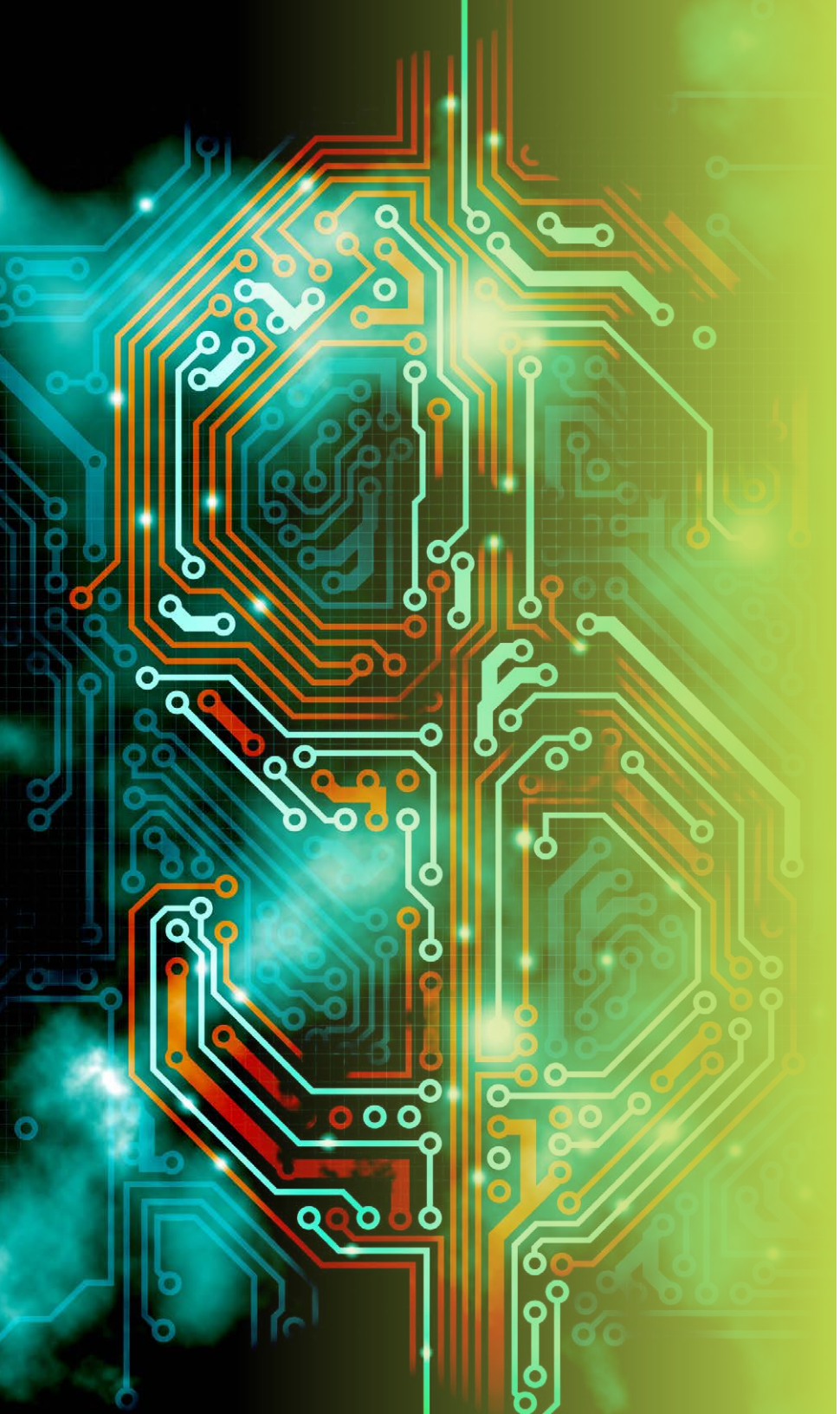
AFP® ASSOCIATION FOR FINANCIAL PROFESSIONALS

Underwritten by

TRUIST

2024 AFP® PAYMENTS FRAUD AND CONTROL SURVEY REPORT

Key Highlights



2024 AFP®
PAYMENTS FRAUD AND CONTROL SURVEY REPORT
KEY HIGHLIGHTS

APRIL 2024

This summary report includes highlights from the comprehensive *2024 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

TRUIST

Truist is proud to share the results of the *2024 AFP® Payments Fraud and Control Survey*. This is the first year Truist has sponsored the survey – and it's part of our ongoing efforts to help businesses manage their payments with simplicity, speed and safety.

The survey results demonstrate that there is an opportunity for organizations to strengthen their fraud controls. Fraudsters are constantly evolving their schemes, and traditional payment methods such as ACH and checks remain vulnerable, while Business Email Compromise (BEC) remains a significant threat.

Some key findings from the survey include:

- The decline in reported payments fraud was short-lived: 80% of organizations reported having been targets of payments fraud activity in 2023, an increase from 65% in 2022.
- Checks continue to be the payment method most susceptible to fraud, as reported by 65% of respondents.
- Furthermore, 70% of organizations using checks have no immediate plans to discontinue their use.
- For the first time since AFP began conducting the payments fraud survey, ACH credits have surpassed wires as the most vulnerable payment type for BEC fraud.
- 63% of organizations experienced some form of BEC in 2023.

Truist's payments professionals work each day to help ensure businesses deliver and receive payments securely. I hope this report provides valuable insights that can help you safeguard your organization and customers.

Regards,

Chris Ward
Head of Enterprise Payments
Truist

TRUIST

TOPICS COVERED IN THE COMPREHENSIVE 2024 AFP® PAYMENTS FRAUD AND CONTROL SURVEY REPORT

Payments Fraud Overview

- Payments Fraud Trends
- Payment Methods Impacted by Fraud
- Losses Incurred Due to Payments Fraud Attacks/Attempts
- Recovering Lost Funds
- Detecting Fraud Activity
- Primary Sources of Attempted/Actual Payments Fraud
- Assistance Sought When Reporting Payments Fraud

Business Email Compromise

- About Business Email Compromise (BEC)
- Business Email Compromise Scams Are Only Getting Better
- Financial Impact of Business Email Compromise
- Payment Methods Impacted by BEC
- Departments Vulnerable to Email Scams

Check Usage

- Checks Continue to be a Popular Payment Method

Payments Fraud Overview

- Business Email Compromise Prevention – Policies and Procedures
- Business Email Compromise Prevention – Security and Compliance Measures
- Preventing BEC
- Check Fraud Controls
- Effective ACH Controls
- Managing Faster Payments
- Validation of Beneficiary Payment Information
- Measures to Improve Controls

INTRODUCTION

Examining the payments fraud landscape in 2023, we see an uptick in fraud activity from the previous year, with 80% of organizations reporting they were a victim of an attempted or actual fraud attack. Despite heightened awareness at organizations about payments fraud and the controls and processes put in place to safeguard organizations' payment systems and minimize instances of fraud, it is clear that perpetrators of fraud are relentless. They are continuously devising ways to infiltrate payment systems at organizations.

