ASSOCIATION FOR FINANCIAL PROFESSIONALS

2026 AFP®

PAYMENTS FRAUD AND CONTROL SURVEY REPORT

Comprehensive Report

Underwritten by TRUIST

TRUIST

What Persistent Payments Fraud Reveals: Insights from the 2026 AFP® Survey

Payments are moving faster. Fraud is keeping pace.

For the third consecutive year, Truist is proud to sponsor the **2026 AFP® Payments Fraud and Control Survey**—because preventing payments fraud is no longer a periodic project. It is a constant operational discipline, embedded in how payments are initiated, approved, monitored, and recovered.

This year's findings are clear:

- More than three quarters of organizations experienced attempted or actual payments fraud.
- Business email compromise remains the most common threat.
- Checks continue to be disproportionately impacted.
- And for many organizations, fraud still results in real financial loss.

For treasury leaders, this isn't abstract. It reflects the daily reality of balancing speed with certainty, automation with oversight, and efficiency with control. The survey reinforces the central role treasury teams play in detection, escalation, and recovery—often coordinating among various technology, risk, legal, and banking partners. Fraud prevention today is not a single control or system. It's an operating model.

From our vantage point working with organizations across industries and payment types, **one theme is consistent: outcomes improve when fundamentals are strong**. Clear verification, disciplined approvals, and timely detection form the backbone of effective fraud prevention—and they matter even more as fraud tactics grow more sophisticated, including early use of deepfake enabled impersonation.

Technology will continue to evolve. **Progress in fraud prevention, however, comes from judgment**—knowing when speed matters most, where controls must be firmest, and where innovation genuinely improves outcomes.

That's how we think about this moment at Truist—anchored in simplicity, speed, safety, and smart execution. Practical standards for payment environments that need to perform under real world conditions.

We're grateful to AFP and to the finance and treasury professionals who shared their experiences to inform this research. We hope this report helps you benchmark your approach, pressure test your assumptions, and make confident decisions about what to strengthen next.

Regards,

Chris Ward
Head of Enterprise Payments
Truist

CONTENTS

INTRODUCTION

Payments fraud refers to a range of deceptive tactics designed to obtain funds or sensitive financial information illegally from either businesses or individuals during payment transactions. It encompasses activities such as identity theft, phishing, email scams, card skimming, deceptive check practices and unauthorized electronic transfers. In recent years, artificial intelligence (AI) has contributed to the evolution of fraud by enabling more sophisticated tactics, including the use of voice and video technologies. As digital payment methods become more prevalent and the risk of payments fraud continues to grow, it is essential for organizations and consumers alike to implement robust fraud controls and security measures and remain vigilant against evolving threats.

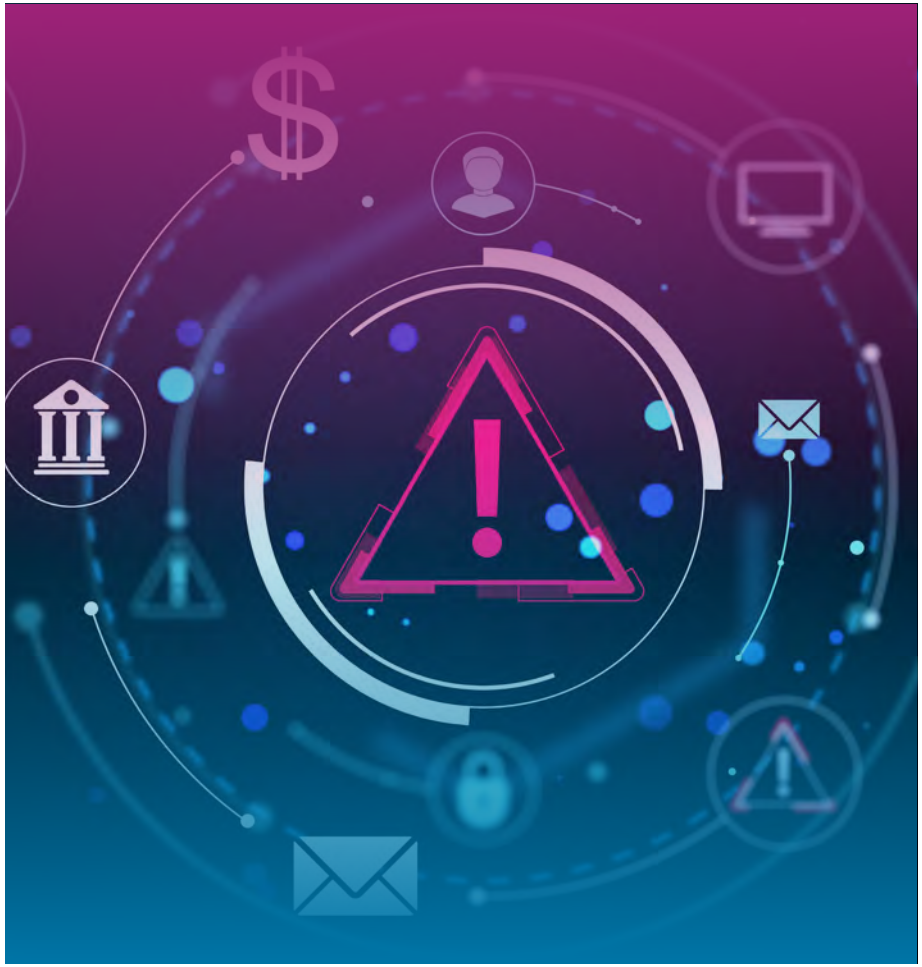
Businesses remain vulnerable to fraudulent activities, and those scams originating via email such as business email compromise (BEC) are widespread. Given the large volume of correspondence conducted via email, this channel is frequently exploited by fraudsters posing as vendors or employees to deceive personnel responsible for disbursements or those in client-facing roles.

