Association for FINANCIAL PROFESSIONALS

2025 AFP®

PAYMENTS FRAUD AND CONTROL SURVEY REPORT

Key Highlights

Underwritten by TRUIST

2025 AFP®

PAYMENTS FRAUD AND CONTROL SURVEY REPORT

Key Highlights

April 2025

This summary report includes highlights from the comprehensive *2025 AFP® Payments Fraud and Control Survey Report*. The comprehensive report comprising all findings and detailed analysis is exclusively available to AFP members.

Learn more about AFP Membership

Underwritten by TRUIST

TRUIST

Navigating the Evolving Landscape of Payments Fraud: Insights from the 2025 AFP® Survey

As your trusted payments partner, Truist is proud once again to share the results of the *2025 AFP® Payments Fraud and Control Survey*. Our continued sponsorship reflects our commitment to empowering businesses with payment solutions that prioritize simplicity, speed, and, above all, safety.

The evolving landscape of payments fraud requires proactive security measures. This year's survey highlights the persistent challenges organizations face in safeguarding their financial transactions. While progress has been made, new threats and vulnerabilities have emerged, underscoring the need for robust fraud controls and proactive strategies.

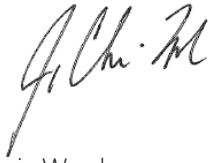
Here are some key findings from the 2025 survey:

- Fraud attempts remain stubbornly high, with 79% of organizations experiencing them, highlighting the urgent need for heightened awareness.
- Business email compromise (BEC) remains the top fraud vector, with 63% of organizations reporting it, impacting businesses with potentially catastrophic losses.
- Check fraud persists as a major vulnerability, cited by 63% of respondents, especially for businesses slow to adopt digital payments.
- Wire transfers are now the most targeted by BEC scams, affecting 63% of respondents, a critical risk for high-value transactions.
- Sophisticated BEC tactics like vendor impersonation are rising, despite a slight decline in "classic" BEC scams.

Truist remains dedicated to partnering with businesses to navigate these complexities. Our payments professionals are committed to providing the insights and solutions needed to secure your transactions and protect your assets. We believe this report will serve as a valuable resource in your ongoing efforts to mitigate risk and ensure the integrity of your payment processes.

We are here to guide you through these challenges, as your trusted payments partner, now and into the future.

Regards,



Chris Ward
Head of Enterprise Payments

TOPICS COVERED IN THE COMPREHENSIVE 2025 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
- ORIGINATIONS OF FRAUD
- ASSISTANCE SOUGHT WHEN REPORTING PAYMENTS FRAUD

BUSINESS EMAIL COMPROMISE

- ABOUT BUSINESS EMAIL COMPROMISE (BEC)
- FRAUDSTERS USING EMAIL ARE RELENTLESS
- FINANCIAL IMPACT OF BUSINESS EMAIL COMPROMISE
- PAYMENT METHODS IMPACTED BY BEC
- DEPARTMENTS VULNERABLE TO EMAIL SCAMS
- BUSINESS EMAIL COMPROMISE PREVENTION — POLICIES AND PROCEDURES
- BUSINESS EMAIL COMPROMISE PREVENTION — SECURITY AND COMPLIANCE MEASURES
- PREVENTING BUSINESS EMAIL COMPROMISE

CHECKS AND ACH

- CHECKS CONTINUE TO BE A POPULAR METHOD OF PAYMENT AT ORGANIZATIONS
- CHECK FRAUD CONTROLS
- ACH DEBIT FRAUD AND CONTROLS

MEASURES TO IMPROVE CONTROLS

INTRODUCTION

Payments fraud activity continues to be elevated. Seventy-nine percent of respondents indicate that their organizations had been targets of either actual or attempted fraud activity in 2024, similar to the 80% reported in 2023. Although organizations are being extremely vigilant in order to avoid falling prey to scammers, it appears that many continue to experience fraud. In today's environment, organizations are increasingly vulnerable, as there are various methods to move cash instantly (e.g., Real-Time Payments [RTP®], FedNow®, Zelle®, etc.). But there is considerable risk in using these methods; once a transaction occurs, it is irrevocable and nearly impossible to retrieve the funds. Being susceptible to greater fraud with these methods could outweigh the convenience of transacting payments immediately.

Payments fraud via email continues to be extensive, although companies are training their employees to be watchful about emails they receive by providing them with continual education about the scam tactics being used. Fraudsters are using AI and are able to target messages very effectively, hindering the ability of employees to differentiate a fraudulent email from an authentic one. AI is also able to bolster fraudsters' attempts in using deep-fake technology successfully. While recorded instances of deep-fake attempts were low in 2024 and are currently not as prevalent as other methods, more organizations could experience these sophisticated fraud attacks in the near future.

Although AI can be a tool for fraudsters to successfully attack their targets, it can also be a tool for organizations to use in order to better safeguard themselves against payments fraud. AI can help predict outcomes with greater accuracy and analyze data faster. The adoption of AI at organizations is currently not extensive, but business leaders might need to pivot and be prepared to invest in AI and other technologies that can help detect fraud and deter attacks.

Payments fraud via check is still extensive; over 60% of survey respondents report that there was check fraud activity at their organizations in 2024. Despite being an easy target for fraud, checks continue to be used by a large majority of organizations, and 75% of organizations do not plan on eliminating the use of checks in the next two years. Mail interference also remains a problem, with 23% of organizations experiencing check fraud due to mailbox thefts.

Over the years, organizations have adopted tried-and-tested safeguards to minimize payments fraud, some of which have proven more effective than others. This report identifies the controls organizations have implemented to mitigate payments fraud via email, checks and ACH, as well as the effectiveness of each type of control.

The Association for Financial Professionals® (AFP) has conducted its *Payments Fraud and Control Survey* every year since 2005. Continuing this research, AFP® conducted the 21st *Annual Payments Fraud and Control Survey* in January 2025. The survey delves into the type and the extent of fraud attacks on business-to-business (B2B) transactions, the payment methods impacted, the increasing role of business email in payments fraud, and the preventative measures organizations are adopting to protect themselves from fraud attempts. This year's survey generated 521 responses from corporate practitioners from organizations of varying sizes and representing a broad range of industries. Results presented in this report reflect data for 2024. Survey respondent demographics are available at the end of this report.

