Association for FINANCIAL PROFESSIONALS

2025 AFP®

PAYMENTS FRAUD AND CONTROL SURVEY REPORT

Comprehensive Report

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.

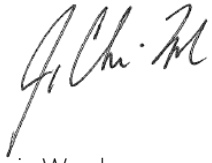
Here are some key findings from the 2025 survey:

- 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

CONTENTS

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.

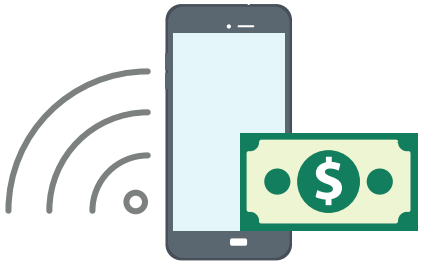
A full 79% of respondents say that their organizations experienced actual or attempted payments fraud in 2024, down slightly from 80% in 2023. The one-percentage-point drop is not very encouraging; 65% of corporate practitioners reported payments fraud at their organizations in 2022. Clearly, fraudsters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

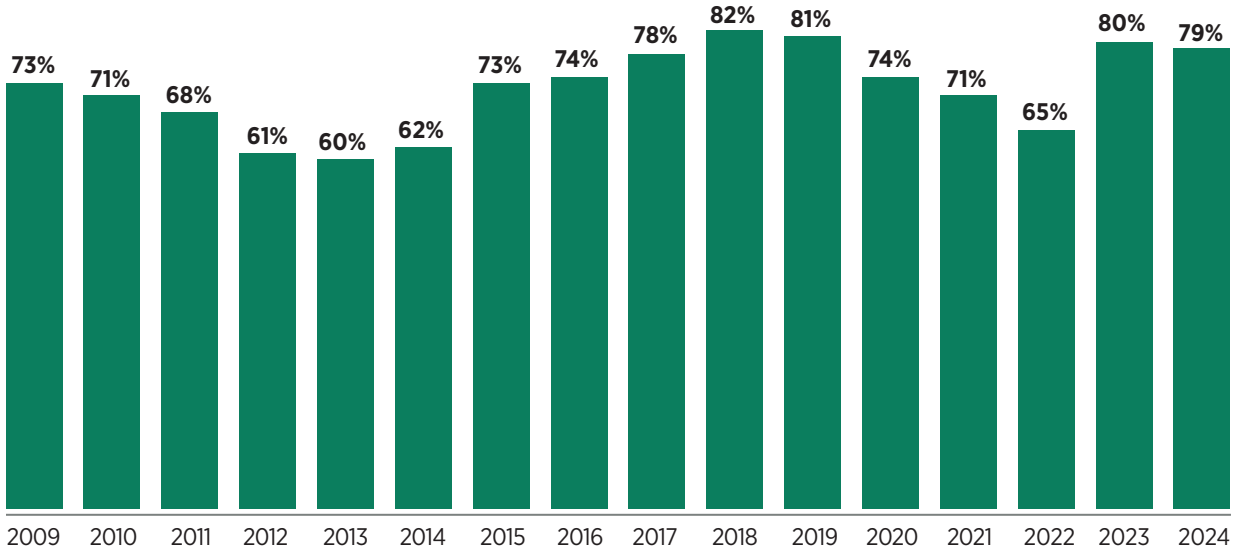
PAYMENTS FRAUD TRENDS

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%.

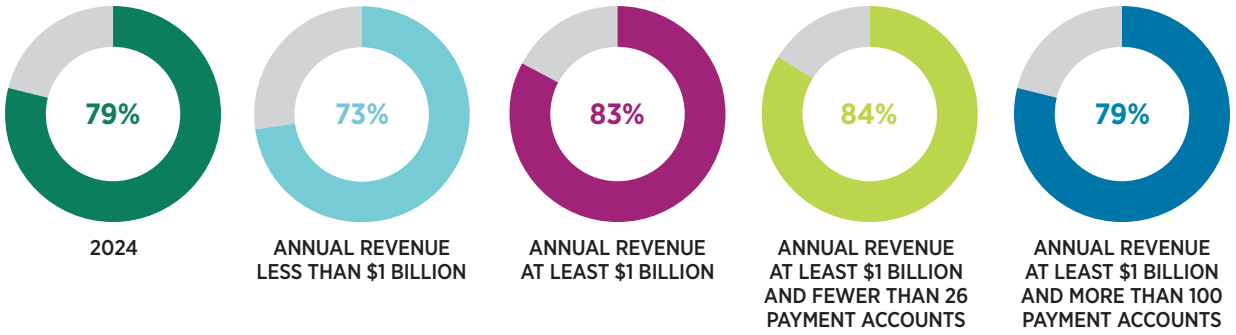
Larger organizations (those with annual revenue of at least $1 billion) were more susceptible to payments fraud attacks than were smaller ones (those with annual revenue less than $1 billion): 83% compared to 73%. A greater share of survey respondents from larger organizations and those with smaller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

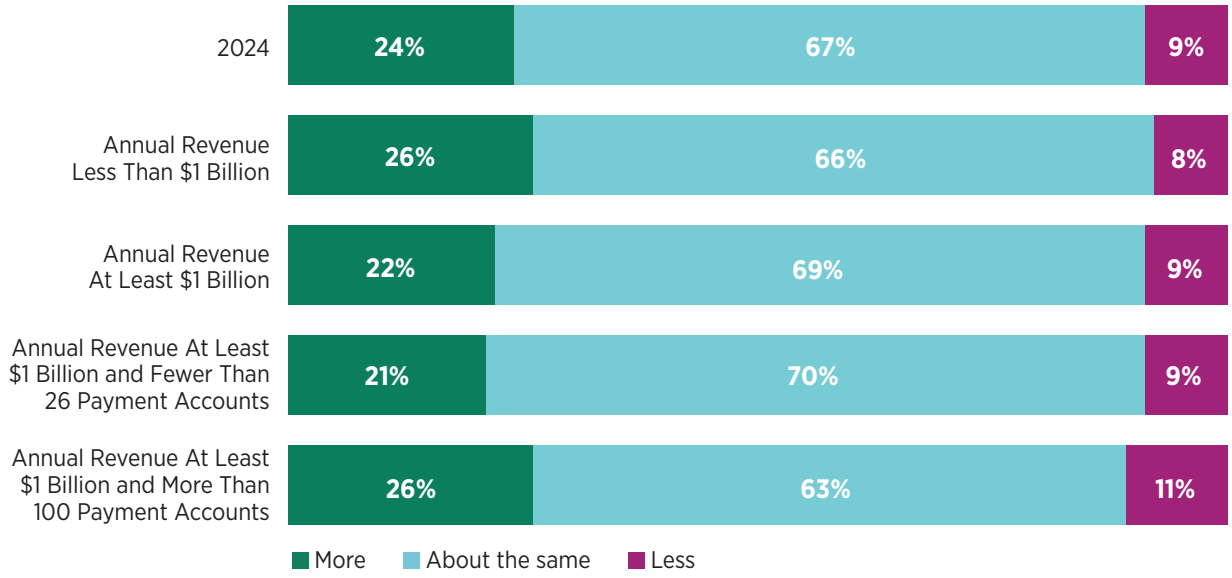


Payments Fraud Unchanged at Two-Thirds of Companies

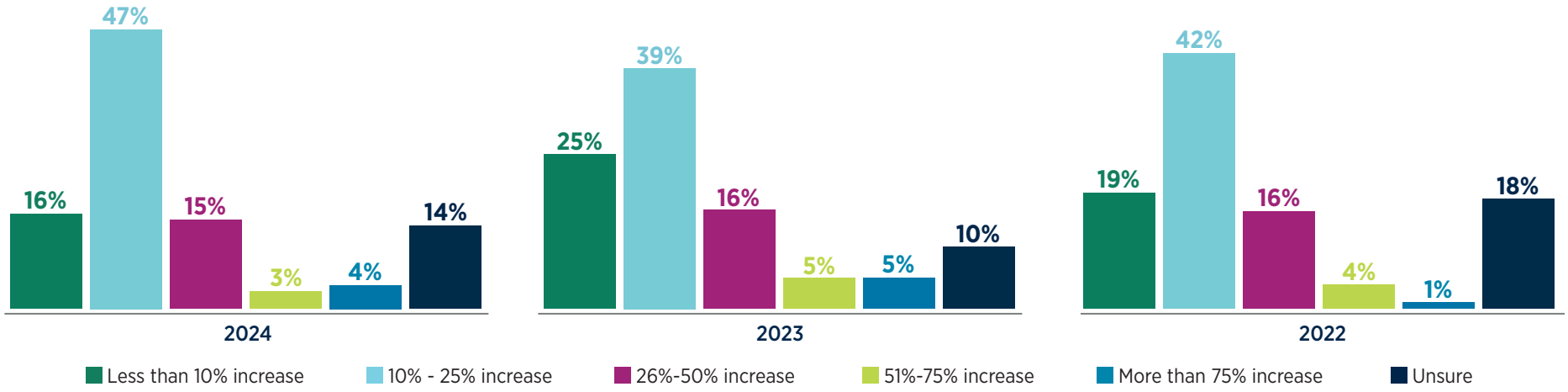
Sixty-seven percent of financial professionals report that the incidence of payments fraud in 2024 was unchanged from that in 2023, while 24% indicate there had been an increase and 9% report a decline. The share of financial professionals reporting an increase in payments fraud activity has steadily declined — from 34% in 2019 to 30% in 2020, and then to 29% in both 2021 and 2022. A slightly higher percentage of respondents from organizations with annual revenue less than $1 billion compared to the share of organizations with annual revenue of at least $1 billion report there was an increase in payments fraud occurrences at their companies in 2024 (26% and 22%, respectively).

Of those organizations that report having experienced an increase in payments fraud activity in 2024, 63% experienced less than a 25% increase in fraud. In 2022 and 2023, over 60% of organizations experienced less than a 25% increase in payments fraud.

Change in Incidence of Payments Fraud in 2024
(Percentage Distribution of Organizations Experiencing Payments Fraud)



Increase in Payments Fraud Compared to Previous Year
(Percentage Distribution of Organizations Reporting More Payments Fraud Attempts in 2024 than in 2023)



PAYMENT METHODS IMPACTED BY FRAUD

Checks Most Susceptible to Payments Fraud

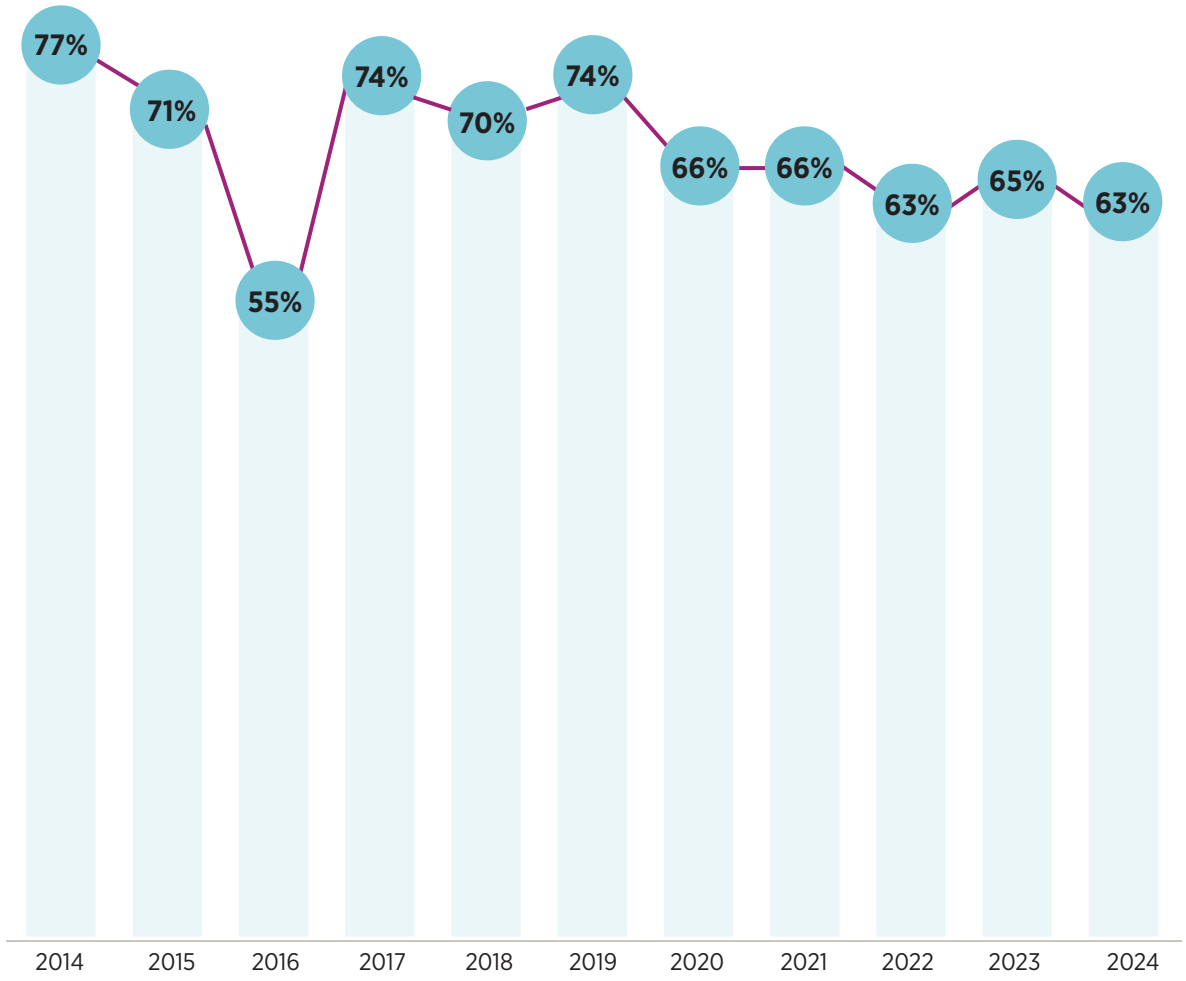
Similar to 2023, checks and ACH debits were the payment methods most often impacted by fraud activity in 2024 (63% and 38%, respectively). Over the past decade payments fraud via checks has declined. Since 2020, the percentage of organizations reporting check fraud activity has been similar — i.e., hovering between 63% and 66%. Sixty-three percent of respondents report that their organizations had been victims of check fraud in 2024.

