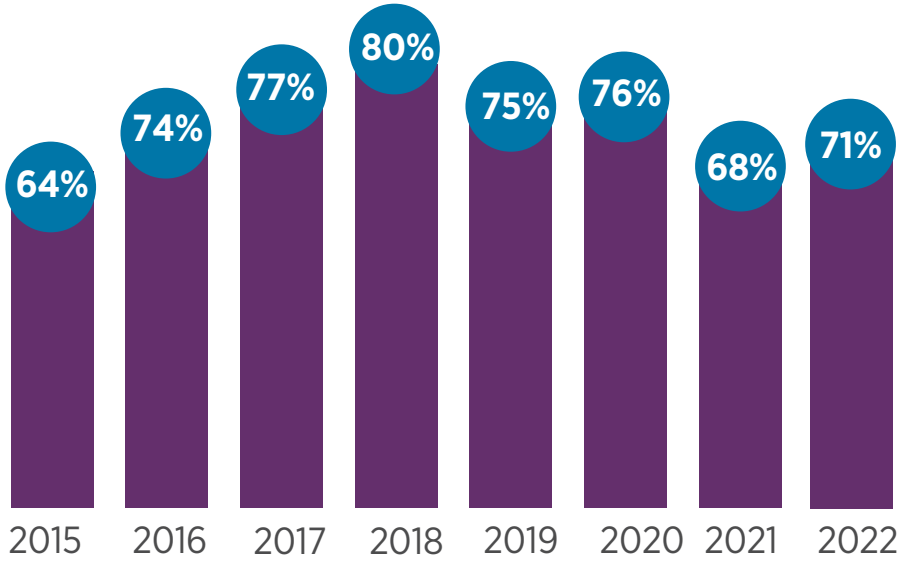
2022		Annual Revenue Less Than $1 Billion	Annual Revenue At Least $1 Billion	Annual Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Annual Revenue At Least $1 Billion and More Than 100 Payment Accounts	2021
Outside individual (e.g., check forged, stolen card, fraudster)	54%	58%	52%	49%	44%	51%
Business Email Compromise (BEC Fraud)	53%	48%	58%	62%	63%	55%
Vendor imposter	37%	29%	46%	49%	48%	–
Bad actor takes over an account, i.e., Account takeover (e.g., hacking a system, adding malicious code – spyware or malware from social network)	20%	19%	23%	17%	30%	16%
Invoice fraud	15%	9%	13%	14%	33%	–
Imposter to client posing as representative from our company	14%	6%	3%	1%	–	–
Third-party or outsourcer (e.g., vendor, professional services provider, business trading partner)	13%	12%	15%	17%	11%	18%
U.S. Postal Service Office interference	11%	7%	13%	9%	22%	–
Organized crime ring (e.g., crime spree that targets other organizations in addition to your own, either in a single city or across the country)	8%	2%	12%	12%	11%	10%
Ransomware	5%	1%	9%	8%	7%	–
Internal party (e.g., malicious insider)	3%	2%	3%	–	7%	2%
Compromised mobile device	3%	2%	2%	3%	4%	3%
Deepfake attempt (e.g., voice and/or video swapping, "deep voice" technology, vishing)	1%	–	–	–	–	–

ABOUT BUSINESS EMAIL COMPROMISE

Business Email Compromise (BEC) Events Increase Slightly

Seventy-one percent of organizations experienced attempted or actual BEC in 2022. This is a three-percentage point increase from 2021, but still a significant drop from the 80 percent reported in 2018. As has been the trend, fewer smaller organizations (with annual revenue less than $1 billion) were targets of BEC fraud than were larger organizations (with annual revenue of at least $1 billion): 63 percent compared to 82 percent. This gap has widened since 2020 when those figures were 67 percent and 78 percent, respectively.

Percent of Organizations that Experienced Business Email Compromise (2015-2022)



"We received a fraudulent email impersonating an executive officer of the company."

HOW CRIMINALS CARRY OUT BUSINESS EMAIL COMPROMISE SCAMS

"Fictitious email was sent by an imposter pretending to be a vendor requesting change in Banking information. Procurement staff changed the banking information not realizing it was fraud. The fraud was quickly detected and our Bank, the local Police and the FBI were notified. Funds were recovered."

BEC Methods

Fraudsters' approaches to BEC in 2022 were similar to those observed in previous years. Criminals carry out BEC scams in the following ways.