AFP® thanks Truist® for its underwriting support of the *2025 AFP® Payments Fraud and Control Survey*. Both questionnaire design and the final report, along with its content and conclusions, are the sole responsibilities of AFP's Research Department.

KEY FINDINGS

Fraud is down very slightly — but remains elevated.

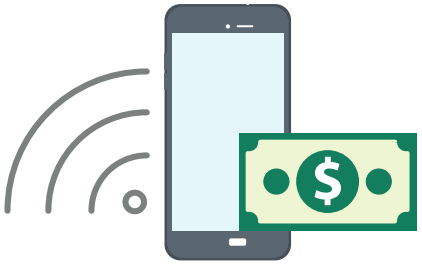
A full 79% of respondents say that their organizations experienced actual or attempted payments fraud in 2024, down slightly from 80% in 2023. The one-percentage-point drop is not very encouraging; 65% of corporate practitioners reported payments fraud at their organizations in 2022. Clearly, fraudsters have not been deterred by any of the anti-fraud protections that organizations have put in place.

Business email compromise (BEC) continues to be a threat.

BEC once again was the number one avenue for attempted and actual payments fraud in 2024, cited by 63% of respondents. Incidence of vendor imposter fraud was also high, at 45%, a sharp increase from 34% in the previous survey. It's important to note that vendor imposter fraud is another form of BEC, as is invoice fraud which increased to 24% in 2024 from 14% in 2023. Spoof emails are still the most prevalent type of BEC, cited by 79% of respondents (up from 77% in 2023).

Check fraud remains constant.

Checks continue to be the payment method most often subjected to payments fraud, with 63% of respondents experiencing attempted or actual fraud via checks in 2024. While that percentage is down slightly from 65% in the previous survey, it is clear that checks remain easy targets for criminals. Nevertheless, more than 75% of organizations currently have no plans to reduce check usage in the next two years.



Wire transfers reclaim their BEC crown.

Wire transfers reclaimed their rank as the payment method most frequently targeted by BEC scammers in 2024, reported by 63% of respondents, up from 39% in the previous survey. Nevertheless, ACH credits — which were the prime targets for BEC in 2023 — were the source of more BEC scam activity in 2024 than in the previous year, rising to 50% from 47%. ACH debits and checks tied for third place at 26% (up from 20% and 18%, respectively).

Classic BEC scams may be falling off.

One significant change seen in this year's survey is the decline in "classic" BEC scams. These are cases in which a fraudster impersonates a senior executive and requests a transfer of funds. In 2023, this method of payments fraud was on par with vendor impersonation, cited by 57% of organizations. In 2024, however, the incidence declined to 49%. Vendor impersonation experienced a slight increase — cited by 60% of respondents — while third-party impersonation remained the most frequent type of BEC scam at 63%. This change in tactics is likely to due to organizations' growing awareness of such "classic" BEC attempts.

Recovering losses has mixed success.

Twenty-two percent of organizations were able to recover 75% or more of the funds lost due to payments fraud in 2024. That is a sharp decrease from results reported for 2023, during which 41% of companies recouped the same amount. However, it is encouraging that the percentage of organizations that were unable to recover anything at all in 2024 was 20%, down from 30% in 2023, and 58% were able to recoup up to 75% of their funds in 2024 (up from 29% in 2023).

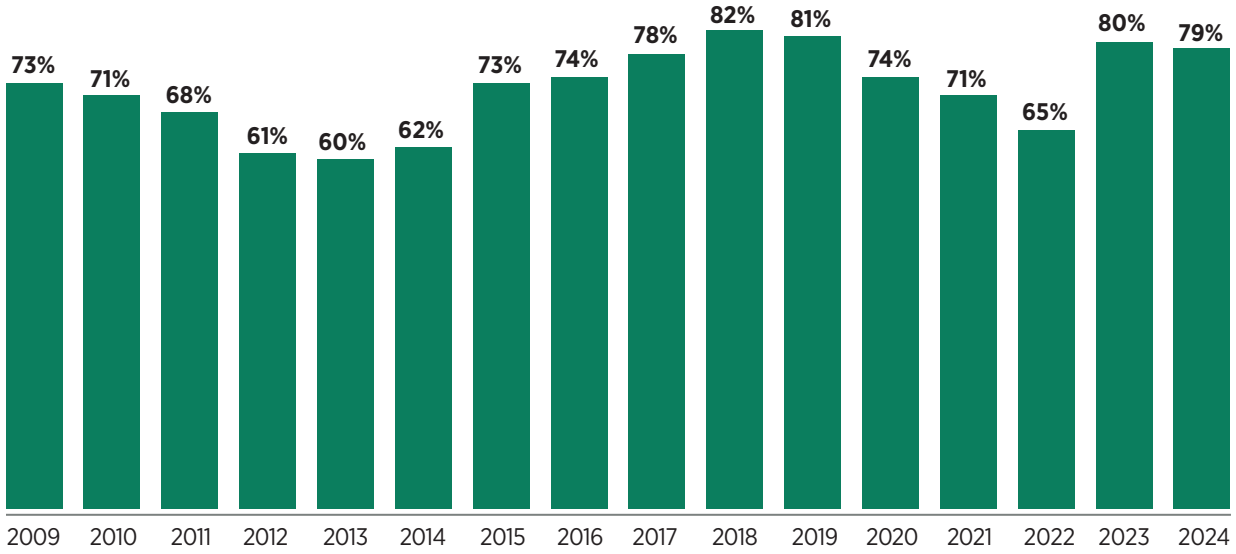
PAYMENTS FRAUD TRENDS

Payments Fraud Attacks on Organizations Continue to Be Elevated

Seventy-nine percent of organizations report they experienced actual or attempted payments fraud activity in 2024 — a slight decrease from the 80% reported for 2023, and in the ballpark of recorded payments fraud since 2015. Note the exception of 2022, during which observed payments fraud activity was 65%.