Email continues to be a pervasive method used by criminals to target organizations. Criminals are attracted to using email as it is a low-cost avenue through which to conduct fraud, and if successful can cause significant financial losses. Initially, organizations were unprepared for fraud initiated via email; unsuspecting employees were often deceived, resulting in organizations falling prey to this crime. But over time, organizations put systems in place to reduce the chances of their employees being deceived. Such controls range from flagging external emails and alerting employees to intensive training for staff so they are effectively able to detect fraudulent emails.

Checks continue to be a popular payment method targeted for fraud at many organizations, but survey results signal that many organizations will likely continue to use checks over the next few years. Seventy-five percent of survey respondents report that their organizations use checks, and nearly 70% of these organizations do not have plans to discontinue the use of checks over the next two years.

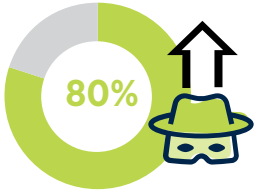
While fraud perpetrators often use technology to carry out their fraud attacks, they are also resorting to methods which are not fueled by technology. In February 2023, the Financial Crimes Enforcement Network (FinCen)[1] alerted financial institutions about check fraud schemes targeting the U.S. Mail (USPS). Fraudsters were intercepting mailed checks, washing them and altering payee information. Initially individuals were being targeted when criminals raided the blue neighborhood USPS mailboxes. Mailed checks were intercepted, altered and inadvertently cashed by unsuspecting bank employees. It was only when individuals questioned a charge they did not recognize in their statements did they realize they had been a victim of a fraud attack. Businesses, too, have become an attractive target for this type of fraud as they continue to use checks extensively. Twenty-one percent of respondents report that their organizations had been victims of USPS interference, a 10-percentage-point increase from the 2023 survey findings (reflecting the experience during 2022). If organizations plan to continue using checks, Accounts Payable teams need to be cognizant of the risks involved with this payment method, ensure that payments via checks are traceable, and that controls such as positive pay are utilized to curb the success of this payments fraud via checks.

Every year since 2005, the Association for Financial Professionals® (AFP) has conducted its *Payments Fraud Survey*. Continuing this research, AFP conducted the 20th Annual *Payments Fraud and Control Survey* in January 2024. The survey examines the nature of and the extent of fraud attacks on business-to-business (B2B) transactions, the payment methods impacted, the increasing role of business email compromise in payments fraud, and the strategies organizations are adopting to protect themselves from fraud attempts. This year's survey generated 522 responses from corporate practitioners from organizations of varying sizes representing a broad range of industries. Results presented in this report reflect data for 2023. Survey respondent demographics are available at the end of this report.

AFP thanks Truist for its underwriting support of the *2024 AFP® Payments Fraud and Control Survey*. Both questionnaire design and the final report, along with its content and conclusions, are the sole responsibility of AFP's Research Department.

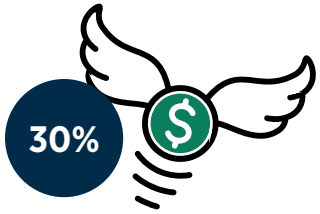
[1]FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail, February 27, 2023, Financial Crimes Enforcement Network

KEY FINDINGS



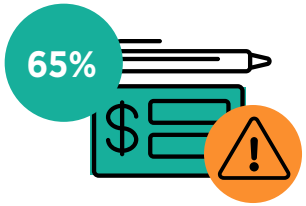
Payments Fraud Activity on the Rise

Overall, 80% of organizations were targets of either an actual or attempted payments fraud attack in 2023. This is an uptick of 15 percentage points from 2022. Organizations most impacted by fraud were those with at least $1 billion in revenue and fewer than 26 payments accounts (86%).



Discovering Fraud

Thirty percent of respondents report that after a successful fraud attempt, their organizations were unable to recover the funds lost due to fraud. At the other end of the spectrum, 29% were able to recoup up to 75% of the funds lost and 41% were successful in recouping more than 75% of the funds lost (mostly via checks).



Checks Continue to be Vulnerable to Fraud

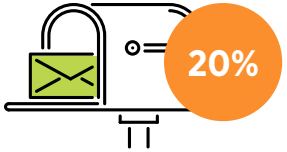
Checks continue to be the payment method most susceptible to fraud, as reported by 65% of respondents. Seventy percent of organizations using checks have no immediate plans to discontinue their use. The primary reason for continued check use is the requirement for checks by small businesses.

Email Targets ACH Credits

This year, ACH credits have surpassed wires as the most vulnerable payment type for BEC fraud. Even as most payment methods continue to be vulnerable to BEC, payments made via ACH credits (47%), wire transfers (39%) and ACH debits (20%) were most often targeted.

Business Email Compromise (BEC) Controls Have Room for Improvement

Less than 60% of organizations have completed the documentation that includes the creation of written policies and procedures which are required to safeguard against BEC, while less than half (49%) have completed testing these policies. Although BEC has been prevalent for over a decade, findings reveal a gap in preparedness to mitigate scams via email.



Organizations Overlook the Vulnerability of Payments Sent by USPS

Over 20% of respondents report fraud due to interference with the United States Postal Service (USPS), which is 10 percentage points higher than the share reported for 2022. Despite alerts from the Financial Crimes Enforcement Network (FinCEN)[2] regarding increased fraud attempts via mail interception, over 80% of respondents indicate their organizations still deliver checks via the United States Postal Service (USPS) — without tracking.