- Spoof an email account or website (experienced by 73 percent of organizations). Senders forge email header elements to trick users into thinking they are interacting with a trusted source.
- Use a domain lookalike (experienced by 57 percent of organizations). Bad actors register look-alike domains to confuse users into believing that they have reached a legitimate site. Visiting these sites may lead to web traffic diversion and/or malware delivery.
- Access a compromised email account (experienced by 54 percent of organizations). Fraudsters will sometimes use compromised email accounts to send fraudulent "change of payment" instructions to potential victims.

Fraudulent emails may contain attachments or links that send users to illegitimate websites or payment portals. Respondents report their firms receive these messages through texts as well as apps, including WhatsApp.

Most Prevalent Types of Business Email Compromise Fraud in 2022
(Percent of Organizations)

73%	57%	54%
Spoof email	Domain lookalike	Legitimate email that was taken over by a fraudster

BENEFICIARY VALIDATION

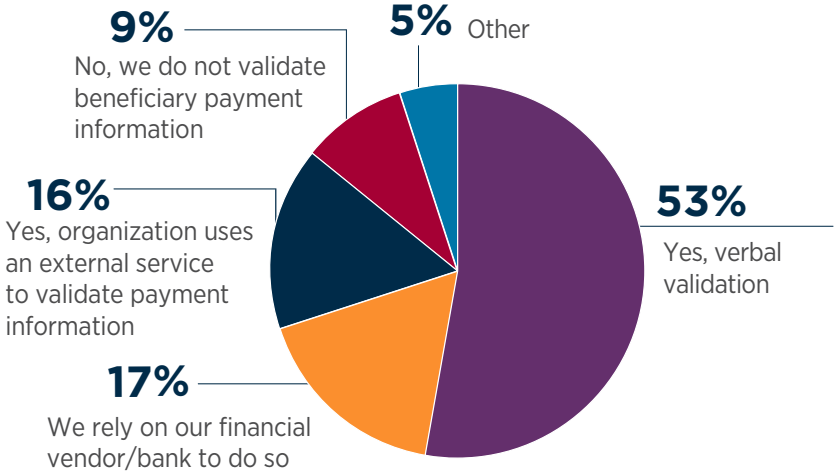
Beneficiary Validation a Common Practice at Most Organizations

Beneficiary payment validation is an important step in ensuring accurate and secure payments. When asked about the validation process for their organizations, 53 percent of respondents report that their organizations validate payments verbally. Some organizations choose to outsource validation:

- Rely on financial vendor/bank (cited by 17 percent of respondents)
- Use of an external service to validate payment information (16 percent)

Nine percent of organizations do not validate beneficiary payment. Some organizations rely on a combination of validation procedures. Verbal validation is often used in conjunction with bank letters and/or written instructions.

Validating Beneficiary Payment Details
(Percentage Distribution of Organizations)



FRAUD REVIEW

Fraud Review Process

Over 60 percent of organizations conduct fraud reviews: 36 percent conduct reviews internally while 25 percent seek the assistance of their bank/vendor. Another 12 percent have plans to conduct a review within the next year. Organizations with annual revenue of less than $1 billion are more prone to conduct reviews internally (42 percent) than are organizations with annual revenue of at least $1 billion (33 percent). In comparison, organizations with annual revenue of at least $1 billion (30 percent) are more likely to seek the assistance of their bank/vendor than are organizations with less annual revenue (21 percent).

At a majority of organizations, Treasury is responsible for the oversight of the fraud review process (cited by 56 percent of respondents). Other departments that have oversight of the fraud review process are:

- Risk (cited by 42 percent of respondents)
- Accounts Payable (37 percent)
- IT (35 percent)

A greater percentage of Risk departments at organizations with annual revenue of at least $1 billion and more than 100 payment accounts are responsible for fraud review than are similar sized companies with fewer payment accounts (64 percent versus 42 percent).

"Attempted fraud was discovered by our supplier setup team calling an established vendor and confirming they had not changed banks, per the email we received."