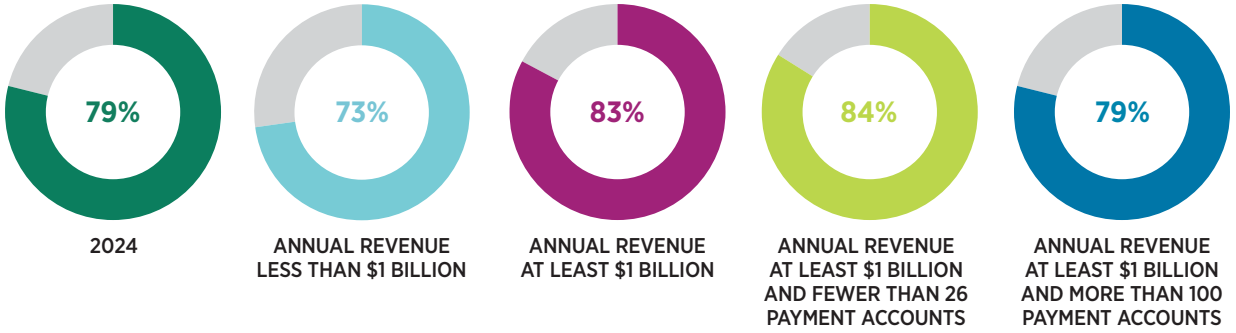
Larger organizations (those with annual revenue of at least $1 billion) were more susceptible to payments fraud attacks than were smaller ones (those with annual revenue less than $1 billion): 83% compared to 73%. A greater share of survey respondents from larger organizations and those with smaller 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 2024 compared with the share of respondents from other organizations.

Prevalence of Attempted/Actual Payments Fraud, 2009-2024
(Percent of Organizations)



> "A perpetrator used valid check information to create a counterfeit check copy with a different payee name. We have begun implementing payee positive pay so that our pay file includes payee name going forward."

Prevalence of Attempted/Actual Payments Fraud in 2024
(Percent of Organizations)



PAYMENT METHODS IMPACTED BY FRAUD

The share of organizations that were victims of fraud attacks via corporate/commercial credit cards in 2024 is very similar to the share reporting such fraud activity in 2023 — i.e., 21% in 2024 compared to 20% in 2023.

Respondents from organizations with annual revenue of at least $1 billion are more likely than those with annual revenue less than $1 billion to report that checks were subject to attempted or actual payments fraud in 2024 (70% compared to 55%).

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

	2024	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	2023
Checks	63%	55%	70%	73%	66%	65%
ACH debits	38%	32%	42%	42%	43%	33%
Wire transfers	30%	25%	34%	23%	46%	24%
Corporate/commercial credit cards (e.g., purchasing, T&E, fleet)	21%	25%	18%	16%	21%	20%
ACH credits	20%	17%	22%	20%	22%	19%
Cash	5%	4%	6%	4%	9%	4%
Virtual cards	5%	6%	4%	5%	5%	3%
Mobile Wallets (Venmo, PayPal®, etc.)	3%	3%	4%	2%	7%	1%
Faster payments (RTP®, FedNow®, etc.)	2%	1%	2%	--	6%	1%
Cryptocurrency (Bitcoin, Ethereum, etc.)	1%	1%	1%	1%	2%	--

"Credit card fraud is the most prevalent fraud we have encountered. We are closing and replacing cards monthly. Our theory is that vendors have systems that are compromised, and our card numbers get stolen."

"Attempted wire fraud was averted when a member of Treasury was asked to verify payment from the originating bank. Since all wires and ACHs are supposed to be initiated by Treasury, this was immediately recognized as fraud and reported to the bank and local authorities."

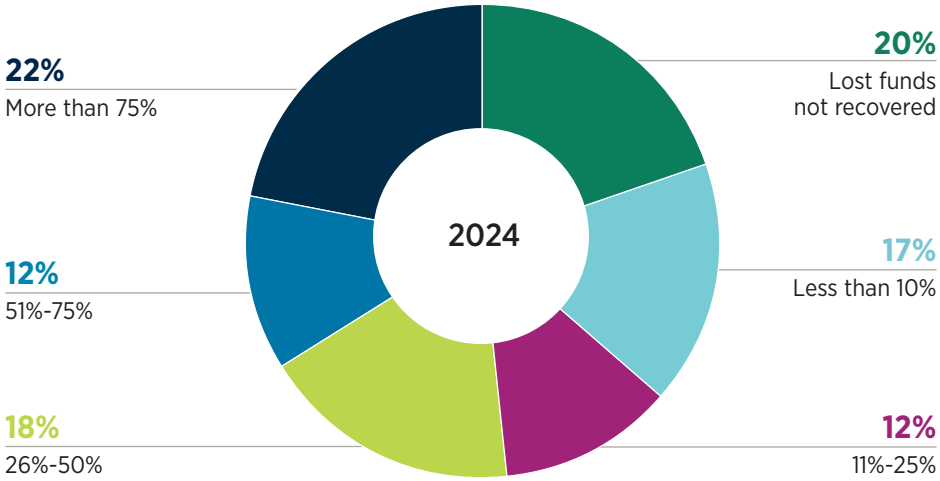
RECOVERING LOST FUNDS

Twenty Percent of Organizations Did Not Recoup Funds Stolen Due to Fraud

Almost six out of 10 organizations recovered up to 75% of any funds lost due to payments fraud in 2024; 22% were successful in recouping more than 75% of the funds lost. Twenty percent of respondents report that after successful payments fraud attempts, they were unable to recover the funds lost due to the fraud.

Smaller organizations with annual revenue less than $1 billion were more successful than larger ones (with annual revenue of at least $1 billion) in recovering funds lost due to payments fraud (16% versus 22%).