[2] https://www.fincen.gov/reports/sar-stats

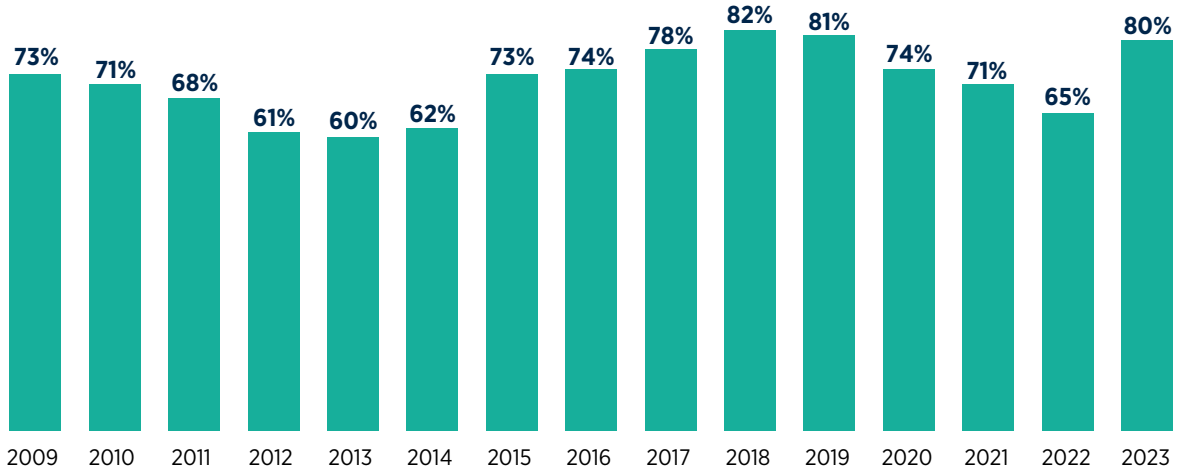
PAYMENTS FRAUD TRENDS

Percentage of Organizations That Are Victims of Payments Fraud Attacks on the Rise

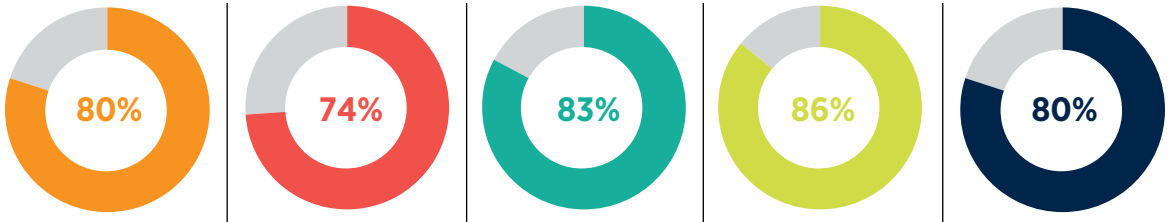
From 2009-2013, the percentage of organizations that experienced attempted or actual payments fraud steadily declined. In 2015, there was an uptick in the share of companies that were victims of payments fraud attempts and attacks: 73% of organizations were targets of payments fraud in 2015 – a significant 11-percentage-point increase from 2014. That upward trend continued: 74% of financial professionals reported that their companies were victims of payments fraud in 2016, peaking in 2018 at 82%. In 2019, 81% of organizations were targets of attempted/actual payments fraud, just shy of the previous year's record-setting 82%. In 2020, the incidence of payments fraud decreased to 74% and further decreased the following year to 71%. In last year's survey (reflecting data for 2022) we saw a decline from prior years with 65% of organizations reporting they had been victims of either a fraud attack or attempt. The pattern ended in 2023, with 80% of organizations reporting having been targets of payments fraud activity.

Larger organizations (with annual revenue of at least $1 billion) are more susceptible to payments fraud attacks than are smaller ones (with annual revenue of less than $1 billion): 83% compared to 74%. A greater share of survey respondents from larger organizations and those with smaller number of payment accounts – i.e., those with annual revenue of at least $1 billion and with fewer than 26 payment accounts – report that their companies experienced payments fraud in 2023 compared with the share of respondents from other organizations.

Prevalence of Attempted/Actual Payments Fraud in 2023
(Percent of Organizations)



Prevalence of Attempted/Actual Payments Fraud in 2023
(Percent of Organizations)



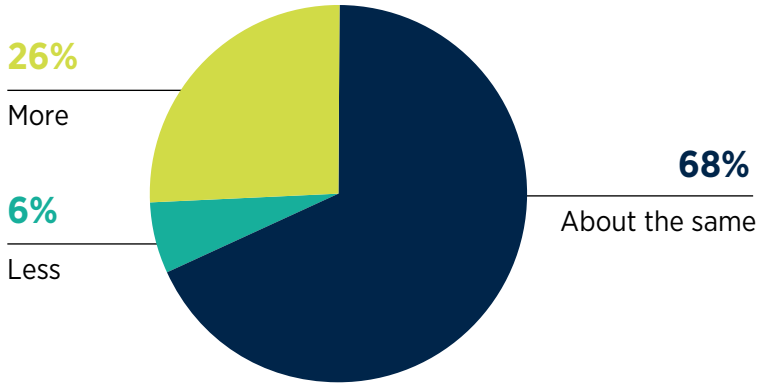
Uptick in Fraud at 26 Percent of Companies

Sixty-eight percent of financial professionals report that the incidence of payments fraud in 2023 was unchanged from that in 2022, while 26% indicate there *had* been an increase and 6% report a decline. The share of financial professionals reporting an increase in payments fraud activity has steadily declined – from 34% in 2019 to 30% in 2020 and to 29% in both 2021 and 2022. A larger percentage of respondents from organizations with annual revenue of less than $1 billion report there was an increase in payments fraud occurrences at their companies in 2023 compared to the share of organizations with annual revenue of at least $1 billion (31% and 26%, respectively).

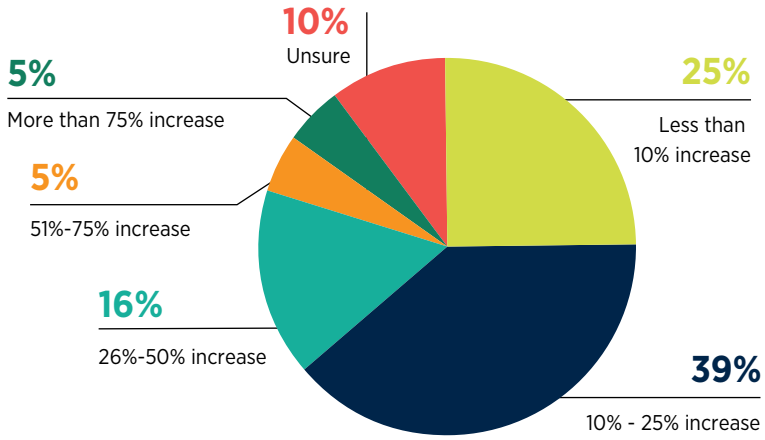
Of those organizations that report having experienced an increase in fraud activity in 2023, over two-thirds experienced an increase of less than 25%.

"We had a sophisticated account takeover fraud event started by a bad actor establishing a website that looked like our secure portal, then paying a Google sponsorship to make the phony website the first Google search result. As a result, the fraudsters were able to harvest credentials from many users, then use those credentials to attempt to change bank account information for disbursements."