Checks continue to be used extensively at organizations; this year's survey results reveal that over 90% of organizations use checks. (Later in this report, we discuss check usage in more detail. See page 35.) Therefore, it is no surprise that checks are the payment method most often impacted by payments fraud.

While fraudsters continue to innovate with new technology, continued use of checks is keeping the oldest methods of fraud alive and well. In a 2024 report, FinCEN found that mail-theft related check fraud may have caused up to $668 million in losses over a six-month period in 2023.[1] This uptick in mail-related check fraud is in line with figures reported in the *2023 AFP Payments Fraud and Control Survey*, as well as the current survey (discussed later in the report in greater detail).

The share of respondents reporting payments fraud via ACH debits rose from 33% in 2023 to 38% in 2024. Over the past three years, ACH debit fraud has been gradually creeping back up, surpassing the record level of 37% in 2021. This increase could be connected to the uptick in the incidence of check fraud, with fraudsters creating an ACH debit with stolen check information. ACH debit fraud has also likely increased due to a rise in overall ACH volume. According to Nacha (which governs the ACH Network), total ACH payment volume rose 6.7% to 33.6 billion transactions in 2024, a value of $86.2 trillion.[2] The increase in ACH credit fraud, however, was minimal, with 20% of organizations experiencing fraud in 2024 while 19% did so in 2023.

Check Fraud Activity: Trends
(Percent of Organizations)



[1] https://www.fincen.gov/news/news-releases/fincen-issues-depth-analysis-check-fraud-related-mail-theft
[2] https://www.nacha.org/content/ach-network-volume-and-value-statistics

PAYMENT METHODS IMPACTED BY FRAUD CONTINUED

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%	--

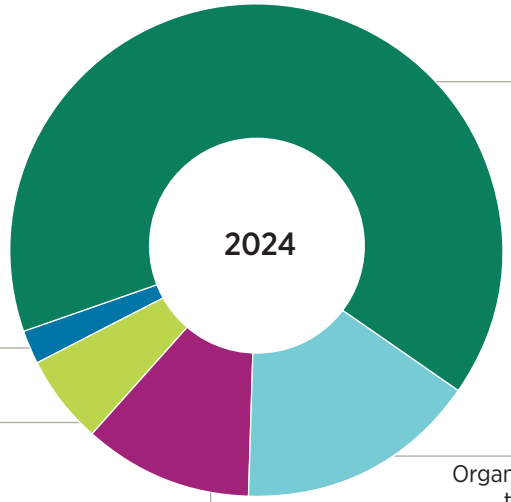
"Credit card fraud is the most prevalent fraud we have encountered. We are closing and replacing cards monthly. Our theory is that vendors have systems that are compromised, and our card numbers get stolen."

"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."

PAYMENT METHODS IMPACTED BY FRAUD CONTINUED

Of those organizations that experienced payments fraud via ACH credits or ACH debits, 65% validate payment details manually. Sixteen percent use an external service to validate payment information and 11% rely on a financial vendor/bank to do so.

Organizations That Validate Beneficiary Payment Information
(Percentage Distribution of Organizations)



65%
Organization validates payment details manually

2%
Organization does not validate beneficiary payment information

6%
Other

16%
Organization uses an external service to validate payment information

11%
Organization relies on financial vendor/bank to do so

Other includes:

- Organization uses third-party service as well as manual verifications
- Payment beneficiaries are validated for certain programs
- Beneficiary banking details are collected via DocuSign® and dual authentication, if necessary, verbal verification is done

LOSSES INCURRED DUE TO PAYMENTS FRAUD ATTACKS/ATTEMPTS

Estimated Total Dollar Amount of Actual Financial Loss and Costs to Manage/Defund/Clean-up Fraud

Historically, actual financial losses from payments fraud attacks are not extensive; that continued to be the case in 2024. Forty-six percent of respondents report that their organizations did not incur a financial loss in 2024, while 21% report that they incurred a loss of less than $25,000. A higher percentage of organizations with annual revenue less than $1 billion report they did not incur a loss than did those companies with annual revenue of at least $1 billion (52% versus 43%).

Estimated Total Dollar Loss to Organization from Payments Fraud
(Percentage Distribution 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	2023
No loss	46%	52%	43%	54%	27%	41%
Up to $24,999	21%	22%	18%	20%	18%	25%
$25,000-$49,999	7%	7%	7%	3%	10%	7%
$50,000-$99,999	8%	8%	8%	7%	6%	7%
$100,000-$249,999	6%	5%	7%	7%	9%	11%
$250,000 - $499,999	4%	3%	5%	3%	6%	5%
$500,000 - $999,999	3%	1%	4%	4%	4%	3%
$1,000,000 - $1,999,999	3%	1%	5%	1%	10%	--
Over $2,000,000	2%	1%	3%	1%	9%	1%

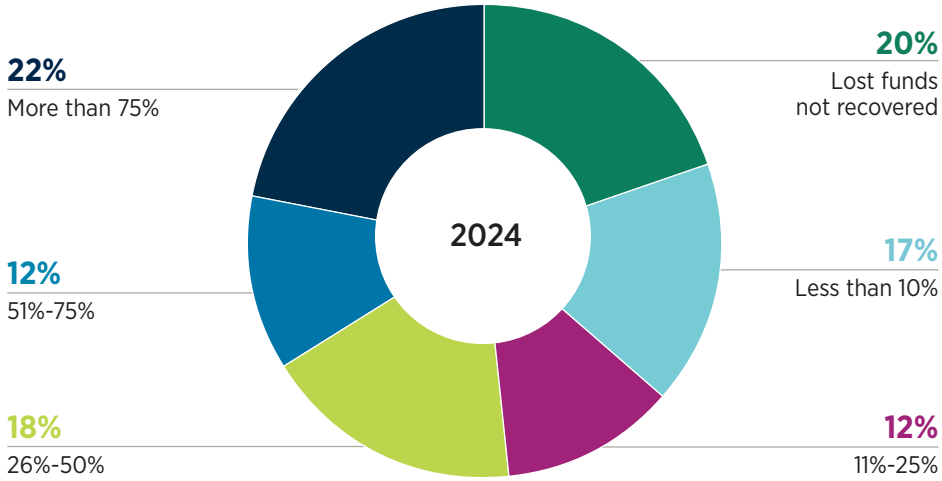
RECOVERING LOST FUNDS

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 was 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."

DETECTING FRAUD ACTIVITY

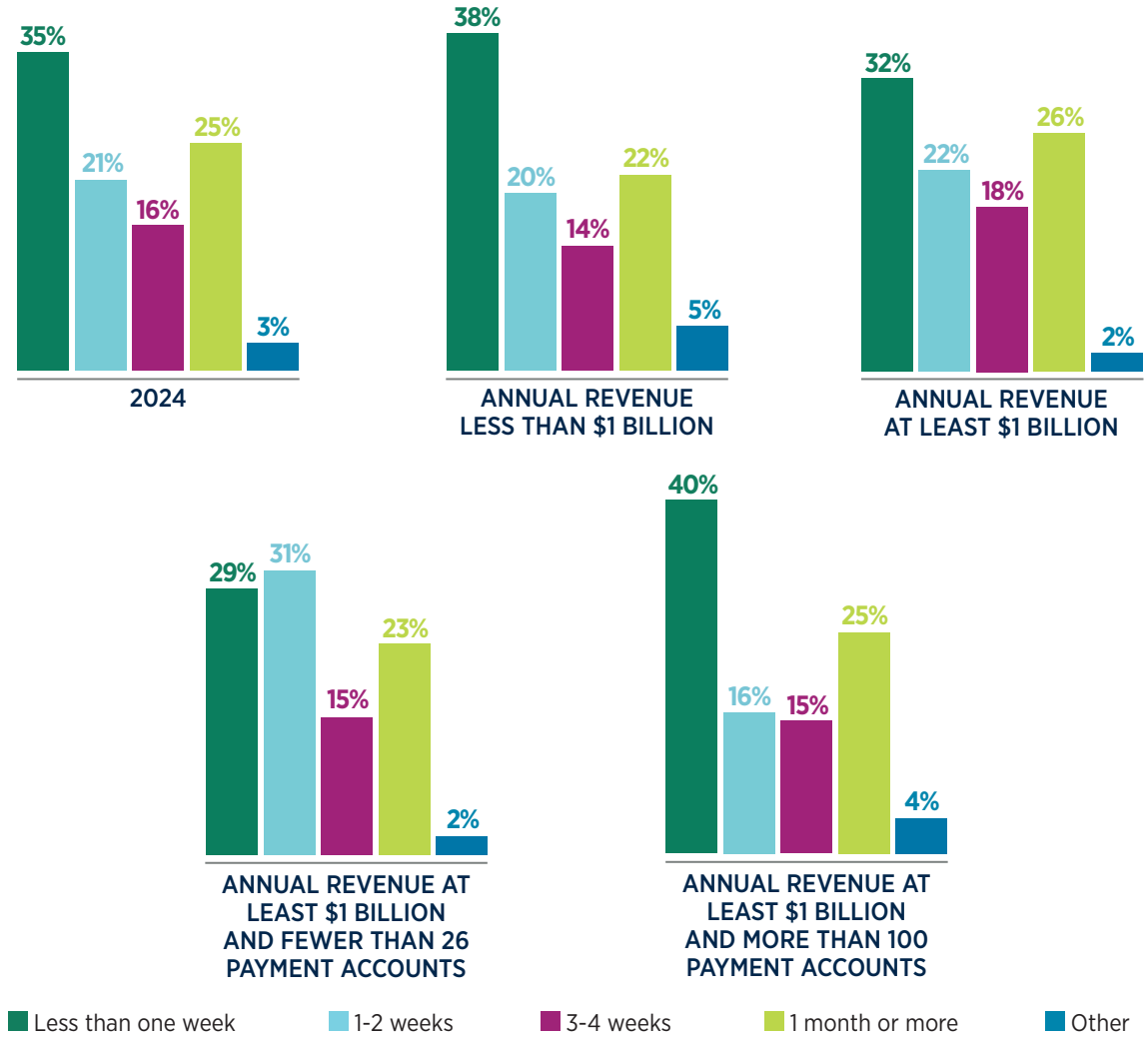
Thirty-Five Percent of Organizations Detect Fraud Activity in Less Than One Week

Of those organizations that were victims of payments fraud attacks and incurred actual losses in 2024, 35% took less than one week to uncover the fraud, and 21% detected the fraudulent activity within one to two weeks. Sixteen percent took an additional two weeks to realize they had been targets of an attack, and 25% took a month or longer to uncover the fraud. Forty percent of organizations with annual revenue of at least $1 billion and more than 100 payment accounts were able to detect fraud in less than one week, while 29% of organizations with similar annual revenue but fewer than 26 payment accounts realized they had been impacted by fraud in the same timeframe.

Organizations need to be vigilant and ensure they can discover fraud before its effects are damaging. While about three-quarters of organizations were successful in realizing they were targeted in less than one month, 25% became cognizant of the fraud attack only after a month or more. The longer it takes to identify the fraud, the greater the possibility that the impact from the fraud can be detrimental.

Those organizations that are unable to detect fraud promptly need to enhance their fraud detection systems so they are able to detect fraud occurrences within a few days rather than discovering an incident weeks or months later. This might require investing in technology, as well as educating employees who are on the frontline of payments fraud. It will encourage financial professionals to be cognizant of fraud attempts and so can halt fraud before its impact is severe. The quicker fraud is detected, the greater the chances of recovery, especially (as noted earlier in this report) since 22% of organizations were successful in recovering more than 75% of funds lost due to fraud.

Time Taken to Discover Fraud
(Percentage Distribution of Organizations Experiencing Actual Losses Due to Payments Fraud)



Other includes:

- Electronic less than one week, checks longer
- Variable per event, type of fraud

Treasury Most Likely to Discover Fraud

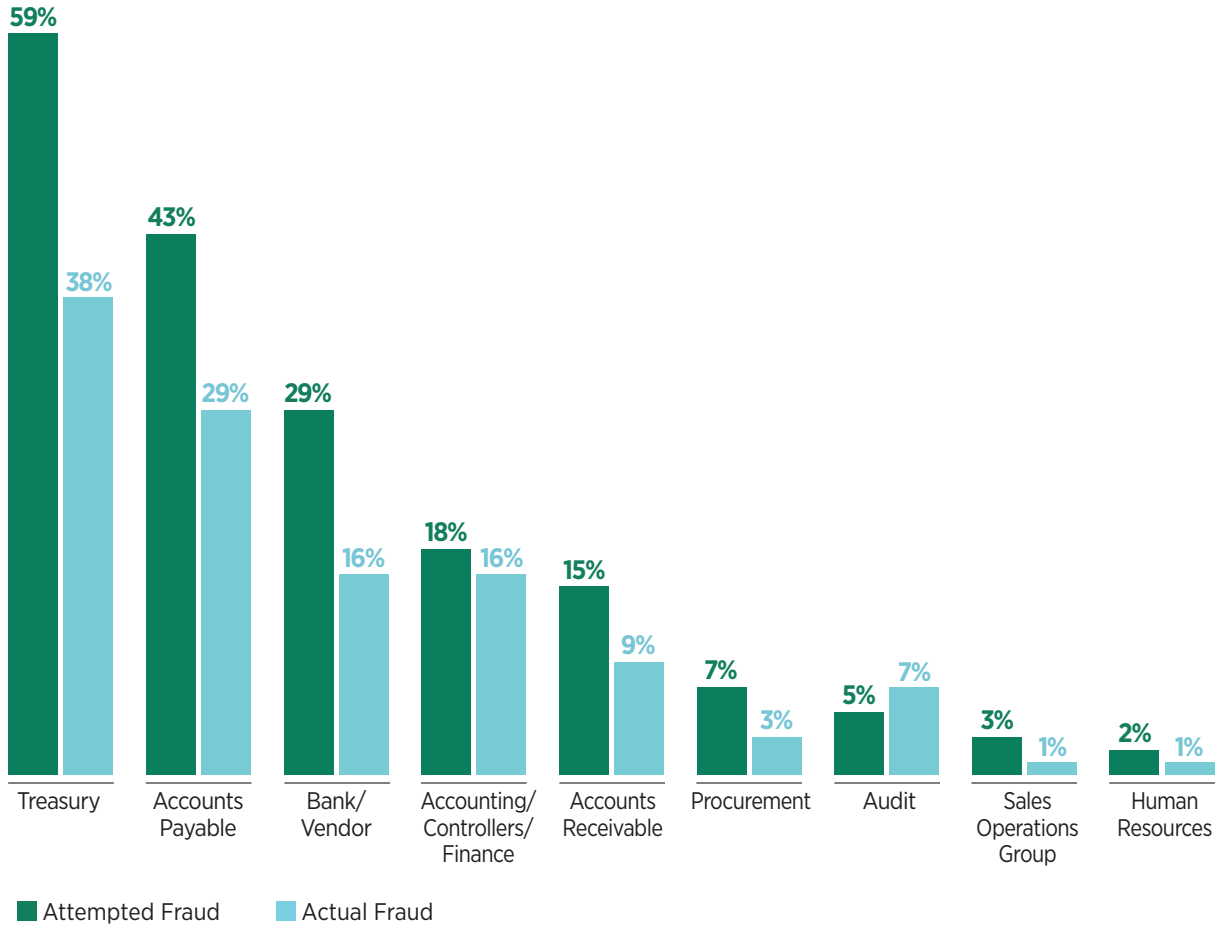
Treasury is the department most likely to uncover both attempted and actual payments fraud activity, followed by accounts payable (AP). This is not surprising since these two teams review payments most often. While fraud detection occurs more often within those departments related to treasury and finance operations, other teams detecting payments fraud activity include audit, procurement, sales operations and human resources. Banks/vendors also play a role in discovering both attempted and actual payments fraud.