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



"An employee did not check the signature on the back of a check that was flagged by the bank, and decided it good to pay. Weeks later it was discovered the check was intercepted by a fraudster as was evident by the the signature on the back. In this instance the bank was not able to recover the funds and the vendor had to be repaid. A police report was not filed as it was a user error by someone internally on the team and the vendor was a related party."

"A spoofed email was received and our AP personnel did not follow internal controls when changing payee bank account data. The funds were wired to fraudsters. With the help of our bank we were able to get the funds returned from China several weeks later."

ORIGINATIONS OF FRAUD

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

	2024	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
Business Email Compromise (BEC)	62%	59%	63%	59%	66%
Individual external to the organization using tactics other than email (e.g., forged check, stolen card, fraudster, corporate synthetic identity fraud)	49%	47%	51%	51%	50%
Vendor imposter	45%	40%	48%	50%	49%
Invoice fraud	24%	22%	26%	23%	32%
U.S. Postal Service office interference	23%	20%	25%	30%	19%
Imposter to a client posing as representative from your company	14%	9%	18%	18%	20%
Third-party or outsourcer (e.g., vendor, professional services provider, business trading partner)	12%	12%	11%	7%	19%
Account takeover (e.g., hacking a system, adding malicious code — spyware or malware from social network)	12%	9%	14%	15%	16%
Compromised mobile device due to spoof/spam text message or call	8%	8%	8%	6%	15%
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)	7%	5%	8%	11%	5%
Deep-fake attempt (e.g., voice and/or video swapping, “deep voice” technology, vishing)	5%	3%	5%	3%	11%
Ransomware	4%	2%	5%	4%	9%
Internal party (e.g., malicious insider)	3%	2%	4%	2%	8%

ABOUT BUSINESS EMAIL COMPROMISE (BEC)

Increased Vigilance is Making a Dent in Successful Email Scams

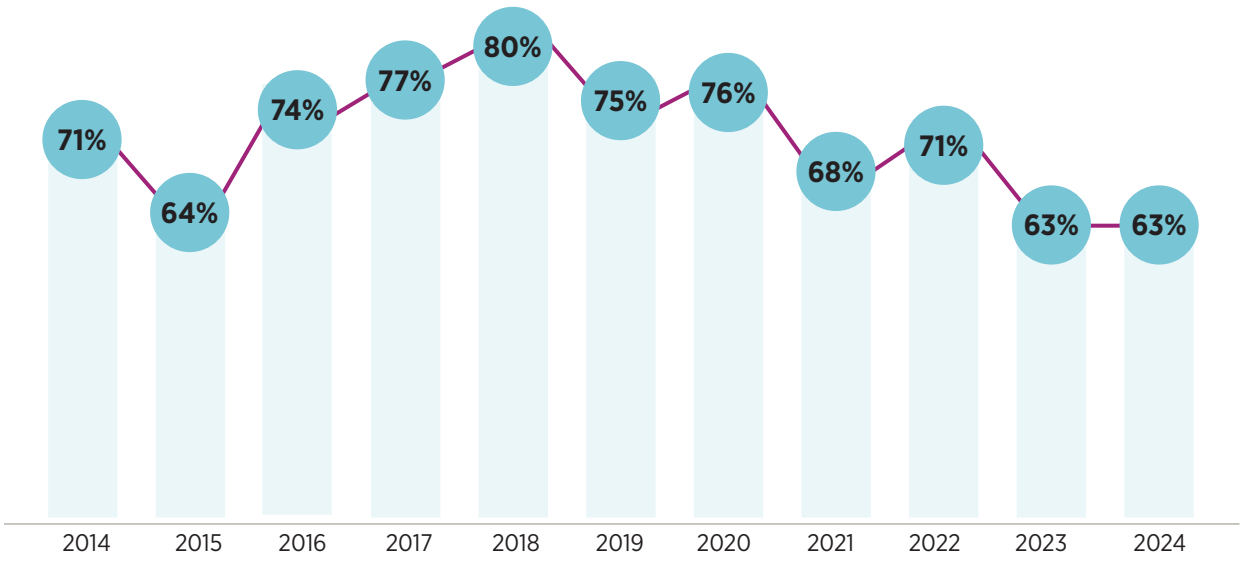
Business professionals predominately use email for communication within their organizations and with clients, vendors, et al. As of April 2024, the U.S. was the country with the largest number of emails sent daily, totaling almost 10 billion.[12] This extensive use of email makes it very susceptible to fraud.

BEC remains a significant threat. Prevention, detection and response protocols are imperative in mitigating the impact of BEC, and organizations are making efforts to minimize fraud via email through various safeguards (addressed later in this report, see page 43). Organizations have enhanced email filtering measures that can intercept fraudulent emails prior to delivery; they are also educating and training employees on how to detect and avoid fraudulent emails. As a result, instances of successful fraud attacks via email have been curbed to some extent. In 2023, there was a decline in the percentage of organizations that experienced attempted or actual BEC. Sixty-three percent of organizations reported experiencing BEC in 2023, an 8-percentage-point decrease from 2022. In 2024, the percentage of organizations experiencing BEC was unchanged from 2023. While it is encouraging that there was no uptick in the figure, payments fraud committed via BEC continues to be reported by over 60% of organizations.