Change in Incidence of Payments Fraud in 2023
(Percentage Distribution of Organizations Experiencing Payments Fraud)



Increase in Fraud over Last Year
(Percentage Distribution of Organizations Reporting More Payments Fraud Attempts in 2023 than in 2022)



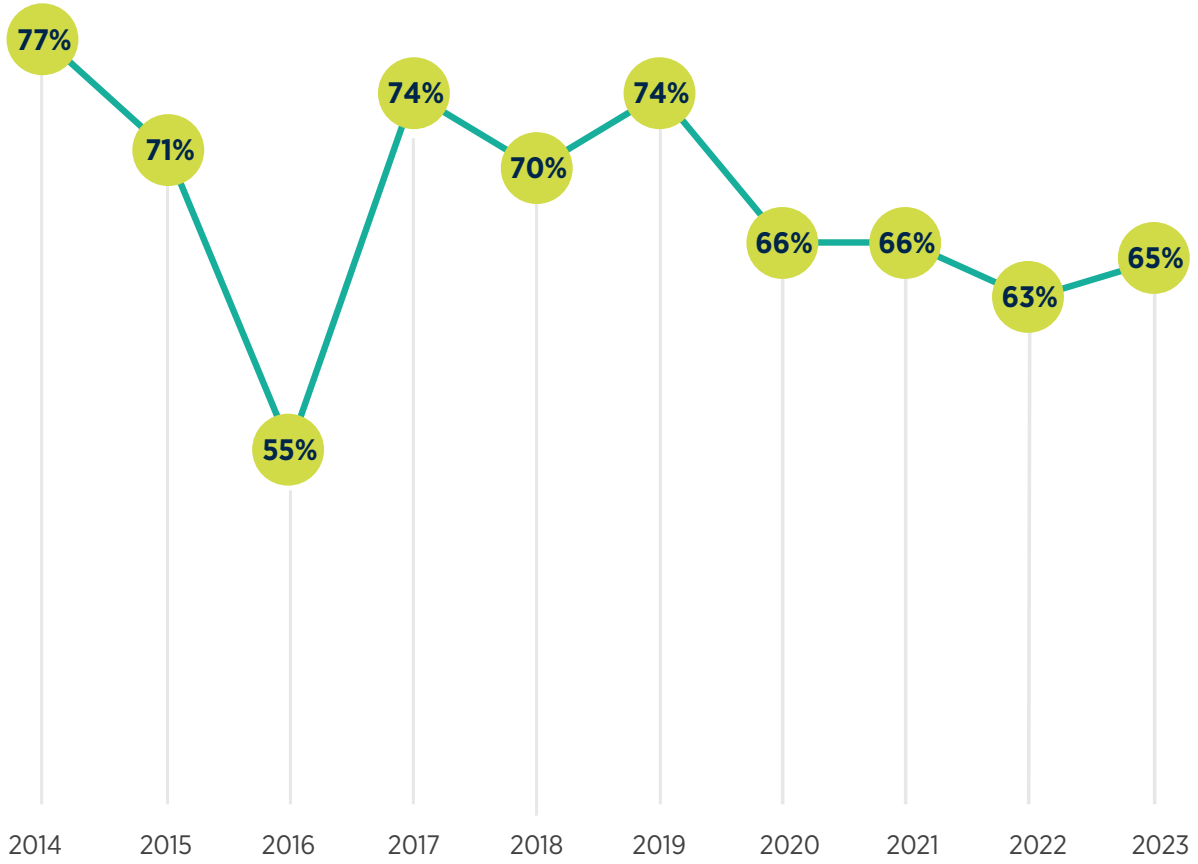
PAYMENT METHODS IMPACTED BY FRAUD

Checks and ACH Debits Most Susceptible to Payments Fraud

In 2023, checks and ACH debits were the payment methods most impacted by fraud activity (65% and 33%, respectively). Payments fraud via checks had been on the decline since 2010, with some intermittent upticks in subsequent years. Seventy percent of financial professionals reported that their organizations' check payments were subject to fraud attempts/attacks in 2018, while 74% reported the same for 2019. We then saw a decrease to 66% in 2020; this was unchanged in 2021. In 2022, a slightly smaller share (63%) of organizations were targets of fraud via checks, and this figure remained relatively stable in 2023, with 65% of respondents reporting their organizations had been victims of check fraud.

The fact that check fraud remains the most prevalent form of payments fraud is not surprising. Checks continue to be the payment method most often used by organizations. In this survey, 75% of respondents note that checks are being used at their organizations, with 34% reporting that over 25% of their payments are made via checks. (Later in this report, we discuss check usage in more detail.) The volume of checks processed by the Federal Reserve declined 8% over the past five years. Despite declining check volumes, the number of Suspicious Activity Reports (SARs), as reported by FinCEN, have increased.[3] In the last three years, there was an increase of SARs for checks (an increase of 40%) and mail (an increase of 57%). Check fraud related to mail theft has become a significant issue for organizations and, more importantly, for the banking industry as they are easy targets for check fraud via mail.

Check Fraud Activity: Trends
(Percent of Organizations)