As the departments that initiate and release various types of payments, treasury and AP must be cognizant of the latest fraud threats. Treasury has a distinct advantage in detecting fraud since it reviews bank account activity daily. AP constantly watches for fraud as it handles transactions — i.e., vendor master, duplicate payments, card fraud, etc. Both departments must be in sync, using the same standards, protocols and tools to identify any suspicious activity.

Other groups that discover fraud:

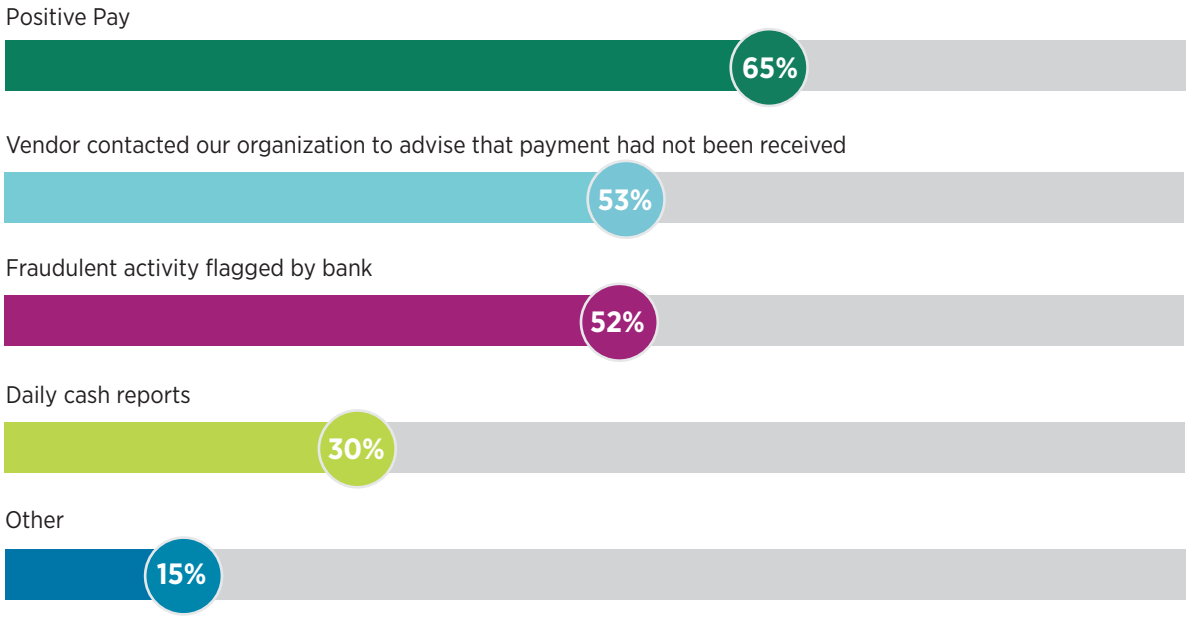
- Security (fraud) department
- IT
- Production department
- Cyber risk, fraud operations team
- Vendor management
- Claims departments
- Customers
- Supplier team

Department Most Likely to Discover Payments Fraud
(Percent of Organizations Experiencing Payments Fraud)



DETECTING FRAUD ACTIVITY CONTINUED

Means by Which Fraud Was Discovered
(Percent of Organizations Experiencing Payments Fraud)



Other includes:

- Expense report audits
- Check images
- Product was not delivered
- Notified by customer
- Callback revealed fraud
- Cardholder identified fraud on card
- Client account was overdrawn

"During our company-wide week-long shutdown for the holidays, several attempts to debit the company's ACH account were made, each was negated by positive pay."

"A vendor check was stolen from the mail and a fraudulent check written. We have payee verification and positive pay. 98% of our check fraud is caught with these two treasury services."

ORIGINATIONS OF FRAUD

Over 60% of Payments Fraud Originates from Email

In 2024, the most common source of payments fraud was via business email compromise (BEC); 62% of respondents report that payments fraud at their companies was the result of a fraudulent email. Nearly 50% of financial professionals report that payments actions by an individual outside the organization was the source of fraud at their companies including forged checks, stolen cards, identity fraud, etc. Forty-five percent of organizations were targeted by vendor impostors, an increase from past years. Greater vigilance and implementation of processes to streamline vendor verification is necessary.

Invoice fraud was experienced at 24% of organizations in 2024, while 23% of respondents report fraud due to interference with the United States Postal Service (USPS). That result is two percentage points higher than the share reported for 2023, signaling organizations continue to be vulnerable to this type of fraud, and need to mandate a verified signature upon delivery of checks or use a reliable tracking system. The Financial Crimes Enforcement Network (FinCEN) received more than 15,000 Bank Secrecy Act reports about possible mail theft-related check fraud during a six-month period in 2023, which were associated with $688 million in actual or attempted transactions, the agency said in a financial trend analysis on the problem.[3] Banks filed 88% of check fraud reports, the majority coming from small-to-medium-sized banks.[4]

Other sources of payments fraud include:

- **Imposter posing to client as an organization representative** (cited by 14% of respondents)
- **Third-party or outsourcer** (12%)
- **Account takeover** (e.g., hacking a system, adding malicious code — spyware or malware from social network) (12%)

In late 2024, FinCEN issued an alert about an increase in fraud schemes involving deep-fake media through generative AI (Gen AI).[5] While payments fraud via deep-fake attempts was observed at only 5% of organizations; that result is an increase from the 1% for 2023, and one that needs to be closely watched. Advances in AI will enable scammers to produce videos and images to easily deceive targets. Although only 3% of financial professionals report fraud by an internal party during 2024, these professionals belong to a variety of departments and are most represented by employees from sales and accounting,

A larger share of respondents from companies with annual revenue of at least $1 billion and more than 100 payments were targets of BEC fraud (66%) in 2024 than were other companies. While it is challenging to anticipate fraud attacks, financial professionals should ensure that their organizations have controls that safeguard against payments fraud. The continued occurrence of "sophisticated" fraud such as account takeovers and attacks utilizing deep-fake media and GenAI, suggests that fraud mitigation — in addition to robust internal controls — should also focus on using the latest and best-in-class security protocols to prevent external parties from gaining access to internal systems.

[3] https://www.fincen.gov/news/news-releases/fincen-issues-depth-analysis-check-fraud-related-mail-theft

[4] Ibid.

[5] https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf

ORIGINATIONS OF FRAUD CONTINUED

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%

ASSISTANCE SOUGHT WHEN REPORTING PAYMENTS FRAUD

Assistance from Banking Partners and Keeping Internal Security Team Informed Are Processes Commonly Used When Reporting Payments Fraud

When looking to report payments fraud, 80% of respondents report that their organizations are most likely to reach out to their banking partners for advice on how to manage such fraud. Therefore, organizations need to ensure their banking partners are well-versed in dealing with fraud and minimizing its impact on clients. When selecting banking partners, organizations should review their RFP for banking services emphasizes payments fraud vigilance as a requirement. Seventy percent of respondents report that they would inform the security/compliance team at their organizations, while 39% report they would file a report with police (local, state or federal).

Over 70% of organizations seeking assistance from banking partners to report payments fraud indicate that they are either very satisfied or satisfied with such assistance from their banks. At the same time, more than 20% are neither satisfied nor dissatisfied, while 5% are dissatisfied with the assistance they received in resolving the issues arising from payments fraud. Organizations need to be confident that their banking partners are sufficiently experienced and knowledgeable to help them in mitigating payments fraud — both before and once the fraud occurs — in order to mitigate the impact. Efficient banking partners that support organizations in their fraud resolution will enable practitioners to focus on their job at hand rather than being distracted in dealing with any fraud attack.

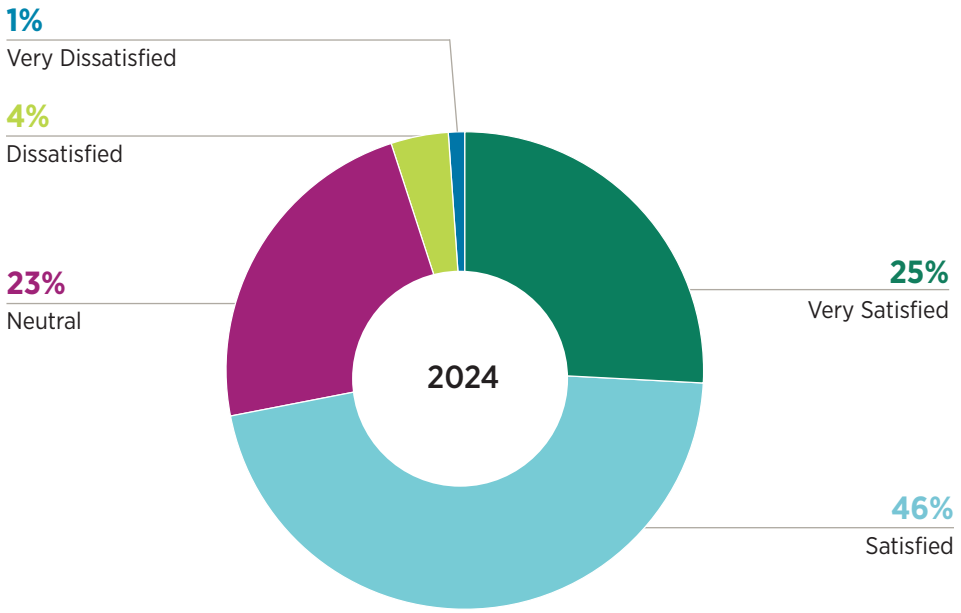
Process Used to Report Payments Fraud
(Percent of Organizations Experiencing Payments Fraud)

	2024
Seek assistance from our banking partner	80%
Inform internal security/compliance team	70%
File report with police (Local, State or Federal)	39%
Inform law enforcement agencies (e.g., FBI)	32%
Inform Federal Trade Commission (FTC)	6%
Other	4%

Other includes:

- Filing of suspicious activity report (SAR) as needed
- Follow regulatory guidelines to report fraud
- Refer to legal department
- Involved USPS Postmaster

Satisfaction with Fraud Resolution Provided by Banking Partners
(Percentage Distribution of Organizations Experiencing Payments Fraud and Seeking Assistance from Banking Partner)



BUSINESS EMAIL COMPROMISE

ABOUT BUSINESS EMAIL COMPROMISE (BEC)

According to the Federal Bureau of Investigation (FBI), business email compromise (BEC) is one of the most financially damaging online crimes. Scams via email exploit the heavy reliance organizations have when conducting business in both their professional and personal lives.[6]

In a typical BEC scam, criminals use social engineering techniques to compromise email messages so that those messages appear to come from a known source making a legitimate request. For example:[7]

- A vendor your company regularly deals with sends an invoice requesting payment. Similarly, the email may appear to come from the CFO with an urgent message about paying an overdue bill.
- A company CEO asks their assistant to purchase dozens of gift cards to send out as employee rewards.
- Emails are sent to the finance department requesting an update of bank account details for payments or to change wiring instructions entirely.

However, these messages are fake and are designed by fraudsters to trick the recipient. In cases like these, hundreds of thousands of dollars have been sent to criminals instead of the intended recipient.

How Criminals Carry Out BEC Scams[8]

Fraudsters utilize a variety of methods to commit payments fraud via business email compromise:

- Spoofing an email account or website
- Sending spear phishing emails
- Using malware to infiltrate a company's network and gain access to legitimate email threads about bills and invoices

While many BEC scams follow familiar patterns, new technology is being adopted to make them harder to detect. Generative AI is being used to create higher quality — and therefore more effective — fraudulent emails. Many employees can now spot obvious spelling and grammatical errors or suspicious email addresses and can recognize many of the telltale signs of a BEC scam (i.e., an urgent message from a senior-level employee asking for an immediate funds transfer). However, AI-generated emails are more sophisticated and have an improved appearance of authenticity.[9] Additionally, fraudsters are targeting high-level executives with EvilProxy phishing technology that tricks users into thinking they are being taken to legitimate websites but are actually directed to phishing pages.[10] Corporate end users need to be even more vigilant in making sure they trust known sources to validate payments, and ensure they have the latest and best tools in place to prevent fraud.[11]

According to the FBI Internet Crime Report, for 2023, **BEC complaints** amounted to **$2.9 billion in reported losses**. **Phishing and spoofing schemes** had over **298,000 complaints**.