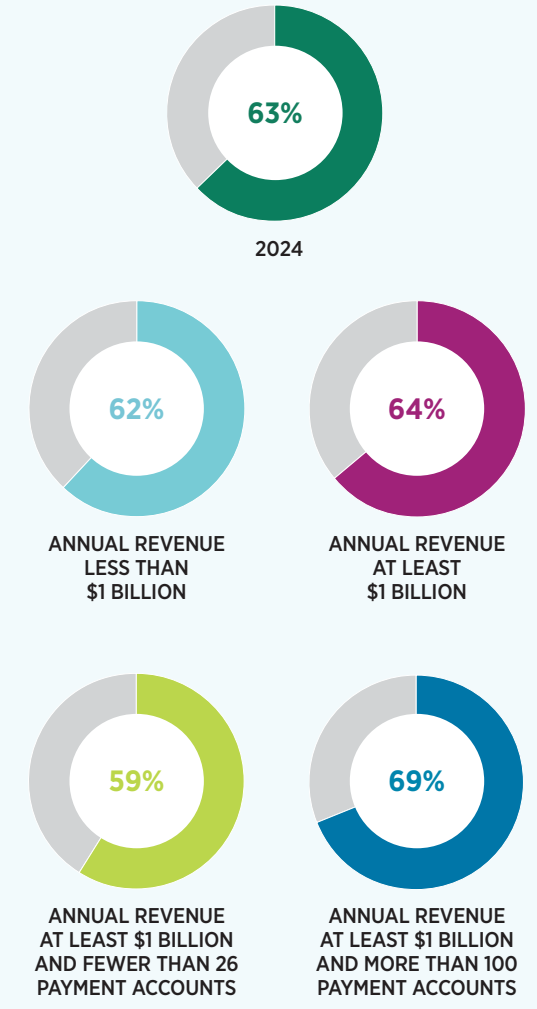
A larger share of organizations with annual revenue of at least $1 billion and more than 100 payment accounts report BEC-based payments fraud than do companies with at least $1 billion revenue and fewer than 26 payment accounts.

[12] https://www.statista.com/statistics/1270459/daily-emails-sent-by-country/

Organizations that Experienced Business Email Compromise (BEC) (2014-2024)
(Percent of Organizations Experiencing Payments Fraud)



Organizations that Experienced Business Email Compromise (BEC) in 2024
(Percent of Organizations)



PAYMENT METHODS IMPACTED BY BEC

Wire Transfers Most Vulnerable to BEC Fraud

Most payment methods continue to be vulnerable to BEC. Payments made via wire transfers (63%), ACH credits (50%), ACH debits (26%) and checks (26%) were the ones most often targeted in 2024. Sixty-three percent of all respondents report wire transfers as the payment method most impacted by BEC. For those organizations with annual revenue less than $1 billion, the share decreases to 55%, while for organizations with annual revenue of at least $1 billion and with more than 100 payment accounts, the percentage increases to 76%. For ACH credits, the incidence is reversed. Forty 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 68% of organizations with annual revenue less than $1 billion report the same.

For a second consecutive year, real-time payments are included as one of the payment methods impacted by BEC. Overall, 4% of respondents indicate real-time payments were targeted via BEC. Instances of BEC fraud via real-time payments occurred primarily in those organizations with annual revenue of at least $1 billion and more than 100 payment accounts.

Larger companies are more often targets for payments 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 may operate in a decentralized manner and so 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 should be vigilant in detecting suspicious activity. Banks are the top sources 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.

Payment Methods Utilized in Business Email Compromise
(Percent of Organizations Experiencing Payments Fraud)

	2024	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
Wire transfers	63%	55%	64%	53%	76%
ACH credits	50%	68%	43%	53%	40%
Checks	26%	23%	26%	29%	16%
ACH debits	26%	23%	26%	18%	28%
Corporate/commercial credit cards (e.g., purchasing, T&E, fleet)	11%	14%	11%	12%	16%
Third-party payouts (e.g., Venmo, PayPal®, Zelle®, etc.)	9%	9%	9%	18%	8%
Cash	8%	14%	6%	12%	4%
Gift cards	6%	14%	2%	--	4%
Mobile wallets	4%	9%	2%	--	4%
Cryptocurrency (Bitcoin, Ethereum, etc.)	3%	--	4%	6%	4%
Real-time Payments (RTP®, FedNow®)	3%	--	4%	--	4%
Virtual cards	--	--	--	--	--