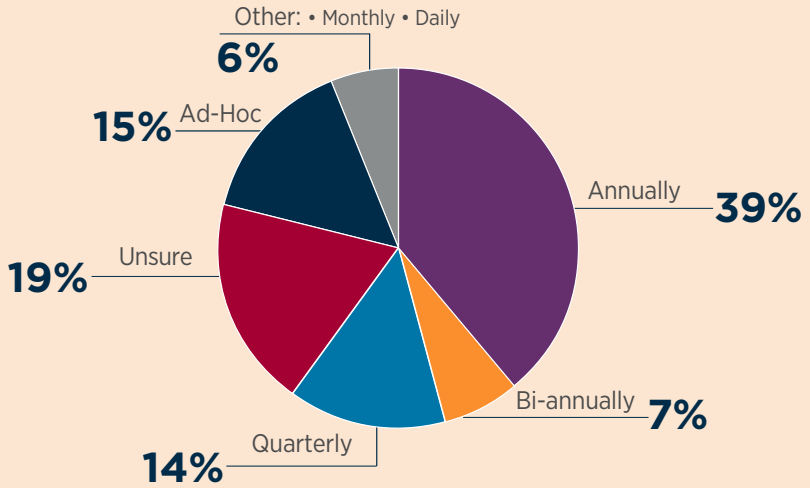
Fraud Review Process
(Percentage Distribution of Organizations)

	All	Annual Revenue Less Than $1 Billion	Annual Revenue At Least $1 Billion
Conduct an internal independent review	36%	42%	33%
Conduct review with the assistance of bank/vendor	25%	21%	30%
Planning to conduct a review within the next year	12%	10%	14%
Do not conduct fraud reviews	27%	27%	24%

FRAUD REVIEW

Fraud review is conducted annually at 39 percent of organizations and conducted more frequently at 21 percent of organizations, either once a quarter or twice a year. Some respondents indicate that these reviews are conducted on an ad-hoc basis at their organizations, and 19 percent are unsure about the frequency that fraud reviews are conducted at their companies.

Frequency of Fraud Review
(Percentage Distribution of Organizations)



CONCLUSION

There are clear signs that payments fraud is abating. After record levels of fraud in both 2018 and 2019 – peaking at over 80 percent – the share of organizations that were targets of attempted/actual payments fraud has been on the decline since. Checks continue to be a prime target for criminals, but with the declining use of checks – and very effective tools to stop check fraud – fraudsters have been having less success. According to the *2022 AFP® Electronic Payments Report*, 33 percent of organizations used checks for business-to-business payments in 2022, while in 2019, 43 percent of companies did so. Because many organizations are unable to eliminate the use of checks completely, fraudsters continue to be able to use checks to target organizations, although perhaps to a lesser extent. Unfortunately, criminals are not easily discouraged; advanced software and social engineering enables them to attempt payments fraud through other payment methods such as wires and ACH payments.

Emails are frequently used to infiltrate company networks. In the current business environment, employees are likely physically distanced; consequently, verbal verification of payment requests become more challenging. Unless formal systems are in place and ingrained in employees, fraud can often occur. Business leaders have made training and education focused on detecting phishing attempts a priority for employees. Indeed, many organizations do not restrict training to just the finance teams, but instead require that employees throughout the entire organization be cognizant about fraud attempts via email and be able to identify them. Employees who inadvertently open emails multiple times which are either actual fraud attacks or simulated phishing attempts are reprimanded, and in some extreme cases may be terminated from their jobs. Despite extensive measures implemented to prevent Business Email Compromise, it continues to be one of the primary sources of fraud at organizations.

The share of organizations experiencing corporate/commercial credit card fraud increased 10 percentage points, from 26 percent in 2021 to 36 percent in 2022. This uptick is similar to the incidence of credit card fraud reported prior to the COVID-19 pandemic in 2019 – 34 percent. As a consequence of the pandemic, organizations reduced workforce, furloughed employees and trimmed discretionary spending by restricting travel. The use of corporate/commercial credit cards also decreased, resulting in fewer card transactions and, therefore, less fraud via that payment method than was reported in 2020 and 2021. As employers are recruiting again and organizations have eased restrictions on travel and other discretionary spending, corporate/commercial credit cards are being used more extensively, resulting in greater incidence of fraud being reported via those payment methods.

Call backs, daily reconciliations and verbal verifications are methods many organizations are using in their efforts to minimize the occurrence of fraud via payment methods. Treasury and finance leaders are increasingly reaching out to banking partners for guidance in reporting and managing fraud. Depending on the extent of the fraud, practitioners are also reporting fraud to police and other law enforcement agencies.