Source: The Federal Bureau of Investigation (FBI) Internet Crime Report (2023)

"We had an international customer wire us money. I sent them a signed wire instruction as a PDF. They received an email right after that from an email address very close to mine stating that I made an error and they needed to send it to a different bank. The PDF even still had my signature on it."

"We recently received a fraudulent invoice for over $48,000. An email with the invoice was sent to our accountant with a fake chain of emails attached to look like an approval. We require multiple approvals over $20,000 so we caught it."

[6] https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise
[7] https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise
[8] https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise
[9] https://www.forbes.com/sites/forbestechcouncil/2023/03/03/prepare-for-the-ai-phishing-onslaught/?sh=174c7e8f1925
[10] https://www.linkedin.com/pulse/indeed-executives-targeted-malicious-evilproxy-phishing/
[11] https://www.knowbe4.com/spear-phishing/

ABOUT BUSINESS EMAIL COMPROMISE (BEC) CONTINUED

Increased Vigilance is Making a Dent in Successful Email Scams

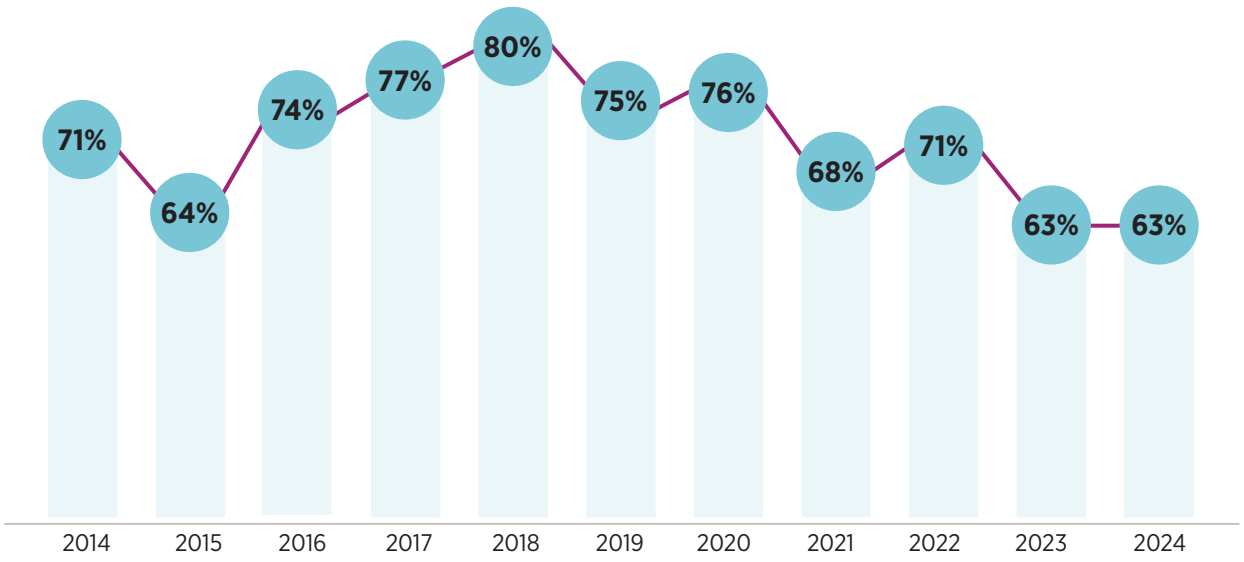
Business professionals predominately use email for communication within their organizations and with clients, vendors, et al. As of April 2024, the U.S. was the country with the largest number of emails sent daily, totaling almost 10 billion.[12] This extensive use of email makes it very susceptible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

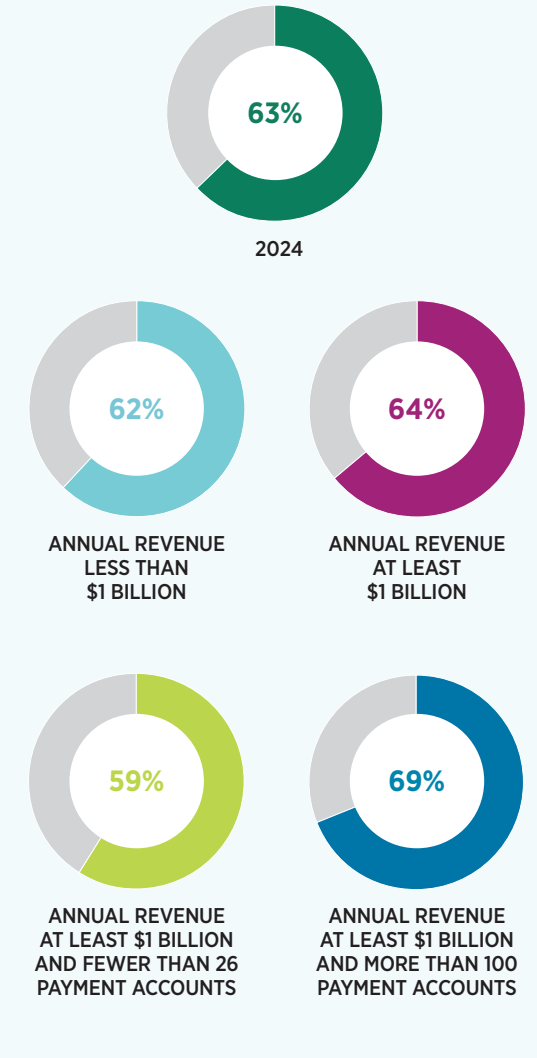
A larger share of organizations with annual revenue of at least $1 billion and more than 100 payment accounts report BEC-based payments fraud than do companies with at least $1 billion revenue and fewer than 26 payment accounts.

[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)



FRAUDSTERS USING EMAIL ARE RELENTLESS

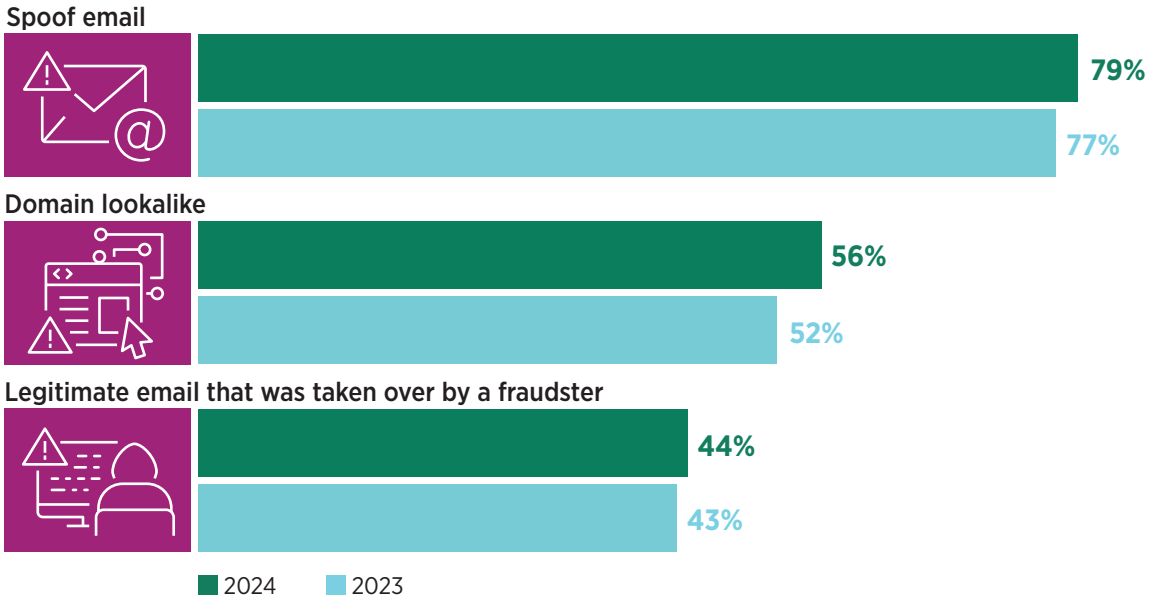
Business Email Compromise Tactics

Fraudsters continue to target organizations through BEC using approaches similar to those observed over the past few years. BEC scammers use few, but effective, schemes to infiltrate organizations.

- **Spoofing an email account or website** (experienced by 79% of organizations, up two percentage points from last year's survey result). Spoofers forge email header elements to trick users into believing they are interacting with a trusted source.
- **Using a domain lookalike** (experienced by 56% of organizations). Bad actors register lookalike 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.
- **Accessing a compromised email account** (experienced by 44% of organizations). Fraudsters use compromised email accounts to send fraudulent change of payment instructions to potential victims.

Fraudsters use a variety of approaches in their email schemes. In many cases, fraudulent emails contain attachments or links that send users to illegitimate websites or payment portals. These links may also expose an organization to malware. Respondents report that their firms receive these messages through other platforms, including via texts (SMS) as well as other messaging apps such as WhatsApp and Signal. As use of this tactic spreads, organizations must be mindful of protecting mobile devices as well.

Most Prevalent Types of Business Email Compromise Fraud
(Percent of Organizations Experiencing Payments Fraud)



"We have a supplier enablement portal (in-house) and one of our vendor's emails was compromised and they requested to update their banking information through the portal. We conduct verbal callbacks for any new or updated banking instructions through our portal."

FRAUDSTERS USING EMAIL ARE RELENTLESS CONTINUED

BEC Perpetrators

BEC perpetrators do not fit a particular mold. However, these fraudsters — from foreign nationals[13] to domestic money mules,[14] — create email compromise schemes designed to deceive an organization into giving up information or making a payment to a fraudulent account.

Sixty-three percent of organizations were targeted by fraudsters impersonating other third parties requesting changes of payment instructions in 2024. Companies with annual revenue of at least $1 billion and more than 100 payment accounts were the organizations most often targeted this way (73%). Organizations with annual revenue less than $1 billion have the most experience with fraudsters pretending to be senior executives directing finance personnel to transfer funds to the fraudsters' accounts (63%).

Some variations of the above include fraudsters intercepting emails from a vendor or customer to insert themselves into the payment process, fraudsters acting as employees requesting changes in direct deposit account information, and fraudsters impersonating vendors in order to obtain shipment information used by them in arranging to pick up and steal cargo.

[13] https://www.justice.gov/usao-md/pr/nigerian-national-arrested-ghana-facing-federal-charges-alleged-75-million-business
[14] https://www.justice.gov/usao-mdal/pr/lake-placid-florida-man-sentenced-participating-business-email-compromise-scheme

Business Email Compromise Fraud Perpetrators
(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	2023
Fraudsters impersonating other third parties requesting changes of bank accounts, payments instructions, etc.	63%	54%	68%	66%	73%	63%
Fraudsters impersonating vendors directing transfers based on invoices to the fraudsters' accounts	60%	63%	59%	57%	67%	57%
Fraudsters pretending to be senior executives directing finance personnel to transfer funds to the fraudsters' accounts	49%	63%	39%	43%	38%	57%

FINANCIAL IMPACT OF BUSINESS EMAIL COMPROMISE

The percentage of financial professionals reporting that their organizations experienced a financial loss due to BEC in 2024 is 36%. This figure is up two percentage points from 2023.

Even when organizations experience financial losses due to BEC, the losses are not typically high dollar amounts. Nineteen percent of organizations incurred a loss of less than $50,000 from BEC-based payments fraud in 2024; only 3% report a loss of more than $1 million. When viewing the data for the past four years, losses in the dollar ranges shown in the figure to the right remain similar. This suggests that even as BEC scams continue to evolve and become more sophisticated, employee training and education, manual verification — along with increased digital transaction security measures — continue to be critical in an organization's comprehensive payments fraud prevention strategy.

The Internet Crime Complaint Center (IC3) estimates that BEC resulted in over $55 billion in losses between October 2013 and December 2023.[15] However, the consequences of BEC extend beyond financial loss. Organizations that have experienced BEC may suffer supply-chain and operational disruptions. BEC incidents can erode the reputation of a brand, causing corporate shares to fall in value and ultimately impacting earnings and employee headcount. Organizations exposed to BEC may also face legal repercussions if personally identifiable information (PII) has been exposed. The loss of trust after an information breach or the damage to brand perception can be difficult to reverse.

[15] https://www.ic3.gov/PSA/2024/PSA240911

Estimated Total Dollar Loss to Organization from Business Email Compromise in 2024
(Percent of Organizations Experiencing Payments Fraud)

	2023	2022	2021	2021
No Loss	64%	66%	60%	65%
Up to $24,999	12%	11%	12%	13%
$25,000-$49,999	7%	5%	5%	5%
$50,000-$99,999	3%	4%	6%	6%
$100,000-$249,999	7%	6%	5%	6%
$250,000 - $499,999	3%	3%	5%	4%
$500,000 - $999,999	1%	4%	3%	2%
$1,000,000 - $1,999,999	2%	1%	2%	--

"A check was intercepted by another tenant of the intended payee. A police report was filed and a fraud investigation has been launched by the bank. Funds have yet to be recovered. This process was kicked off 2-3 weeks ago."