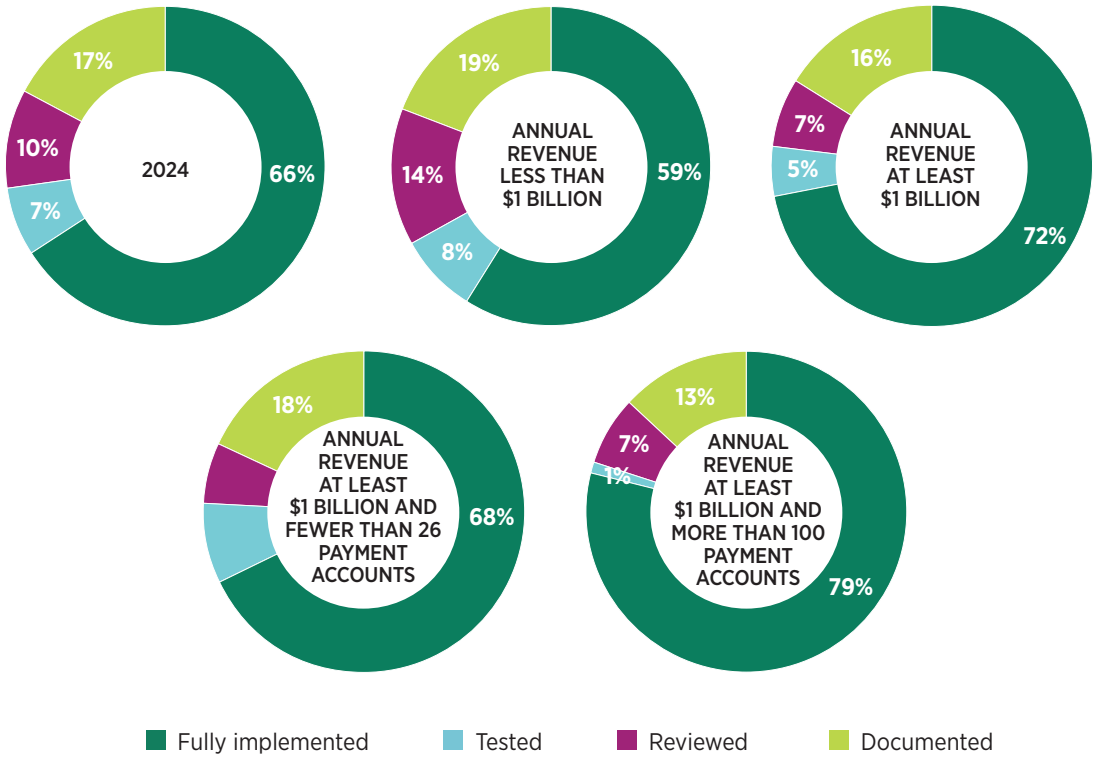
PREVENTING BUSINESS EMAIL COMPROMISE

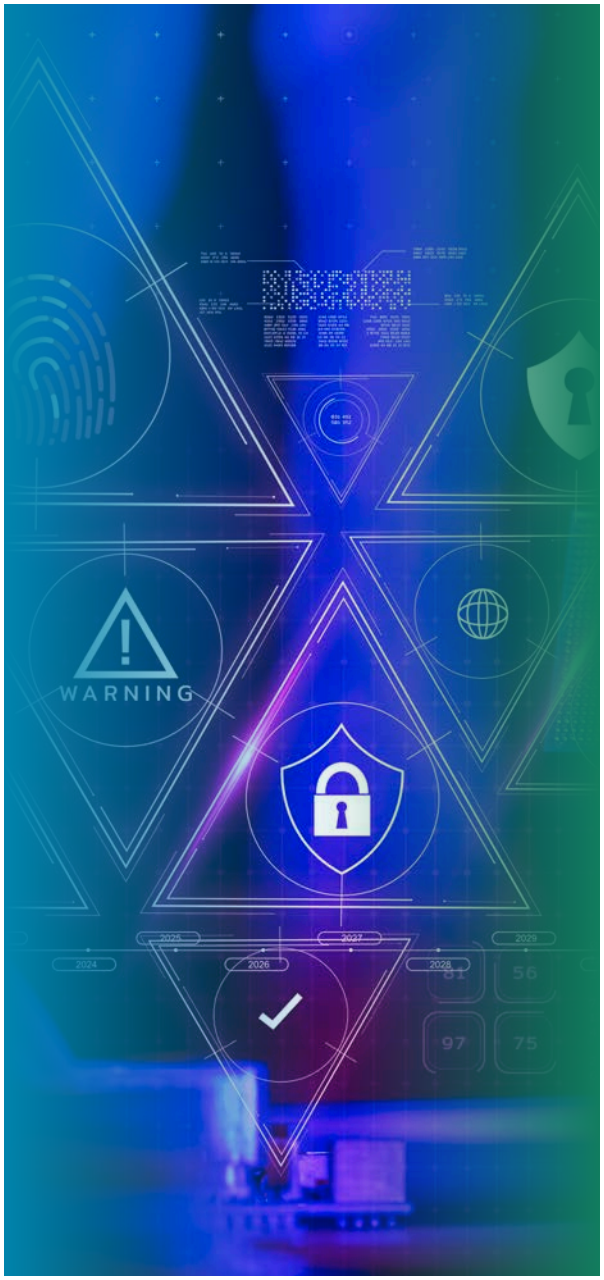
Rollout of Policies and Procedures Designed to Prevent Business Email Compromise

As BEC attacks become more effective and sophisticated, organizations need to be intentional about creating policies and procedures designed not only to limit their exposure to such attacks, but also to minimize the impact of the fraud. As noted earlier, a variety of policies and processes are effective in minimizing BEC attacks at organizations, but that minimization can only happen if companies employ a targeted approach to the systemic application.

Of those organizations with BEC preventions and policies, 66% have fully implemented them, 17% have completed the necessary documentation, 10% have completed the review process and 7% are testing their BEC policies and procedures. Since two-thirds of organizations have implemented BEC policies and procedures, it is evident that organizations are taking BEC seriously, and a majority is preparing to protect themselves against BEC. Remaining organizations are at various stages in the process of completing and implementing these policies.