In the past, actual financial losses from payments fraud attacks were not damaging; that continued to be the case in 2022. However, this is not a reason for companies to lose focus on preventing fraud. While loss of confidential and personnel information does not directly impact an organization's bottom line, extensive effort and resources are required to resolve such situations.

It is evident that the steps business leaders are taking to prevent fraud are having success. However, historical payments fraud survey data show different types of fraud emerge in the wake of such success. Fraudsters are relentless and will continue to target organizations and any vulnerable payment networks. Therefore, treasury leaders will want to ensure that they are prepared for the next type of fraud that is in the works. It is vital that treasury and finance professionals stay ahead of the perpetrators so that fraud attacks do not interrupt business operations and organizations' financial losses remain at a minimum.

ABOUT SURVEY RESPONDENTS

In January 2023, the Research Department of the Association for Financial Professionals® (AFP) surveyed treasury practitioner members and prospects. The survey was sent to treasury professionals with the following job titles: Vice President of Treasury, Treasurer, Assistant Treasurer, Director of Treasury, Treasury Manager, Director of Treasury and Finance, Senior Treasury Analyst, and Cash Manager. A total of 471 responses were received from practitioners, which form the basis of the report.

AFP thanks J.P. Morgan for underwriting the *2023 AFP® Payments Fraud and Control Survey.*

Both the questionnaire design and the final report, along with its content and conclusions, are the sole responsibilities of the AFP Research Department. The following tables provide a profile of the survey respondents, including payment types used and accepted.

Type of Organization's Payment Transactions
(Percentage Distribution of Organizations)

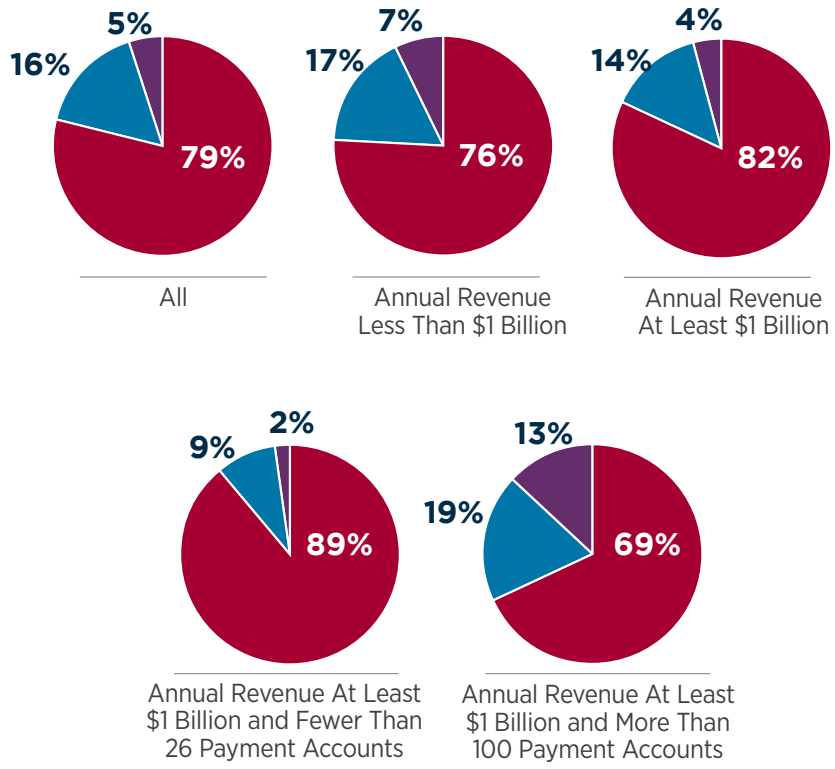
	Primarily consumers	Split between consumers and businesses	Primarily businesses
When making payments	9%	27%	64%
When receiving payments	21%	29%	50%

Number of Payment Accounts Maintained
(Percentage Distribution of Organizations)