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)

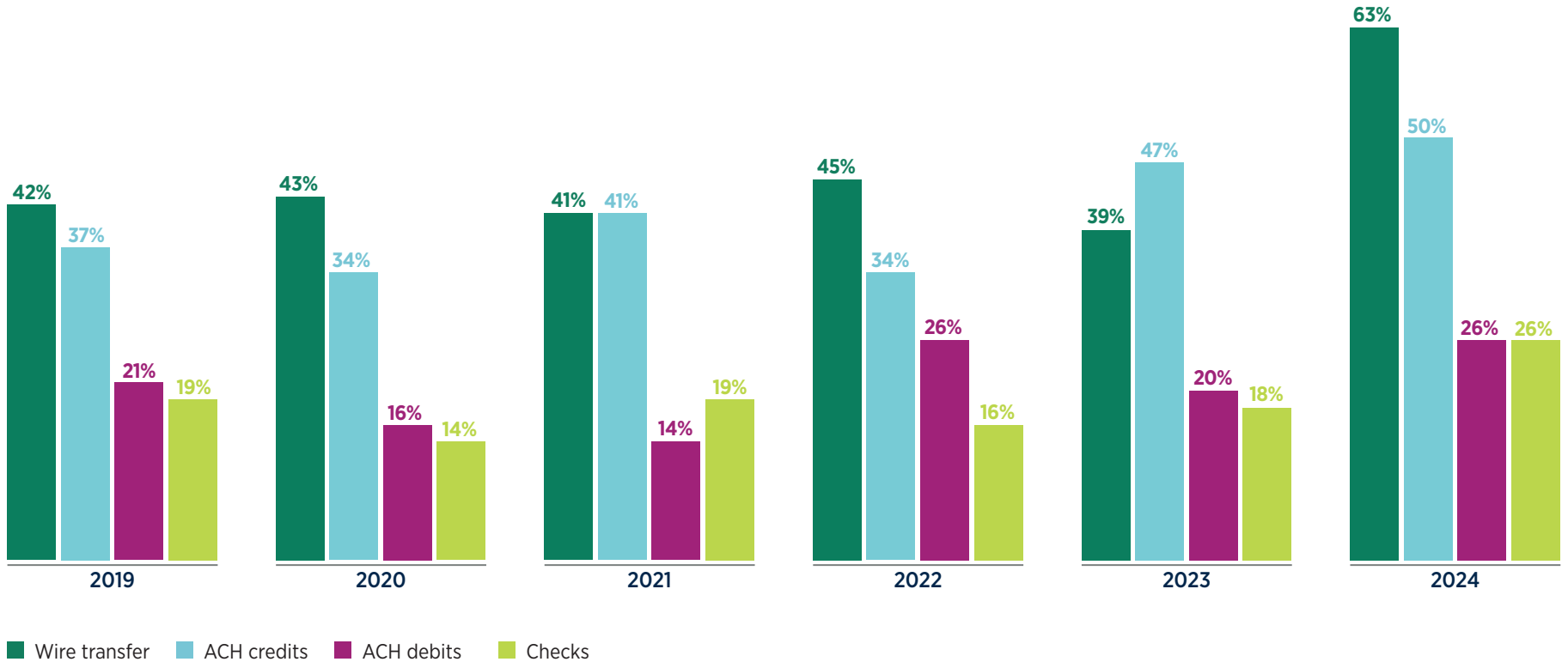
	2024	ANNUAL REVENUE LESS THAN $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION AND FEWER THAN 26 PAYMENT ACCOUNTS	ANNUAL REVENUE AT LEAST $1 BILLION AND MORE THAN 100 PAYMENT ACCOUNTS
Wire transfers	63%	55%	64%	53%	76%
ACH credits	50%	68%	43%	53%	40%
Checks	26%	23%	26%	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	--	--	--	--	--

PAYMENT METHODS IMPACTED BY BEC CONTINUED

In this year's survey, wire transfers replaced ACH credits 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 increased 24 percentage points in 2023 to 63%. ACH credits are the most-often used payment method targeted in BEC by 50% of respondents, a three-percentage-point increase from 2023. The share of respondents reporting that ACH debits were used by fraudsters to infiltrate organizations via email scams increased in 2024 by 6 percentage points.

The return to targeting wire transfers via BEC is likely due to this payment method previously being viewed as the most effective vehicle for these scams. While ACH credits surpassed wires in the *2023 AFP® Payments Fraud and Control Survey*, this was likely an aberration; the new 2024 data reveal that BEC scammers have returned to their old ways.

Top Payment Methods Impacted by Business Email Compromise, 2019-2024
(Percent of Organizations Experiencing Business Email Compromise)



DEPARTMENTS VULNERABLE TO EMAIL SCAMS

Accounts Payable Department Continues to be the Most Vulnerable to BEC

While organizations have been vigilant about detecting email scams by improving their systems — as well as ensuring their employees are able to detect fraudulent emails by providing training and education — email fraud continues to prevail. Email can easily infiltrate an organization, and with AI and other enhanced technologies, scammers are able to create emails that look very authentic and well targeted.

More than half of practitioners that their AP departments (56%) most vulnerable to email fraud in 2024. This figure has remained steady over the past few years — 59% in 2023, 60% in 2022 and 58% in 2021 — likely because AP departments are where payments originate. Rounding out the top three departments vulnerable to BEC are treasury (cited by 9% of respondents) and C-suite (9%), but both to a significantly lesser degree than AP. Other departments within organizations reported to be the most vulnerable include:

- Customer service
- Operations
- Agency commissions
- Production
- Project managers/vendors
- Sales
- Supplier team

Departments Most Vulnerable to Business Email Compromise
(Percentage Distribution of Organizations Experiencing Business Email Compromise)

	2024	2023	2022
Accounts Payable	56%	59%	60%
Treasury	9%	10%	9%
CEO, COO, CFO, or other C-Suite Executive	9%	7%	5%
Procurement/Sourcing	8%	12%	10%
Accounting/Controllers	5%	4%	2%
Accounts Receivable	4%	1%	2%
Human Resources/Payroll Department	1%	2%	4%
Other	8%	6%	7%

NOTE: Some detail may not add to 100% due to rounding

"Email spoofed and our AP personnel did not follow internal controls when changing payee bank account data. The funds were wired to fraudsters."

BUSINESS EMAIL COMPROMISE PREVENTION — POLICIES AND PROCEDURES

Business Email Compromise Prevention Takes Various Forms

Organizations are focused on implementing policies that will support their employees in detecting fraudulent emails and enhancing their internal systems in order to flag such emails before they are delivered. These efforts help in minimizing email-based payments fraud and its impact. Employees who fall victim to these email scams by simply clicking on a link or opening an attachment can cause severe damage and inconvenience to their organizations. To prevent having to deal with the effects of an email scam, organizations are working hard to develop and implement a variety of policies and procedures designed to prevent payments fraud via BEC.

At the top of the list in this year's survey is *implementation of end-user education and training on the BEC threat and how to identify spear phishing attempts;* 96% of respondents report having implemented these measures. Eighty-four percent of organizations that have implemented end-user education have found it to be very effective or effective in curbing payments fraud attacks via BEC.

Ninety-four percent of companies have *implemented company policies for providing appropriate verification of any changes to existing invoices*, bank deposit information and contact information. This approach appears to have been effective in controlling BEC as reported by 93% of respondents.

Other policies and procedures implemented by organizations to curb BEC fraud are:

- **Confirming a request for a funds transfer by executing a callback to a verified and authorized contact at the payee organization using a phone number from a system of record** (implemented at 91% of organizations)
- **Stronger internal controls prohibiting payments initiation based on emails or other less secure messaging systems** (91%)
- **Requiring authorized signoff of senior management for transactions over a certain threshold** (89%)
- **Providing additional training to/reprimanding employees who repeatedly fail simulated testing or open phishing emails** (79%)
- **Using passcodes known only to both parties in proposed wire transactions** (not contained in an email) (42%)
- **Terminating employees who repeatedly fail simulated testing or open phishing emails** (33%)

The weak link in policies and procedures is the human element. IC3 advises organizations to stay vigilant against BEC, using secondary channels or two-factor authentication to verify requests for changes in account information.[16] Financial professionals should verify any email addresses used to send emails by ensuring the sender's address matches who it supposedly came from. They should also ensure that the settings on their computers are enabled to allow full email extensions to be viewed.

[16] https://www.ic3.gov/CrimeInfo/BEC

BUSINESS EMAIL COMPROMISE PREVENTION — POLICIES AND PROCEDURES CONTINUED

Effectiveness of Policies and Procedures Implemented by Organizations to Prevent Business Email Compromise
(Percent of Organizations)

	IMPLEMENTED	VERY EFFECTIVE	EFFECTIVE	SOMEWHAT EFFECTIVE	NOT VERY EFFECTIVE	VERY INEFFECTIVE
End-user education and training on the BEC threat and how to identify spear phishing attempts	**96%**	43%	41%	14%	2%	--
Implementing company policies for providing appropriate verification of any changes to existing invoices, bank deposit information and contact information	**94%**	56%	37%	7%	--	1%
Confirming requests for transfer of funds by executing a call back to a verified and authorized contact at the payee organization using a phone number from a system of record (not numbers listed in an email)	**91%**	65%	26%	9%	--	--
Stronger internal controls prohibiting payments initiation based on emails or other less-secure messaging systems	**91%**	53%	36%	10%	1%	--
Requiring authorized signoff of senior management for transactions over a certain threshold	**89%**	51%	36%	11%	2%	--
Providing additional training to/reprimanding employees who repeatedly fail simulated testing or open phishing emails	**79%**	33%	46%	18%	3%	--
Using passcodes known only to both parties in a proposed wire transaction (not contained in an email)	**42%**	54%	31%	12%	2%	1%
Terminating employees who repeatedly fail simulated testing or open phishing emails	**33%**	29%	26%	30%	13%	2%

BUSINESS EMAIL COMPROMISE PREVENTION — SECURITY AND COMPLIANCE MEASURES

Business Email Compromise Prevention Includes Effective Controls

Organizations are also attempting to control BEC-based payments fraud by adding a layer of protection through the application of various security and compliance measures. In this year's survey, respondents cite *the adoption of two-factor authentication (or other added layers of security) in order to access a corporate network or to initiate payment* as the most effective compliance measure. When "very effective" and "effective" ratings are combined, two-factor authentication is cited by 91% of respondents as an effective measure to combat BEC fraud. Two-factor authentication is used at 92% of organizations in their efforts to mitigate payments fraud via email (up from 89% in 2023).

Practitioners are increasingly relying on other compliance measures commonly being utilized at organizations that also appear effective in curbing BEC, including:

- **Review of emails forwarded outside of your organization** (implemented at 71% of organizations)
- **Color-coded emails with colored banners or other methods of distinction, etc., indicating they are external** (63%)
- **Intrusion detecting systems that flag emails with extensions similar to company emails** (example: where "rn" could be in the place of an "m," etc.) (63%)
- **Prohibiting, or at least quickly detecting, emails where the "reply" email address is different than the "from" email address shown** (57%)
- **Utilizing a bank/vendor solution that captures beneficiary information managed by the beneficiary for refunds/returns** (51%)
- **Implementing TLS keys between the sender and bank in lieu of an encrypted email or password-protected document to validate payment information via email** (45%)

BUSINESS EMAIL COMPROMISE PREVENTION — SECURITY AND COMPLIANCE MEASURES CONTINUED

Effectiveness of Security and Compliance Measures Utilized by Organizations to Prevent Business Email Compromise
(Percent of Organizations)

	IMPLEMENTED	VERY EFFECTIVE	EFFECTIVE	SOMEWHAT EFFECTIVE	NOT VERY EFFECTIVE	VERY INEFFECTIVE
Adopting at least a two-factor authentication or other added layers of security for access to company network and payments initiation	**92%**	56%	35%	9%	--	--
Review of email forwarded outside of your organization	**71%**	34%	42%	21%	2%	1%
Color-coded emails with colored banners or other methods of distinction, etc., indicating they are external	**63%**	34%	35%	25%	5%	1%
Intrusion detecting system that flags emails with extensions that are similar to company email (example: where "rn" could be in the place of an "m," etc.)	**63%**	41%	41%	15%	3%	--
Prohibiting, or at least quickly flagging, emails where the "reply" email address is different than the "from" email address shown	**57%**	35%	44%	17%	4%	--
Utilizing a bank/vendor solution that captures beneficiary information managed by the beneficiary for refunds/returns	**51%**	43%	41%	13%	1%	2%
Implementing TLS keys between the sender and bank in lieu of an encrypted email or password-protected document to validate payment information via email	**45%**	46%	36%	15%	3%	--

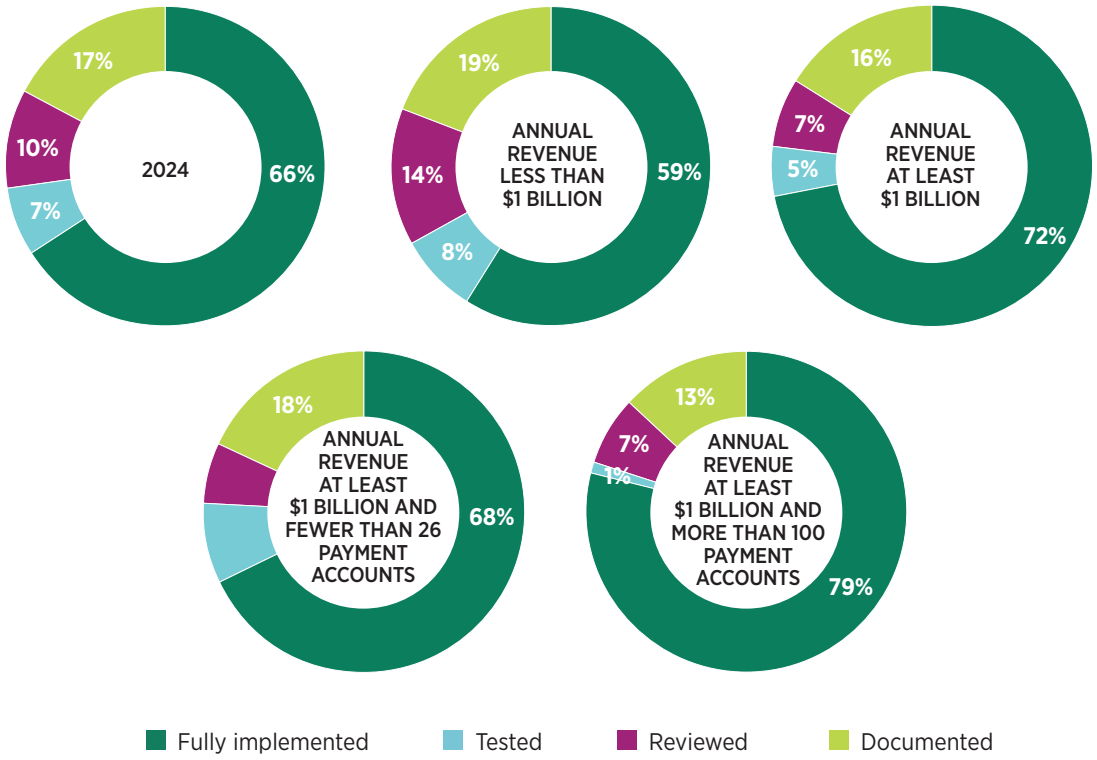
PREVENTING BUSINESS EMAIL COMPROMISE

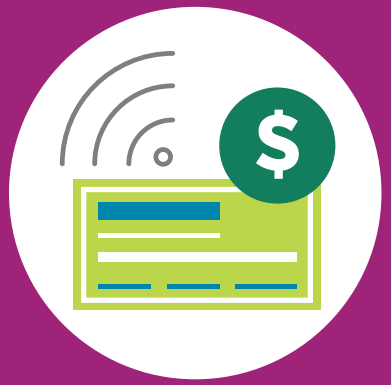
Rollout of Policies and Procedures Designed to Prevent Business Email Compromise