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





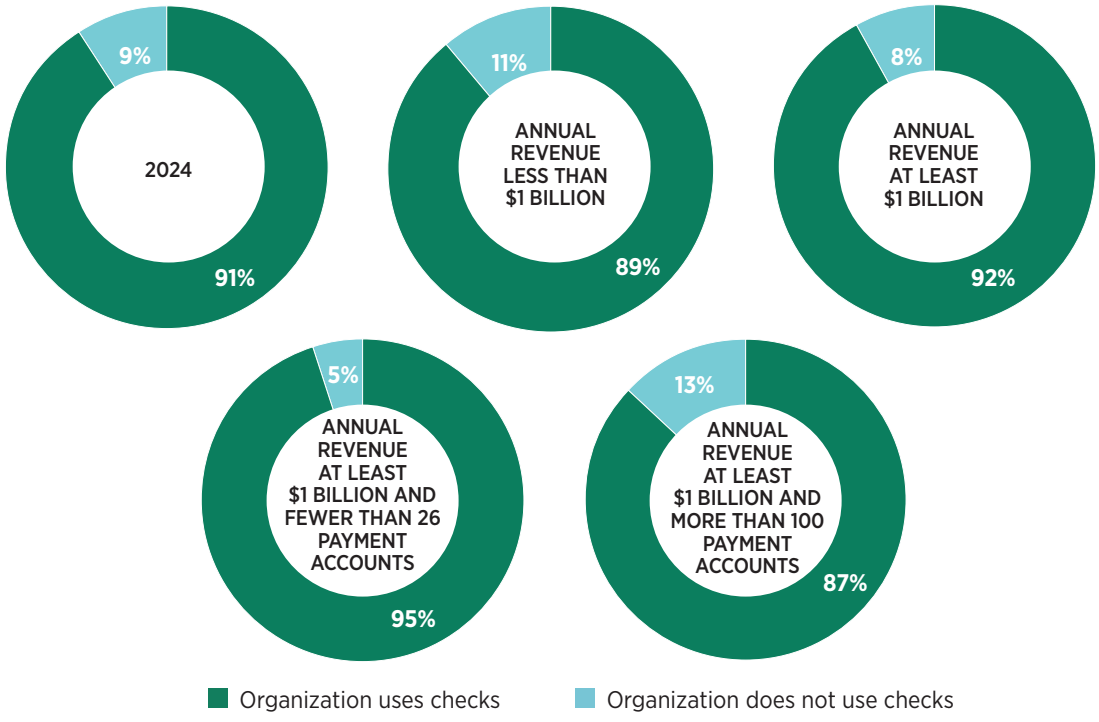
CHECKS CONTINUE TO BE A POPULAR METHOD OF PAYMENT AT ORGANIZATIONS

Check Usage

Checks continue to be a favored payment method at organizations — and they are used extensively. Ninety-one percent of respondents report that their organizations are currently using checks. This figure is up from 75% in 2023. While it is unclear why check usage increased somewhat dramatically in 2024, some organizations may have been misled into thinking that check payments are safer than digital payments. This view is clearly false after reviewing the data collected in the annual AFP Payments Fraud surveys (since 2015). But many businesses may be looking at things from a different point of view. Payment technology has been evolving rapidly — as are fraud techniques that target newer payment methods. Consequently, many business leaders who are unfamiliar with these new technologies may be inclined to fall back on what they know, perhaps being lulled into thinking that the least secure method of payment is the most secure.

Seventy percent of organizations make less than 25% of their payments via checks, while 30% of respondents report that checks are being used for over 25% of payments. Over 50% of organizations with annual revenue of at least $1 billion and more than 100 payment accounts make 10% or less of their payments via check, suggesting larger organizations with numerous payment accounts are not using checks as extensively as other payment methods.

Check Usage at Organizations
(Percentage Distribution of Organizations)



Annual Check Usage to Make Payments
(Percentage Distribution of Organizations that Use Checks)

	2024	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
10% or less	41%	43%	40%	35%	52%
11%-25%	29%	28%	30%	34%	20%
26%-50%	20%	19%	20%	19%	19%
Over 50%	10%	10%	10%	12%	9%

CONCLUSION

Actual and attempted payments fraud in 2024 continued to be very high, with 79% of organizations reporting such activity. Still, at two-thirds of organizations, the incidence of fraud in 2024 was unchanged from that in 2023. Organizations are grappling with containing payments fraud activity while attacks are becoming more sophisticated; fraudsters are able to circumvent the controls organizations have implemented to safeguard themselves.

Similar to results in 2023, checks and ACH debits were the payment methods most impacted by payments fraud activity in 2024 (63% and 38%, respectively). Since 2020, the percentage of organizations reporting payments fraud via checks has been similar, i.e., in the ballpark of 63%-66%. Checks continue to be a preferred payment method at organizations, and they are used extensively at a vast majority of organizations. The popularity of check usage explains the high incidence of check fraud being reported. Findings suggest that a majority of organizations is not deterred from using checks, even though they are aware of their susceptibility to fraud and acknowledge the administrative burdens involved with check payments. But eliminating the use of checks is problematic; the size of other companies with which organizations work and the requirement of check use by those partners is preventing them from eliminating check payments.

While a majority of organizations recouped up to 75% of any funds lost due to payments fraud in 2024, not all organizations had that same level of success. Twenty percent of respondents report that after a successful payments fraud attempt, their organizations were unable to recover the funds lost.

Of those organizations that were victims of payments fraud and incurred actual losses in 2024, 35% took less than one week to uncover the fraud; 21% detected the fraudulent activity within one to two weeks. Treasury is the department most likely to uncover both attempted and actual payments fraud activity, followed by accounts payable (AP). Treasury leaders need to ensure that they are best prepared to detect fraud; the longer it takes to discover an attempt/attack, the more challenging it will be to recover funds.

In 2024, the most common source of payments fraud was via business email compromise (BEC), with over 60% of respondents reporting such fraud at their companies was the result of a fraudulent email. Another frequent source of fraud was individuals outside the organization; methods include forged checks, stolen cards, identity fraud, etc. Additionally, organizations were often targeted by vendor impostors. Greater vigilance and implementation of processes to streamline vendor verification is necessary.

BEC continues to be a significant threat with 63% of respondents reporting their organizations had been targets of this type of fraud. However, organizations are making efforts to minimize fraud via email through various measures, and therefore instances of successful email attacks have been curbed to some extent. Organizations have enhanced email filtering measures that can intercept fraudulent emails prior to delivery. They have also been educating and training employees on how to detect and avoid fraudulent emails. Prevention, detection and response protocols are imperative to mitigate the impact of BEC. More than half of practitioners report that their AP department is most vulnerable to email fraud.

Treasury leaders will want to focus on reducing payments fraud activity by ensuring their employees are well trained in detecting fraud and specifically equipping departments prone to attacks with tools and technology to mitigate fraud. As we have observed, fraud techniques are getting more sophisticated and targeted with the help of AI and other technologies; staying ahead of fraudsters criminals is key. While organizations are not reporting significant incidences of payments fraud attempts via deep-fake software currently, in a few years the environment might be very different. The use of AI and other technologies for visual and audio impersonations might be a common occurrence.

DEMOGRAPHICS

ABOUT SURVEY RESPONDENTS

In January 2025, 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 were received from practitioners, which form the basis of the report.

AFP® thanks Truist® for underwriting the *2025 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.