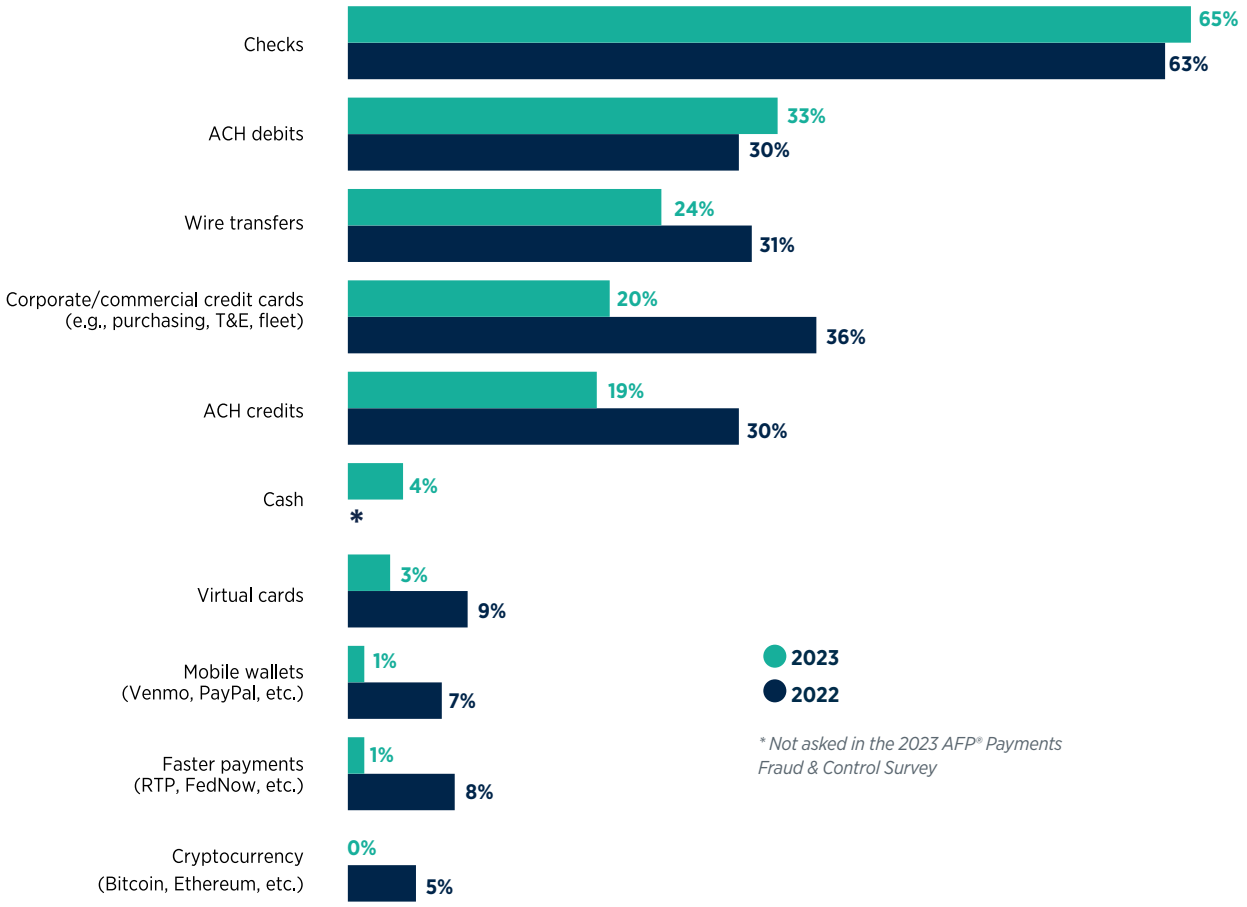
[3] https://www.fincen.gov/reports/sar-stats

The share of respondents reporting fraud via ACH debits increased from 30% in 2022 to 33% in 2023. This small increase could be connected to the uptick in the incidence of check fraud. Fraudsters are creating an ACH debit with stolen check information. The incidence of payments fraud via wire transfers decreased from 31% in 2022 to 24% 2023. The percentage of organizations that were victims of fraud via wire transfer has been on a steady decline – 48% in 2017, 45% in 2018, 40% in 2019, 39% in 2020 and 32% in 2021. Companies have become better at identifying wire fraud attempted via business email compromise (BEC) scams; the steady decline in such fraud is proof that companies' efforts to combat payments fraud via wire transfers continue to work.

The share of organizations that were victims of fraud attacks via corporate/commercial credit cards decreased significantly – from 36% in 2022 to 20% in 2023 – as did attacks via ACH credits – down from 30% in 2022 to 19% in 2023.

Respondents from organizations with annual revenue of at least $1 billion are more likely than those from other companies to report checks were subject to attempted or actual payments fraud in 2023 (72% compared to 52% for organizations with annual revenue less than $1 billion).

Payment Methods Subject to Attempted/Actual Payments Fraud
(Percent of Organizations)



"ACH fraud occurred in an instance where the instructions were changed – by request – to change from check to ACH; the ACH went to the fraudster's account. It was caught quickly and by working with the bank we were able to get 100% of the transfer credited back to our account."

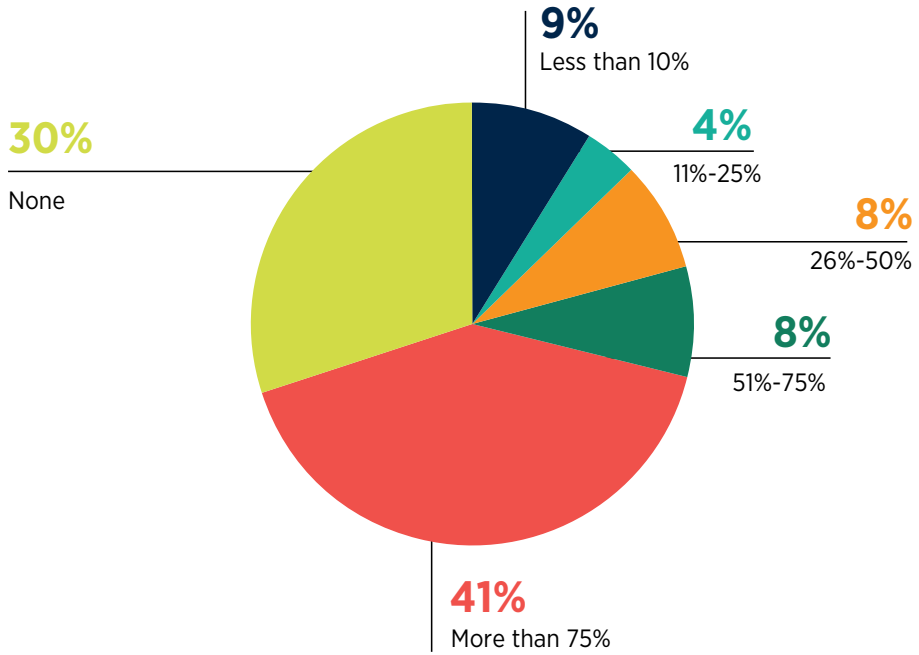
RECOVERING LOST FUNDS

Nearly 40% of Organizations Recoup Less than 10% of Funds Stolen Due to Fraud

Thirty percent of respondents report 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, 29% were able to recoup up to 75% of the funds lost and 41% were successful in recouping more than 75% of the funds lost.

"Even though we knew the day before the ACH payment settlement date, we could not stop the payment to the fraudulent account. I wish I had known to contact the FBI's Internet Crime Complaint Center (ic3.gov) immediately, as it can disregard privacy controls the banks have in place and may have been able to freeze the account."

Percentage of Lost Funds Recovered
(Percentage Distribution of Organizations Experiencing Payments Fraud)



PAYMENT METHODS IMPACTED BY BEC

ACH Payments Frequently Targeted by Fraudsters

Most payment methods continue to be vulnerable to BEC. Payments made via ACH credits (47%), wire transfers (39%) and ACH debits (20%) were the ones most often targeted. Checks (18%) rank a close fourth. Forty-seven percent of all respondents report ACH credits as the payment method most impacted by BEC. For those organizations with annual revenue less than $1 billion, the share increases to 57%, while for organizations with annual revenue of at least $1 billion and with more than 100 payment accounts, the percentage shrinks to 20%. For wire transfers, the incidence is reversed. Eighty percent of respondents from organizations with annual revenue of at least $1 billion and with more than 100 payment accounts report that wire transfers are the most targeted payment method, while 29% of organizations with annual revenue less than $1 billion report the same.