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 AND ACH

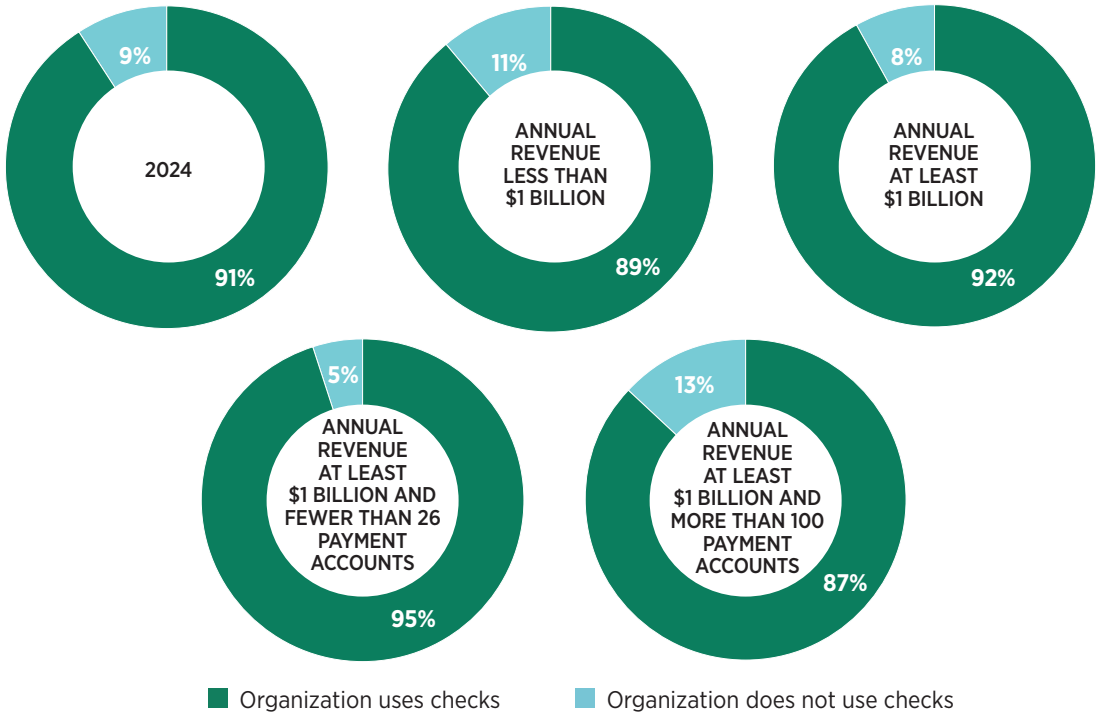
CHECKS CONTINUE TO BE A POPULAR METHOD OF PAYMENT AT ORGANIZATIONS

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%

CHECKS CONTINUE TO BE A POPULAR METHOD OF PAYMENT AT ORGANIZATIONS CONTINUED

Plans to Eliminate Checks

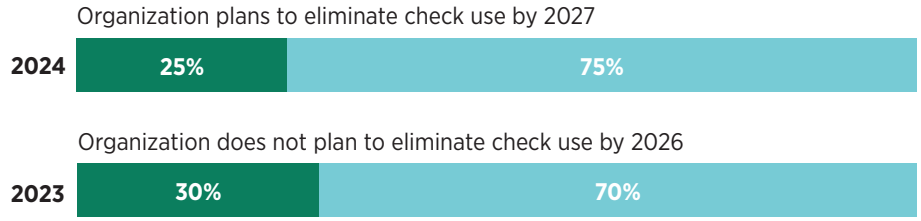
Of those organizations currently using checks, 25% plan to eliminate check use within the next two years. This is down slightly from the 30% of organizations that indicated they planned to curb check use in the *2024 Payments Fraud and Control Survey* (reflecting results for 2023) in two years.

Practitioners cite various reasons in support of eliminating checks. The top reason is the burden of manually processing checks (cited by 75% of respondents). Other reasons reported by a majority of respondents include:

- **Vulnerability to fraud** (cited by 66% of respondents)
- **Administrative and labor costs** (61%)
- **Administrative burden** (56%)

Intent to Eliminate the Use of Checks by 2027

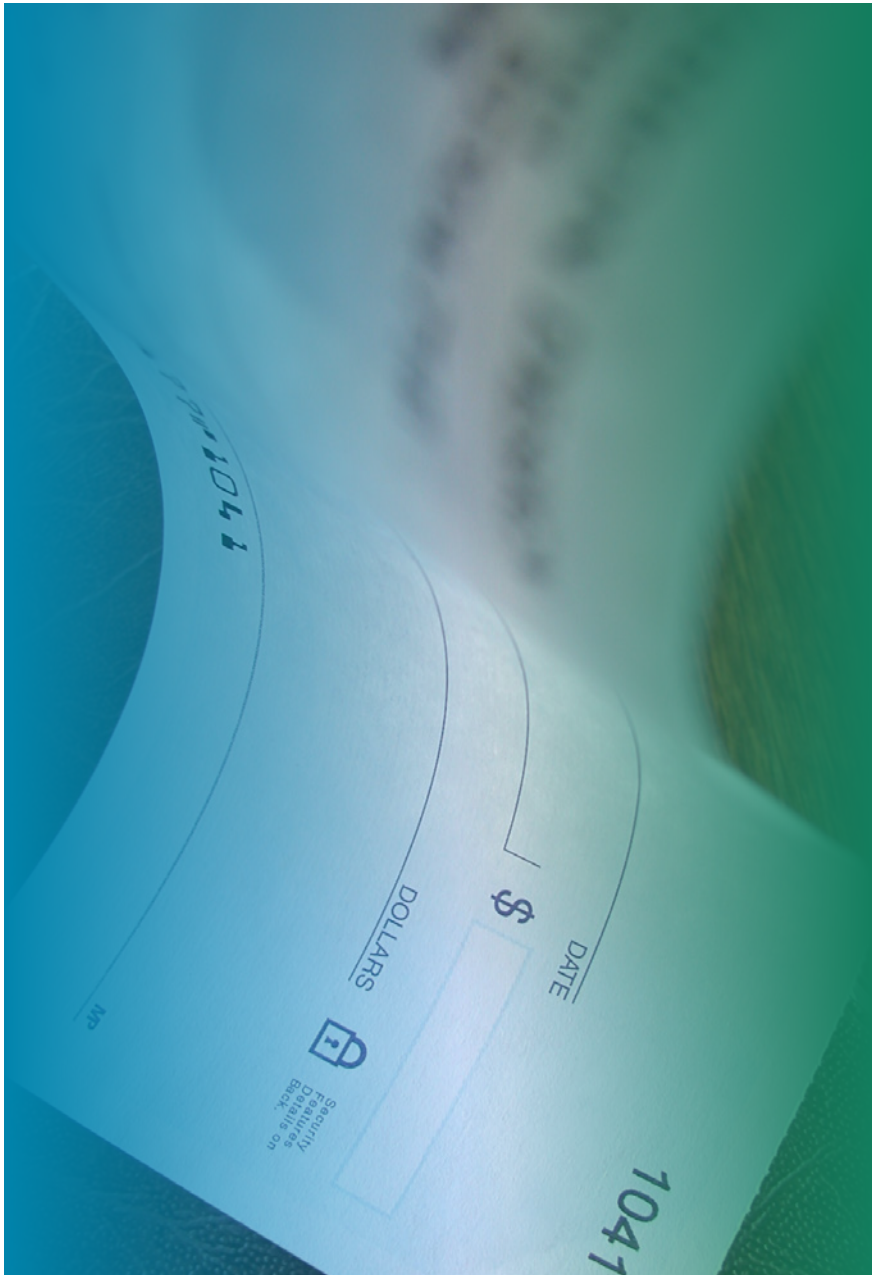
(Percentage Distribution of Organizations Using Checks)



Reasons for Considering Eliminating the Use of Checks

(Percent of Organizations Planning to Eliminate Use of Checks)

Manual process	75%
Vulnerability to fraud	66%
Administrative and labor costs	61%
Administrative burden	56%
Escheatment process	26%
Float time	25%

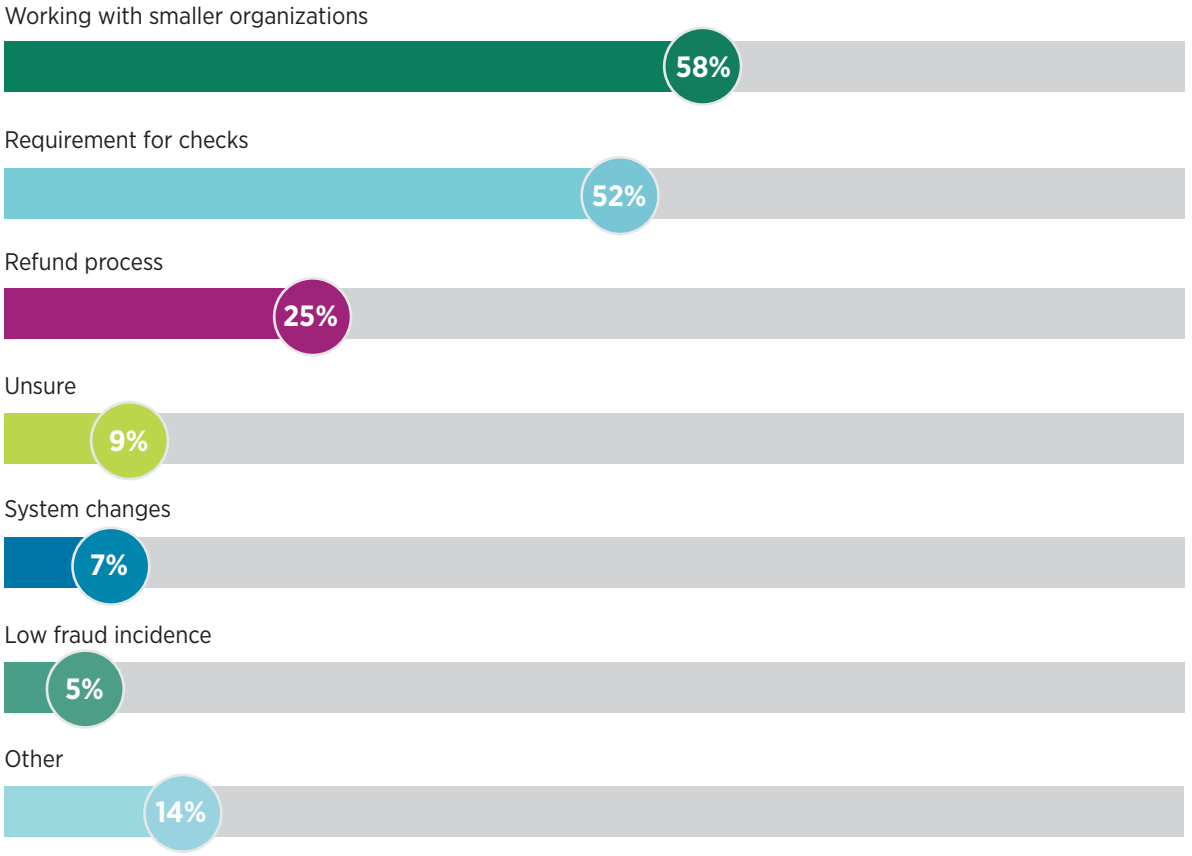


CHECKS CONTINUE TO BE A POPULAR METHOD OF PAYMENT AT ORGANIZATIONS CONTINUED

Despite the concerns about fraud and the burden of processing when it comes to check use, many organizations remain undeterred from discontinuing checks. The top three reasons preventing checks from being eliminated are:

- **Working with smaller organizations** (cited by 58% of respondents)
- **A requirement for checks in general** (52%)
- **Refund processing** (25%)

Reported Obstacles for the Elimination of Checks
(Percent of Organizations Not Planning to Eliminate Use of Checks)



Other includes:

- Lack of data or technology resources needed to send digital payments
- Institutional requirements/reluctance
- Senior management believes checks are safer
- Government requirements
- Claim payments
- Payee's preference for checks

CHECKS CONTINUE TO BE A POPULAR METHOD OF PAYMENT AT ORGANIZATIONS CONTINUED

Disbursing Checks

Organizations disburse checks through various methods including the U.S. Postal Service (USPS), courier services, in-person distribution and digital check solutions. Seventy-five percent of organizations continue to send checks via U.S. mail without including tracking information.