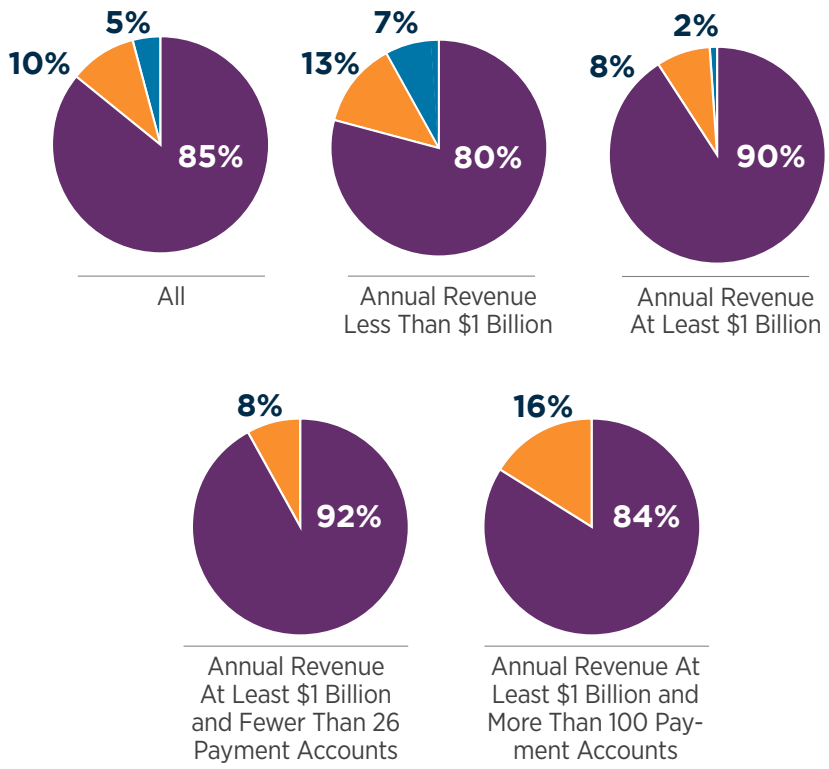
	All	Annual Revenue Less Than $1 Billion	Annual Revenue At Least $1 Billion	Annual Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Annual Revenue At Least $1 Billion and More Than 100 PaymentAccounts
Fewer than 5	24%	32%	17%	28%	_
5-9	23%	24%	23%	38%	_
10-25	19%	18%	21%	34%	_
26-50	9%	10%	8%	_	_
51-100	10%	6%	12%	_	_
More than 100	15%	9%	19%	_	100%

ABOUT SURVEY RESPONDENTS

Methods to Maintain Payments Accounts
(Percentage Distribution of Organizations)