In this year's survey, ACH credits replaced wire transfers as the payment method most often targeted in BEC. The share of respondents citing wire transfers as the most often used payment method exploited via BEC declined 6 percentage points from 2022 to 39%. ACH credits are reported as the most often used payment method targeted in BEC by 47% of respondents, a 13-percentage-point increase from 2022. The share of respondents reporting that ACH debits were used by fraudsters to infiltrate organizations via email scams decreased in 2023 by 6 percentage points.

The shift to targeting ACH transactions through BEC is likely because ACH transactions are typically done in batches, and for the large payors, those transactions originate from Accounts Payable which is considered to be most susceptible to BEC scams. Furthermore, treasury typically processes fewer transactions than does Accounts Payable. Also, for Accounts Payable, payments could originate from a compromised employee who inputs false information into the procurement system, or changes vendor bank account details without proper validation as part of the vendor master process. In 2023, half of companies with annual revenue of at least $1 billion and fewer than 26 accounts had ACH credits targeted. For this segment, wire transfers were targeted 30% of the time, and ACH debits, 23%.

For the first time, real-time payments is included as one of the payment methods. Overall, one percent of respondents indicate real-time payments were targeted via BEC. For organizations with annual revenue less than $1 billion, this share increased to five percent.

Larger companies are more often targets for fraud, as criminals take advantage of organizational process differences, system differences and multiple locations. Organizations with at least $1 billion in annual revenue and more than 100 payment accounts could operate in a decentralized manner and possibly have more global operations/locations, making them attractive targets for payments fraud -- especially via wires. Employees who have a touchpoint with payment initiation and release must be trained to be vigilant in detecting suspicious activity. Banks are the number-one source for information; therefore, asking about products that will help with the centralization of payments – in addition to asking for training on various bank products used – is also important.

"Vendor management is decentralized to multiple departments, as result there is an increased penetration risk. We will be reassessing the end-to-end vendor management/bank information change process to determine if centralization makes more sense for the organization. In addition, looking to add AVS as an additional layer in the ACH/Wire verification process."

Payment Methods Utilized in Business Email Compromise

(Percent of Organizations Experiencing Payments Fraud)

	2023	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	2022
ACH credits	47%	57%	43%	50%	20%	34%
Wire transfers	39%	29%	43%	30%	80%	45%
ACH debits	20%	14%	23%	23%	27%	26%
Checks	18%	14%	19%	13%	20%	16%
Corporate/commercial credit cards (e.g., purchasing, T&E, fleet)	7%	5%	8%	3%	13%	8%
Gift cards	4%	--	6%	3%	7%	4%
Virtual cards	3%	--	4%	3%	7%	4%
Third-party pay-outs, e.g., Venmo, PayPal, Zelle etc.	3%	5%	2%	--	7%	5%
Real-time Payments (RTP, FedNow)	1%	5%	--	--	--	*

**not asked in 2022*

The table to the right highlights the usage trends for the four payment methods most impacted by BEC. While the figures for checks impacted by BEC have remained relatively steady, there has been a sharp increase in the targeting of ACH credits – from 34% in 2022 to 47% in 2023. Wire transfers and ACH debits both experienced a 6-percentage-point decrease in having been targeted via BEC from 2022 to 2023.

Top Payment Methods Impacted by Business Email Compromise, 2019-2023

(Percent of Organizations)

	2023	2022	2021	2020	2019
ACH credits	47%	34%	41%	34%	37%
Wire transfer	39%	45%	41%	43%	42%
ACH debits	20%	26%	14%	16%	21%
Checks	18%	16%	19%	14%	19%

Disbursing Checks

The most often used procedure being followed at companies on realizing their checks have been lost, stolen or damage is to issue a stop payment (75 percent) and if they have used positive pay, they issue a void (72 percent). As noted earlier, over 90 percent of organizations have implemented positive pay.

Methods for Disbursing Checks

(Percent of Organizations Using Checks)

	2023	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
USPS general mail (without tracking)	82%	79%	83%	85%	78%
Commercial carrier (FedEx, UPS, DHL, etc.)	51%	50%	52%	52%	50%
USPS with tracking	26%	23%	27%	25%	35%
Hand/Courier delivery	20%	17%	21%	25%	15%
eCheck	17%	20%	15%	11%	23%

Other includes:

- Bank handles all steps of issuing and dispersing checks
- Outsourced to third-party

"A group of individuals used bank routing and account information obtained from a company check to make various payments online."

"Fraudsters stole a batch of checks from a U.S. Postal Service box. We discovered this because several checks appeared in our payee positive pay filter at once. We placed stop payments on the remaining checks in the batch, as we were confident they had been stolen as well."