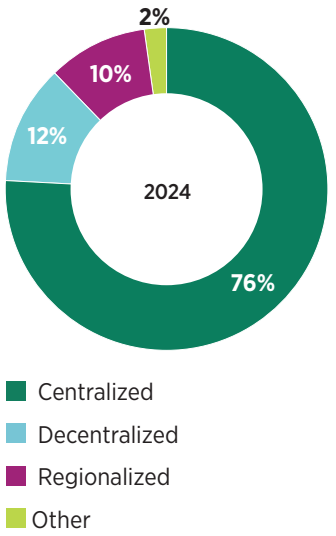
Type of Organization's Payment Transactions
(Percentage Distribution of Organizations)

	PRIMARILY CONSUMERS	SPLIT BETWEEN CONSUMERS AND BUSINESSES	PRIMARILY BUSINESSES
When making payments	5%	26%	69%
When receiving paymnets	18%	32%	50%

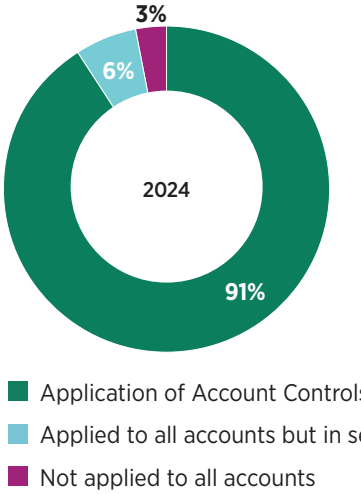
Number of Payment Accounts Maintained
(Percentage Distribution of Organizations)

	2024	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	23%	34%	16%	34%	--
5-9	14%	18%	12%	25%	--
10-25	19%	17%	19%	41%	--
26-50	8%	7%	9%	--	--
51-100	8%	7%	7%	--	--
More than 100	28%	17%	37%	--	100%

Methods to Maintain Payments Accounts

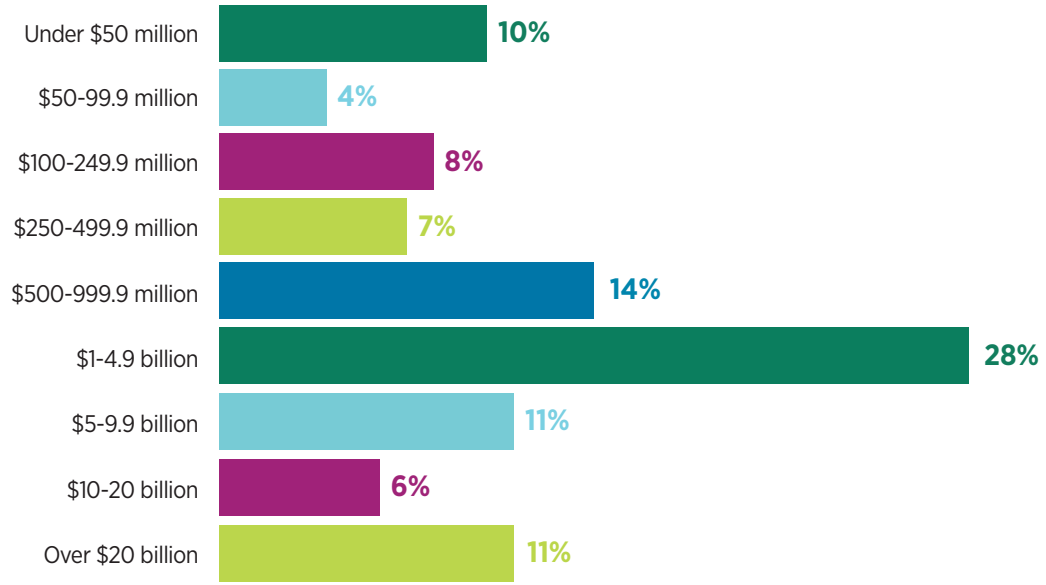


Application of Account Controls
(Percentage Distribution of Organizations)



ABOUT SURVEY RESPONDENTS CONTINUED

Annual Revenue (USD)
(Percentage Distribution of Organizations)



Industry Classifications
(Percentage Distribution of Organizations)

Agricultural, Forestry, Fishing & Hunting	2%
Administrative Support/Business services/ Consulting	2%
Banking/Financial services	14%
Construction	2%
E-Commerce	1%
Education (K-12, public or private institution)	2%
University or other Higher Education	5%
Energy	4%
Government	3%
Health Care and Social Assistance	7%
Hospitality/Travel/Food Services	3%
Insurance	7%
Manufacturing	14%
Mining	--
Non-profit	5%
Petroleum	1%
Professional/Scientific/Technical Services	3%
Real estate/Rental/Leasing	5%
Retail Trade	4%
Wholesale Distribution	2%
Software/Technology	4%
Telecommunications/Media	3%
Transportation and Warehousing	3%
Utilities	4%

Organization's Ownership Type
(Percentage Distribution of Organizations)

	2024	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	36%	21%	47%	42%	52%
Privately held	43%	55%	33%	34%	32%
Non-profit (not-for-profit)	13%	17%	10%	12%	8%
Government (or government owned entity)	8%	7%	10%	12%	8%

All inquiries should be addressed to:
Association for Financial Professionals
12345 Parklawn Dr., Ste 200, PMB 2001
Rockville, MD 20852
Phone: 301.907.2862
E-mail: AFP@AFPonline.org
Web: www.AFPonline.org

Association for
FINANCIAL PROFESSIONALS

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, and financial accounting and reporting. Click **HERE** to view study reports on a variety of topics, including AFP's annual Compensation and Benefits Survey Report.

About AFP®

As the certifying body in treasury and finance, the Association for Financial Professionals (AFP) established and administers the Certified Treasury Professional (CTP) and Certified Corporate Financial Planning and Analysis Professional (FPAC) credentials, setting the standard of excellence in the profession globally. AFP's mission is to drive the future of finance and treasury and develop the leaders of tomorrow through certification, training and the premier event for corporate treasury and finance.

12345 Parklawn Dr., Ste 200, PMB 2001
Rockville, MD 20852
T: +1 301.907.2862 | F: +1 301.907.2864

www.AFPonline.org

TRUIST

Fraudsters persist. Are you prepared?

We're here to help safeguard your business.

Protecting your business from fraud is always on our mind. As your trusted partner, Truist Wholesale Payments has the knowledge, people, and tools to keep your organization safe.

Talk to us about custom fraud solutions that offer simplicity, speed, and safety.

Learn more: Check fraud control | Truist

Reach us at Wholesale_Payments@truist.com.