However, there is a real and continued risk for mail theft-related check fraud. In the six months following the February 2023 alert on mail theft-related fraud by FinCEN, over 15,000 Bank Secrecy Act (BSA) reports were filed by 841 financial institutions amounting to more than $688 million.[17] Fraudsters typically initiate one of three primary actions taken after checks are stolen: checks are altered then deposited, checks are used as templates to create counterfeit checks, or checks are fraudulently signed and deposited.[18]

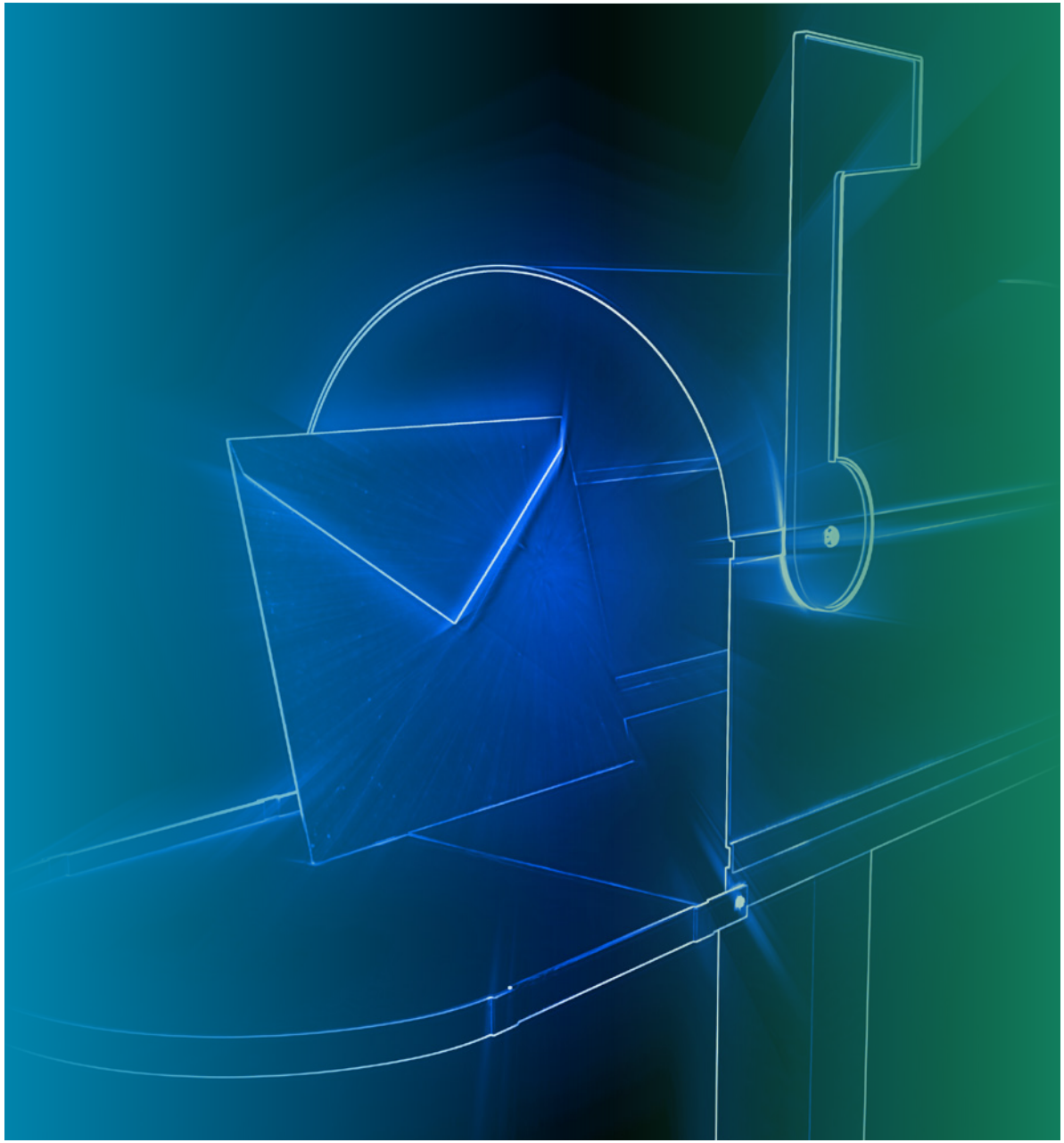
To provide additional security, 41% of organizations utilize a commercial carrier such as FedEx®, UPS®, DHL®, etc., while 23% take advantage of USPS tracking services.

[17]FinCEN Issues In-Depth Analysis of Check Fraud Related to Mail Theft, September 9, 2024, Financial Crimes Enforcement Network
[18]Ibid.

Methods for Disbursing Checks
(Percent of Organizations Using Checks)

USPS general mail (without tracking)	75%
Commercial carrier (FedEx®, UPS®, DHL®, etc.)	41%
USPS with tracking	23%
Hand/courier delivery	16%
eCheck	13%
Other	5%

Other includes: Bank/third party prints and sends checks



CHECK FRAUD CONTROLS

Due to the extensive use of checks at organizations (as noted earlier), check fraud remains a persistent threat to businesses, financial institutions and individuals. Effective controls are critical to mitigating payments fraud risk, ensuring financial security and maintaining trust in payment systems. Organizations must focus on implementing robust measures to detect and prevent fraudulent activities. With a vast majority of organizations using checks to some extent, safeguarding against check fraud is a critical issue for treasury professionals. Treasury practitioners are very aware of the vulnerability of checks to fraud, and their organizations have identified controls that provide strong protection against check fraud. Ninety-three percent of respondents report that their organizations have implemented positive pay to curb check fraud. At least 85% utilize the following controls to mitigate fraud:

- **Daily reconciliation and other internal processes** (cited by 90% of respondents)
- **Segregation of accounts by function for single purpose** (86%)
- **Payee positive pay** (85%)

Overall, survey respondents are extremely satisfied with payee positive pay and positive pay, with 97% and 96%, respectively, indicating these services are effective or very effective in mitigating check fraud. Two additional controls — the "post no checks" restriction on depository accounts and reverse positive pay are each cited to be effective or very effective in mitigating check fraud by 91% of respondents.

Some instances, such as forged endorsements and other alterations, force organizations to follow up with their banks to file affidavits. These cases create an administrative burden and require manual processing. Organizations are turning to third-party solutions to assist with check fraud prevention and detection, including secure check printing and issuance, check verification and software enhancement/improved automation.

Because of their effectiveness, a majority of organizations has implemented most of these procedures. There are still some gaps between effectiveness and implementation. For example, 91% of organizations consider reverse positive pay to be an effective check control; however, just 52% have implemented it. Reverse positive pay, according to AFP's *Essentials of Treasury, 7th Edition*,[19] is a process whereby a bank transmits a file of the checks presented for payment to a company on a daily or intraday basis. Within a specified deadline, the company matches this file to a list of checks issued and notifies the bank of any items to be returned.

Reverse positive pay is a more burdensome process than positive pay and does not include checks cashed/deposited at bank branches since the bank does not have access to the check issuance file. In traditional positive pay, a check issuance file is sent to the bank, the bank matches those checks for payment against the file, and exceptions are reviewed by the company and actioned. In payee positive pay, the payee line of the check is incorporated into the check issuance file, and any alterations that don't match become exceptions to action. Organizations who still pay by check must understand the nuances of positive pay, payee positive pay and reverse positive pay, and determine which solution is best for helping them mitigate fraud.

[19] *AFP® Essentials of Treasury Management 7th. Edition, CTP Body of Knowledge, 2023*

Effectiveness of Fraud Control Procedures and Services Used to Protect Against Check Fraud
(Percent of Organizations Using Checks)

	IMPLEMENTED	VERY EFFECTIVE	EFFECTIVE	SOMEWHAT EFFECTIVE	NOT VERY EFFECTIVE	VERY INEFFECTIVE
Positive pay	**93%**	73%	23%	4%	--	--
Daily reconciliation and other internal processes	**90%**	50%	37%	11%	1%	1%
Segregation of accounts by function for single purpose	**86%**	45%	39%	13%	2%	1%
Payee positive pay	**85%**	76%	21%	2%	1%	--
Tamper resistant features on checks	**83%**	33%	32%	24%	8%	3%
"Post no checks" restriction on depository accounts	**73%**	66%	25%	7%	1%	1%
Reverse positive pay	**52%**	60%	31%	9%	--	--
Non-bank fraud control services	**47%**	37%	36%	23%	3%	1%

ACH DEBIT FRAUD AND CONTROLS

ACH Debit Usage

Eighty-eight percent of organizations use ACH debits. As the preferred payment method of choice, ACH debits are reliable and more efficient compared to paper checks, as they are digital and automated.

Still, organizations must still be vigilant against payments fraud via ACH debits. Even though more than a third of organizations (38%) experienced attempted or actual fraud via ACH debits in 2024 (a five-percentage-point increase compared to 2023), ACH debits continue to be a payment method of choice.

An area of payments fraud vulnerability via ACH debits is through BEC. ACH debits are the third most targeted payment type after wire transfers and ACH credits (tied for third place with checks) for fraud. Twenty-six percent of all organizations report that BEC targeted ACH debits in 2024. For those organizations with annual revenue of at least $1 billion, this figure is slightly lower — 23% — and the figure drops further to 18% for organizations with annual revenue of at least $1 billion and fewer than 26 payments accounts.

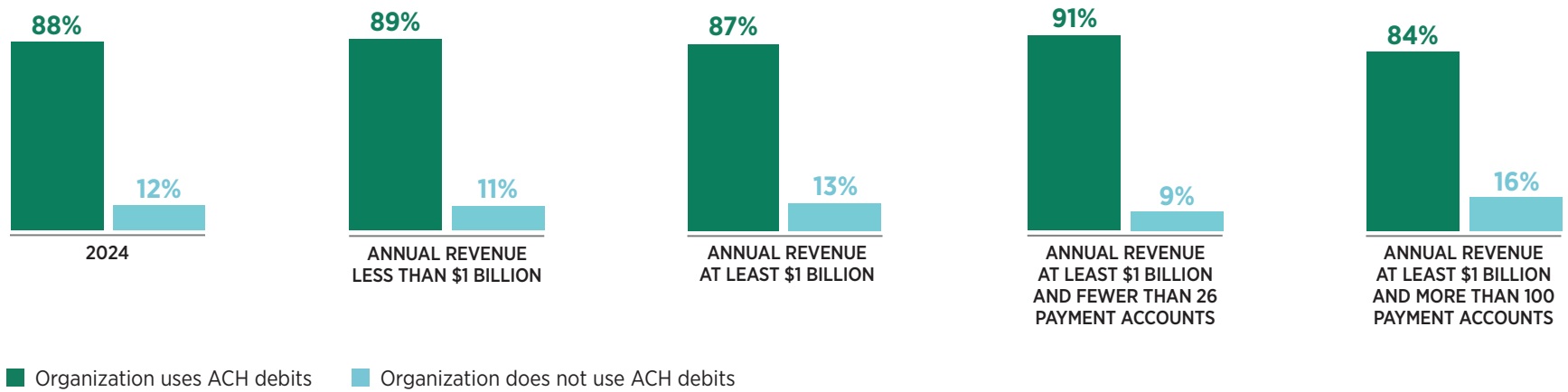
Financial professionals need to understand how fraudulent ACH debits might occur. A fraudster obtains a company check through mail theft or other means, takes the MICR information from the check and issues an ACH debit using the routing and account number. Fraudsters can also gain access to bank information from an organization's invoice. ACH debits are issued in small amounts first, then those amounts gradually get larger as fraudsters see what they can get away with. Once the fraud is discovered by the organization, any compromised account should be quickly closed.

Understanding the ACH rules around return windows is also essential for knowing the process for making returns. According to Nacha, the return deadline for an ACH debit to a business or commercial account is two days.[20] If a fraudulent debit is found after that two-day return deadline, the receiving organization would need its bank to request permission from the originating bank for a late return. If an originator realizes that it has fallen victim to a BEC scam, it must quickly notify the receiving bank so that the funds can hopefully be held and returned. ACH payments sent to consumer-based accounts have a 60-day return window, so there is considerably more time for originators and consumers to catch suspicious transactions.

Organizations need to know that debits are fully authorized and have the proper debit filters and blocks in place. A daily reconciliation of activity can verify that all transactions are accounted for and deemed legitimate. When issuing ACH debits, a digital or paper trail follows the activity that can be quickly validated should a return be submitted by the receiving party.

[20] https://www.nacha.org/rules/reversals-and-enforcement

ACH Debit Usage
(Percentage Distribution of Organizations)



ACH DEBIT FRAUD AND CONTROLS CONTINUED

Effectiveness of ACH Controls

There are a number of effective controls available to organizations to assist them in minimizing payments fraud via ACH debits.

Blocking all ACH debits except on designated accounts set up with an ACH debit filter is the control most often implemented by organizations (92%). It is also the one most-often cited as "very effective" (by 75% of organizations). Treasury practitioners rely on the following ACH fraud mitigation strategies as well, with a majority reporting the measures as "very effective:"

- **Block ACH debits on all accounts** (cited by 68% of respondents)
- **Debit block on all consumer items with debit filter on commercial ACH debits** (65%)
- **Reconcile accounts daily to identify and return unauthorized ACH debits** (58%)

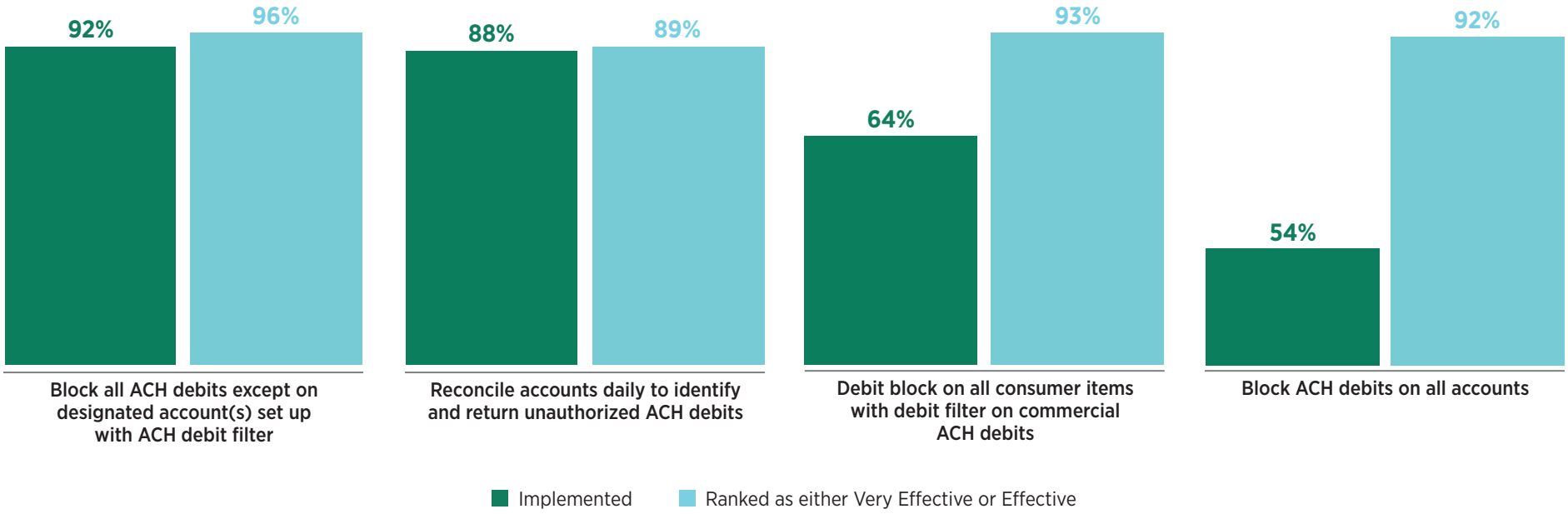
Effectiveness of Controls in Mitigating ACH Debit Fraud
(Percent of Organizations)

	IMPLEMENTED	VERY EFFECTIVE	EFFECTIVE	SOMEWHAT EFFECTIVE	NOT VERY EFFECTIVE	VERY INEFFECTIVE
Block all ACH debits except on designated account(s) set up with ACH debit filter	**92%**	75%	21%	3%	1%	--
Reconcile accounts daily to identify and return unauthorized ACH debits	**88%**	58%	31%	10%	1%	--
Debit block on all consumer items with debit filter on commercial ACH debits	**64%**	65%	28%	6%	1%	--
Block ACH debits on all accounts	**54%**	68%	24%	6%	2%	--

ACH DEBIT FRAUD AND CONTROLS CONTINUED

When the responses indicating that the controls are "very effective" or "effective" are combined, the controls featured in the survey are those that provide the expected protections. As with check controls, survey results reveal a gap between the "effectiveness" rating and the "level of implementation." For example, blocking ACH debits on all accounts is implemented by 54% of responding organizations, while 92% of respondents rank this control as either "very effective" or "effective."