PREVENTING BUSINESS EMAIL COMPROMISE

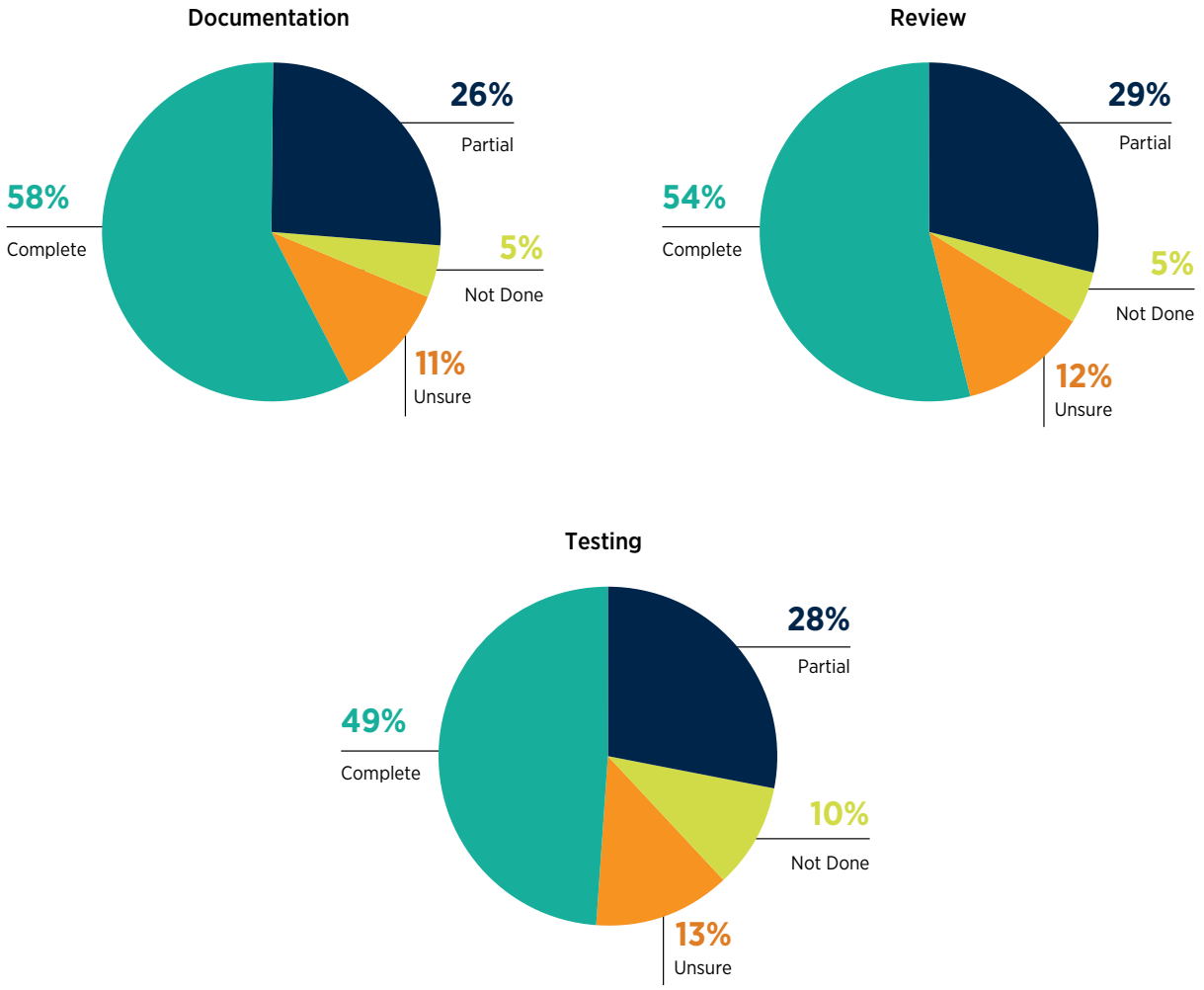
Roll-out of Policies and Procedures Designed to Prevent Business Email Compromise

With an increase in both the quantity and quality of BEC attacks, organizations need to be intentional about creating policies and procedures designed to not only limit their exposure to such attacks, but to also minimize the impact of the fraud. As noted in the previous section of this report (see page 21), a variety of policies and methodologies are working for organizations, but that can only happen if companies employ a targeted approach to the systemic application.

Of those organizations with BEC preventions and policies in the documentation stage, 58% have completed the necessary documentation while 54% of respondents have completed reviewing BEC policies and procedures. Nearly half of respondents indicate that their organizations have completed the testing stage.

.

Status of Organizational Policies and Procedures Designed to Prevent Business Email Compromise
(Percentage Distribution of Organizations)



CONCLUSION

The findings of the *2023 AFP® Payments Fraud and Control Survey* show that while there had been a steady decline in overall payments fraud activity from 2018 to 2022, in 2023 fraud attempts were on the upswing. Eighty percent of organizations experienced actual or attempted payments fraud last year, up from 65% in 2022. While it is hard to pinpoint the specific reason/reasons for this increase, there are various factors contributing to the uptick in fraud activity.

Checks continue to be used extensively at organizations. Due to the hesitancy, and in some cases inability, to eliminate the use of checks for business transactions, the percentage of check fraud reported in the past few years has been consistent; about 60% of organizations experienced check fraud. Respondents admit that checks' susceptibility to fraud is a strong reason to eliminate the use of checks. Treasury leaders might want to begin the process of eliminating check use – even if gradually – by using alternate and safer methods to make payments which will help safeguard against fraud.

In 2023, the most common source of payments fraud was an external source or individual (e.g., forged check, stolen card, corporate synthetic identity fraud, etc.). Two-thirds of financial professionals report that payments fraud at their companies was the result of actions by an individual outside the organization. Business Email Compromise (BEC) continues to be a common source of payments fraud activity, although to a lesser degree than in past years. The emphasis that organizations have placed on detecting fraudulent email is paying off to some extent. Payments fraud due to interference with the U.S. mail is on the uptick; this can be a significant issue with organizations continuing to use checks extensively and using regular mail devoid of any tracking.

When looking to report payments fraud, organizations are most likely to seek assistance from their banking partners to receive guidance on minimizing the impact from such fraud. Even though many of these organizations are satisfied with the support received from their banking partners, there are some that are less satisfied. The onus of selecting a banking partner that is able to work with the organization in resolving issues arising from fraud is on treasury leaders.

Treasury practitioners at organizations are keenly aware that payments fraud activity is extensive, especially as criminals are relentless in targeting various payment types as well as using different methods to commit fraud. However, practitioners are not always able to predict what tactics fraud perpetrators might resort to next. Using technology to safeguard payments might be sound advice, but fraudsters are also using advanced technology to hack into organizations' payment systems. Although a mere one percent of survey respondents reports their organizations were targets of deepfake attempts (e.g., voice and/or video swapping, "deep voice" technology, vishing), this could very well change as AI becomes increasingly accessible.

Unfortunately, implementing stronger controls to protect against payments fraud is not a sufficient deterrent to those determined to commit fraud. Treasury and IT professionals at organizations need to be always on alert to ensure their organizations have adequate controls in place so that fraud attempts are unsuccessful. While financial losses from successful payments fraud attacks are not debilitating, the resources – both financial as well as personnel – necessary to detect, clean up and resolve issues arising from fraud occurrences are likely to be burdensome.

DEMOGRAPHICS

ABOUT SURVEY RESPONDENTS

In January 2024, 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 521 responses were received from practitioners, which form the basis of the report.

AFP thanks Truist for underwriting the *2024 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.

.