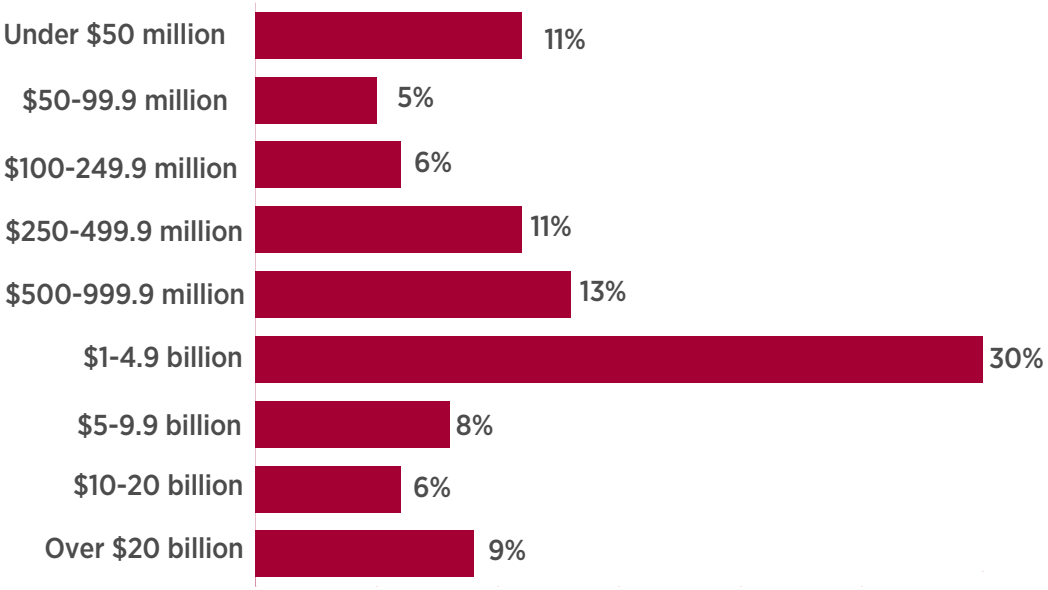


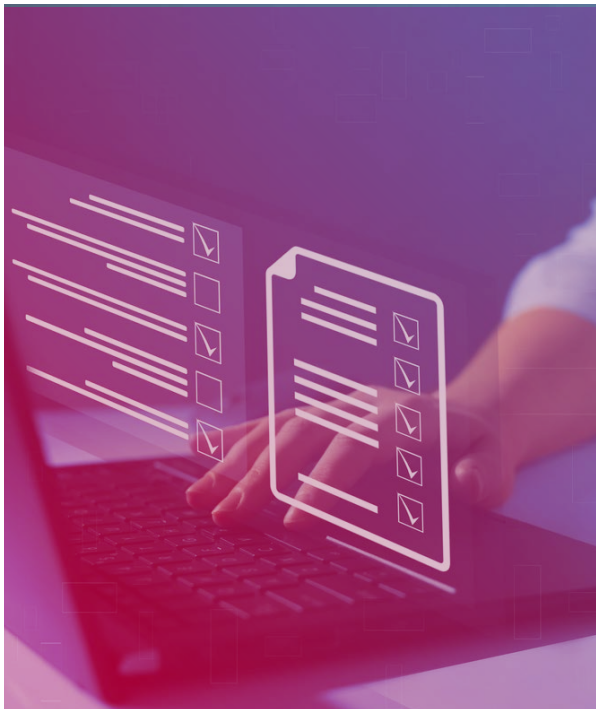
Application of Accounts Controls
(Percentage Distribution of Organizations)



ABOUT SURVEY RESPONDENTS

Annual Revenue (USD)
(Percentage Distribution of Organizations)





Organization's Ownership Type
(Percentage Distribution of Organizations)

	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 PaymentAccounts
Publicly owned	35%	15%	51%	49%	59%
Privately held	41%	53%	30%	33%	28%
Non-profit (not-for-profit)	16%	22%	11%	8%	6%
Government (or government owned entity)	9%	10%	8%	10%	6%

ABOUT SURVEY RESPONDENTS

Industry Classification
(Percentage Distribution of Organizations)

	ALL
Agricultural, Forestry, Fishing & Hunting	–
Administrative Support/Business services/Consulting	1%
Banking/Financial services	14%
Construction	4%
E-Commerce	2%
Education (K-12, public or private institution)	2%
University or other Higher Education	4%
Energy	5%
Government	6%
Health Care and Social Assistance	9%
Hospitality/Travel/Food Services	2%
Insurance	5%
Manufacturing	17%
Mining	–
Non-profit	5%
Petroleum	1%
Professional/Scientific/Technical Services	3%
Real estate/Rental/Leasing	4%
Retail Trade	4%
Wholesale Distribution	5%
Software/Technology	2%
Telecommunications/Media	1%
Transportation and Warehousing	3%
Utilities	2%

All inquiries should be addressed to:

Association for Financial Professionals

4520 East West Highway, Suite 800

Bethesda, MD 20814

Phone: 301.907.2862 Fax: 301.907.2864 E-mail: AFP@AFPonline.org

Web: www.AFPonline.org

AFP Research

AFP Research provides financial professionals with proprietary and timely research that drives business performance. AFP Research draws on the knowledge of the Association's members and its subject matter experts in areas that include bank relationship management, risk management, payments, FP&A and financial accounting and reporting. Studies report on a variety of topics, including AFP's annual compensation survey, are available online at www.AFPonline.org/research.

About AFP®

Headquartered outside of Washington, D.C. and located regionally in Singapore, the Association for Financial Professionals (AFP) is the professional society committed to advancing the success of treasury and finance members and their organizations. AFP established and administers the Certified Treasury Professional® and Certified Corporate FP&A Professional® credentials, which set standards of excellence in treasury and finance. Each year, AFP hosts the largest networking conference worldwide for more than 7,000 corporate financial professionals.

4520 East-West Highway, Suite 800

Bethesda, MD 20814

+1 301.907.2862

www.AFPonline.org

J.P.Morgan

The threat of fraud is real

The question is, are you ready?

As fraud becomes more sophisticated, so does our approach to security. Get the critical information and advanced tools you need to safeguard your organization.

LEARN MORE

or contact your J.P. Morgan representative today.