Most Effective Controls in Mitigating ACH Debit Fraud
(Percent of Organizations)



MEASURES TO IMPROVE CONTROLS

MEASURES TAKEN IN 2024 TO IMPROVE CONTROLS

Reduced Check Disbursement

- Eliminated checks
- Reduced manual check disbursements
- Reduced the number of checks dispersed
- Removal of "auto pay" features for utilities services and turning to a company-originated online payment option; continuous reduction of physical checks issued and utilization of an online pay feature for tax payments to federal/state/local municipalities.
- Reduced check issuance to avoid fraud associated with that method of payment

Increased Education and Training

- Monthly fraud trainings; increasing banking validation processes
- Better training for staff and holding staff accountable that do not follow procedures; added more targeted training with the groups that handle payments; detected fraud emails are being shared with departments as lessons learned, process worked.
- Additional reviews; additional email phishing training; lengthier processes for new vendors
- Continued BEC training, continued efforts to move vendors to ACH and using a system where vendors manage payment accounts
- Continued education of AP and purchasing/sourcing teams on the importance of separately confirming vendor bank changes with known contacts
- Continued phishing tests/training, implementing payee positive pay (instead of regular positive pay) on a few remaining accounts
- Performed random email fraud testing to all employees; encouraged the use of phishing alert report in outlook to report any suspicious emails
- Initiated a focused training program on all aspects of fraudulent email/hacking activities in the workplace
- Added more training on BEC fraud and strengthened multifactor authentication for banking and vendor portals
- Increased training and investigated third-party account verification services
- Trained employees; moved corporate credit cards under treasury to impose standard controls on processes
- Primarily education and emphasis on vendor callbacks to validate banking or any other changes
- Improved controls due to the fact we had employees take training sessions; in 2025 we plan to do the same
- Widened education for employees, as well as implemented tighter controls on cybersecurity measures and technology to improve controls
- Offered and conducted training and lectures on fraud prevention
- Ongoing payments fraud control training; no more checks for payments, only exceptions
- Lots of training; improved faster fraud detection
- Reeducated staff on current fraud schemes and reemphasized the importance of always doing a call-back
- Training and policy implementation were the main changes made in 2024; training, training, training, as well as documentation of policies and processes
- Revisited schedule of authority and provided reinforced mandatory training to all team members
- Significantly more employee training and education to be alert to fraud and scams; continuous payment control improvements and policy strengthening
- Periodic phishing email tests with our employees to see if they recognize the phishing attempt; Implemented MFA for everyone accessing our network

Added Callbacks/Verification

- Callback verification and more auditing
- Callback on new vendor bank details when received via email instructions
- Initiated verbal verification for any payment information changes
- Payee name verification
- Use of an account verification system to validate account information when setting up ACH payments to vendors
- Verification of known vendor individuals when a change to wire instructions is received. Increased awareness of fraudulent schemes and ways to prevent them
- Verification of payment instructions via phone with a known contact
- Authorizations for wires must be wet signatures; calls to signers done to known numbers before payments are actually sent; no electronic verifications allowed
- Centralizing the vendor-related verification controls under one department; improved employee training
- Bank information collection for new vendors and changes done through DocuSign with two-factor authentication; if this is not possible, a verbal verification is performed; keeping a log of all new vendors with how banking was verified (who, position, contact information)
- More of an understanding by our business partners as to why we do callbacks on payment information — even for new vendors
- Payments are issued by template use only; if a vendor changes its account, we do a voice call to verify with our contact person

MEASURES TAKEN IN 2024 TO IMPROVE CONTROLS

Third-Party Support

- Exploring third-party account ownership validation service (currently there's no foolproof solution and they only provide limited coverage even for domestic accounts; not sure if this is a valuable service to procure
- Brought in a third party to tighten security
- Implemented third-party software to review international banking instructions and implemented third-party AP disbursement. Would like to see the reduction of checks continue or payments sent to a third-party AP if they can't be moved to ACH
- Better third-party systems to verify banks with legit owners
- More involvement by law enforcement in preventing/investigating these types of fraudulent activity
- Moved to using a supplier portal to have the supplier enter their banking information 2024
- Moved to remote check print; our bank prints our checks remotely instead of using in-house check print
- Attempted to use a third party to manage beneficiary business and bank details but was not implemented well in 2024
- Independent audits by external auditors

Improved Fraud Detection

- Improved spam e-mail detection
- All vendor bank changes verified with known vendor contact, not number provided
- Changed check serial numbers to make fraud checks stand out further in a high-volume payroll account
- More digital security
- Software enhancement, training
- Two-factor authentication and fraud protection for apps like Cash App and Venmo
- Two-factor authentication request to change vendor banking information verified through a phone call to the vendor where they are asked to verify all banking information and data
- We licensed a 2FA vendor that performs automated screening on outgoing payments via an API integration with our TMS. This is meant to take the place of callbacks in ~75% of cases. We believe this is the direction the fraud prevention industry needs to move as AI/deep-fakes get better and better, threatening to make callbacks essentially useless in the coming years.
- We set dual controls on all payment systems. We set daily payment limits on bank accounts and daily limits for approvers. We meet regularly with our banks to ensure that our accounts have all available protections. We ensure that access is tightly controlled and granted for specific purposes. It is our goal to reduce manual payments including ACHs and wires.
- We split responsibilities within the AP department to limit individuals' need for access. We implemented a third-party account verification process to supplement our supplier portal and implemented required callbacks on any new/changed banking instructions tied to payments.
- Revamped our internal controls and cybersecurity technology segment of the business. Enhanced the depth and breadth of our internal audit and compliance team working in tandem with our AP/AR team to monitor and quickly detect financial payment and process fraud.
- We changed our approval process for invoices. We strengthened our IT policies to ensure people are not doing anything personal on work machines.
- In 2024, we migrated a majority of our vendors towards using services such as Paymode® and payables.
- Company controls: laptops are prevented from recognizing thumb drives; non-corporate email addresses are blocked by firewalls; employees are not able to send emails to non-corporate email addresses; firewalls are very secure and block many unsolicited emails from outside the company; controls over website accesses are implemented — some are not allowed; emails containing confidential attachments are typically sent encrypted; attachments are password protected; VPN in place
- Ran analysis on false positives to better service customers and improve system notifications. Improved positive pay services to better analyze checks with payee match verification
- Moving to integrated payables/virtual card payments
- Better assistance for our customers making payments to us, to allow them to submit authorization to make debits but have better validation tools for the customer on self-service sites. Almost 70% of our identified returns or NOCs are due to incorrect routing/account information on our customer self-service site.

Bank Support

- Adopted all bank compliance and fraud tools offered
- Employed our banking partner's online check issuing services, which reduced fraud from local mailboxes and provided estimates for receipt of payment timing.
- Evaluating bank account verification services
- Implemented a bank verification policy for new suppliers and bank change requests that require independent phone call verification; created an internal fraud escalation to respond to incidents
- We use our bank's early warning system for validating beneficiary bank information. A very high percentage of these come back as "unknown," which led us to just rely on our manual processes.
- We implemented payment out of a central bank for vendors that require a check.
- Reviewing for a bank that can provide risk scores back on bank instructions to identify potential higher risk transactions

MEASURES RESPONDENTS WOULD LIKE TO SEE IMPROVED OR CHANGED IN 2025

- [We] would like to implement more training for the treasury and AP team to heighten awareness; would also like to set up notifications so we don't miss positive pay or ACH filter deadlines. Our default is return so we won't experience fraud but most of the positive pay items end up being valid and if we miss the deadline, the item is returned and has to be resent.
- Would like to put additional BEC and fraud training in place for the company
- Would like to further automate treasury and AP workflows
- Would like to move to a third-party bank validation provider to ensure that bank account validations are performed consistently in accordance with corporate policy
- Greater use of technology to flag fraud early
- Would like to see less checks
- I personally think that disciplinary measures should be in place if an employee continually fails the phishing tests/training.
- We are going to provide more training globally for our personnel, send updated policies, etc.
- Components of fraud are always changing, so in 2025, I'd like to see our organization remain on top of training and documentation. If we can remain ahead, we can keep fraud at bay.
- Finish implementation of ACH change validation and a control method in which treasury receives PII on wire instructions
- Looking at ways to verify banking changes by vendors
- Would like to implement multifactor authentication in 2025
- We are implementing software across the company to help us mainstream our payments and also track and control them more closely.
- We are looking at third-party vendors to add additional vendor banking verifications and payment anomaly screening.
- Recommendation in 2025 to move risk to beneficiaries and have them manage their details in the payment system
- Reduce the number of checks being dispersed in 2025
- Would like to implement software tools to identify fraud and errors earlier
- Plan to implement targeted annual fraud training for payment processors in 2025
- Would like to see controls implemented by function; there may be some room for prevention of accessing fraudulent sites
- I would like to see the banks offer additional security controls for customers because it seems like the scams are becoming more and more frequent.
- Would like to see better banking solutions and support to prevent fraud
- Would like to see improved bank account validation
- In 2025, looking to implement a vendor portal onboarding process and elimination of check payments

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.

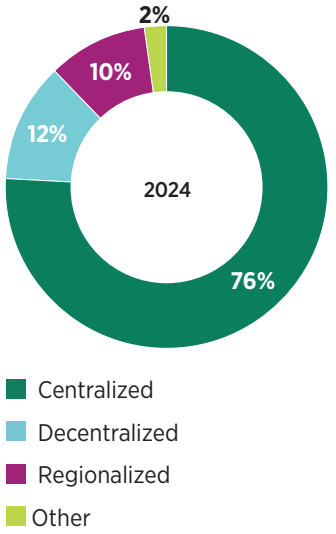
Type of Organization's Payment Transactions
(Percentage Distribution of Organizations)

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

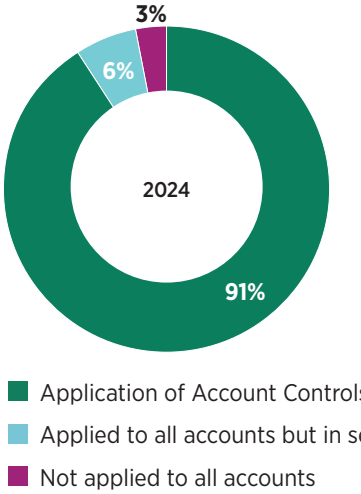
Number of Payment Accounts Maintained
(Percentage Distribution of Organizations)

	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

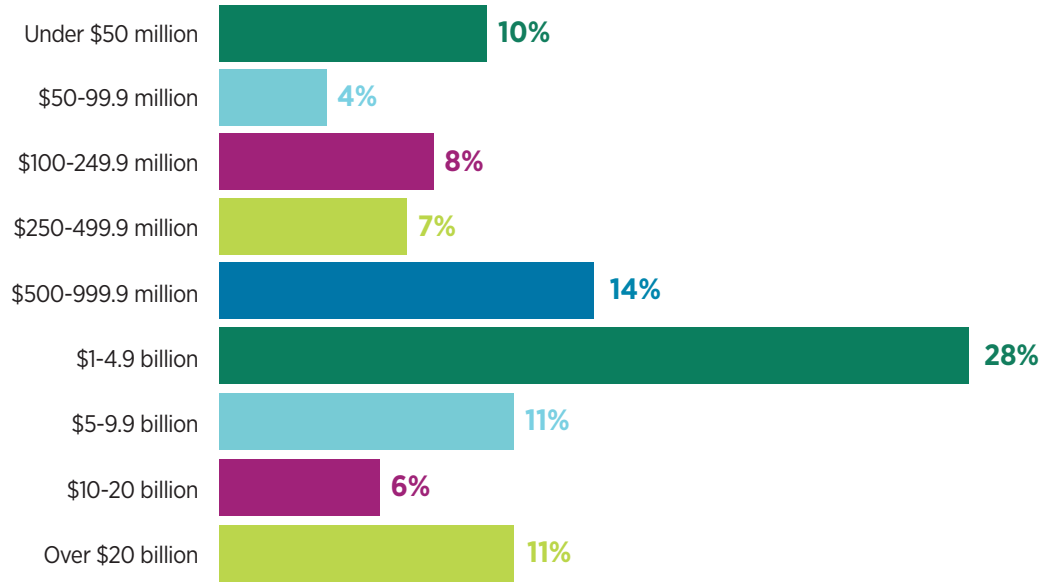


Application of Account Controls
(Percentage Distribution of Organizations)



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%

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

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

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.