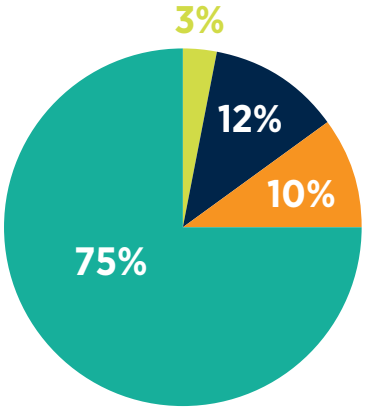
Type of Organization's Payment Transactions
(Percentage Distribution of Organizations)

	PRIMARILY CONSUMERS	SPLIT BETWEEN CONSUMERS AND BUSINESSES	PRIMARILY BUSINESSES
When making payments	6%	24%	70%
When receiving payments	18%	29%	53%

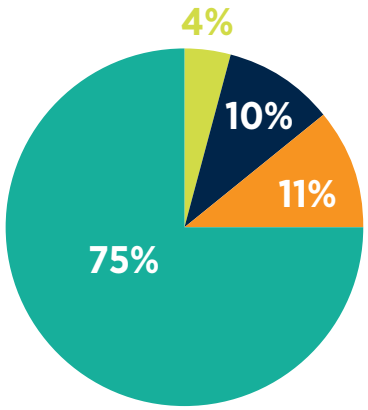
Number of Payment Accounts Maintained
(Percentage Distribution of Organizations)

	2023	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
Fewer than 5	24%	28%	22%	40%	--
5-9	17%	18%	17%	30%	--
10-25	18%	19%	17%	30%	--
26-50	8%	9%	7%	--	--
51-100	9%	10%	9%	--	--
More than 100	24%	16%	28%	--	100%

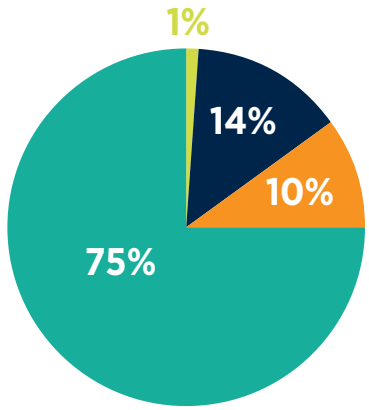
Methods to Maintain Payments Accounts
(Percentage Distribution of Organizations)



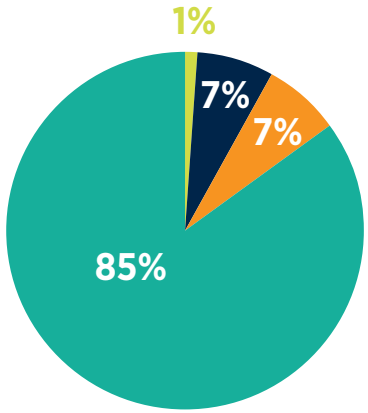
2023



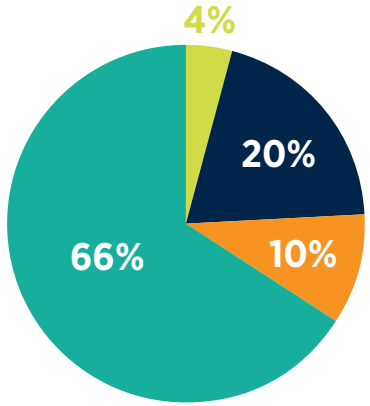
Annual Revenue Less Than $1 Billion



Annual Revenue At Least $1 Billion



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

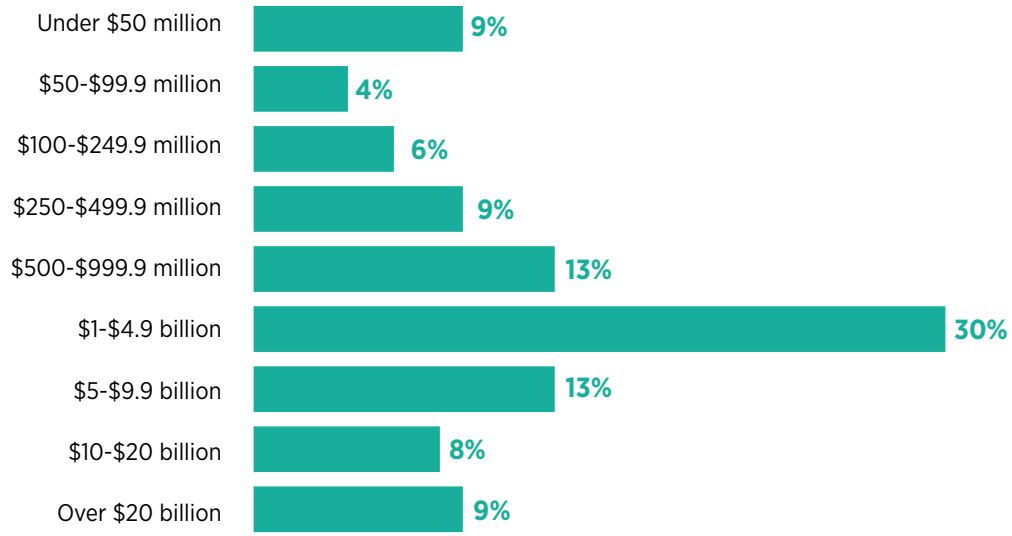


Annual Revenue At Least $1 Billion and More Than 100 Payment Accounts

- Centralized
- Decentralized
- Regionalized
- Other

Annual Revenue (USD)

(Percentage Distribution of Organizations)



Organization's Ownership Type

(Percentage Distribution of Organizations)

	2023	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
Publicly owned	39%	22%	51%	41%	65%
Privately held	44%	56%	35%	41%	24%
Non-profit (not-for-profit)	11%	16%	8%	11%	4%
Government (or government owned entity)	6%	6%	6%	7%	7%

Industry Classification

(Percentage Distribution of Organizations)

	2023
Agricultural, Forestry, Fishing & Hunting	2%
Administrative Support/Business services/Consulting	3%
Banking/Financial services	8%
Construction	4%
E-Commerce	--
Education (K-12, public or private institution)	1%
University or other Higher Education	3%
Energy	5%
Government	4%
Health Care and Social Assistance	8%
Hospitality/Travel/Food Services	4%
Insurance	7%
Manufacturing	15%
Mining	--
Non-profit	4%
Petroleum	2%
Professional/Scientific/Technical Services	3%
Real estate/Rental/Leasing	5%
Retail Trade	6%
Wholesale Distribution	2%
Software/Technology	5%
Telecommunications/Media	2%
Transportation and Warehousing	3%
Utilities	3%

2024 AFP® Payments Fraud and Control Report

All inquiries should be addressed to:

Association for Financial Professionals, Inc.

12345 Parklawn Dr Ste 200

PMB 1001

Rockville, MD 20852

Phone: 301.907.2862

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. Click here to view them on online.

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.

Association for Financial Professionals, Inc.

12345 Parklawn Dr Ste 200

PMB 1001

Rockville, MD 20852

T: +1 301.907.2862 | www.AFPonline.org

TRUIST

Fraud will affect 3 in 4 businesses.

We're here to help you prevent it.

Fraud is ever-evolving. As your trusted payments partner, Truist Wholesale Payments has the know-how and resources your business needs to stay ahead of fraudsters and strengthen your controls.

Talk to us about custom fraud solutions to protect your organization.

Learn more: Truist.com/commercial

Contact us: Wholesale_Payments@truist.com