Furthermore, organizations have not yet been able to fully eliminate their reliance on checks. Checks are still commonly used for payments, and check-related fraud persists at rates higher than that via other payment methods; In recent years, perpetrators have increasingly intercepted and altered checks, redirecting funds to fraudulent accounts. Additionally, although deepfake technology is not as pervasive, its emergence poses significant risks; manipulated audio and video can convincingly mimic authentic communications and undermine organizational security. While fraudsters may only need to succeed once, organizations must consistently maintain accuracy and vigilance, making fraud prevention a top priority for many institutions.

The severity of fraud attacks has been acknowledged by the White House, too. In January, the Trump administration announced the creation of the **Department of Justice's (DOJ) new division for national fraud enforcement**. This division will enforce criminal and civil laws targeting federally funded programs, federally funded benefits, nonprofits and private citizens.

Organizations have prioritized fraud controls and safeguards in efforts to prevent payments fraud, some of which have proven more effective than others. Along with highlighting recent trends and the effects of payments fraud, this report discusses the strategies organizations use to fight fraud through email, checks and ACH, and evaluates how effective each method is.

Since 2005, the Association for Financial Professionals® (AFP) has run its *Payments Fraud and Control Survey* annually. Continuing this tradition, AFP® conducted the 22nd *Annual Payments Fraud and Control Survey* in January 2026. The survey investigates the types and scope of fraud targeting business-to-business (B2B) payments, explores which payment methods are affected, highlights how business email is increasingly used in fraud, and reviews how organizations are protecting themselves from these threats. The study also examines the prevalence of deepfake technology within organizations and assesses its impact. This year, 465 corporate professionals from a wide variety of industries and company sizes participated. The report presents data for 2025, with a breakdown of respondent demographics provided at the end.



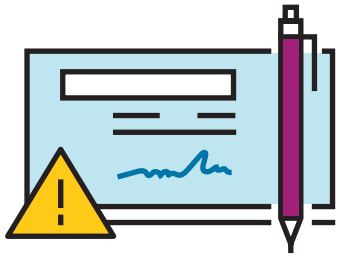
AFP® thanks Truist® for its underwriting support of the *2026 AFP® Payments Fraud and Control Survey*. Both questionnaire design and the final report, along with its content and conclusions, are the sole responsibilities of AFP's Research Department.

KEY FINDINGS

Adoption of AI for fraud prevention remains limited, despite recognized benefits

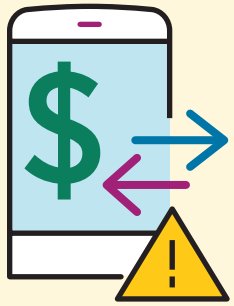
Few organizations (17%) report using AI to combat payments fraud. While adoption is higher among large organizations – i.e., those with annual revenue of at least $1 billion – most respondents cite immaturity of technology, cost and reliance on existing controls or banking partners as reasons for limited use, despite reported benefits such as improved detection and efficiency.

Checks continue to be the payment method most frequently impacted by fraud



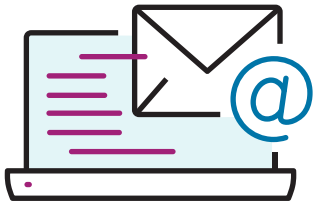
Despite declining fraud activity via their use, checks continue to be the most-often targeted method for fraud, reported by 58% of organizations in 2025 – outpacing fraud via ACH debits (30%) and wire transfers (25%). Check usage continues to be widespread; 68% of companies use checks for vendor payments because vendors require payment via checks. That is a 16% increase from 2024. Nearly three-quarters (72%) of organizations plan to continue using checks for the foreseeable future.

Payments fraud remains widespread; over three-quarters of surveyed organizations experienced either attempted or actual fraud attacks in 2025



Payments fraud remains widespread; over three-quarters of surveyed organizations experienced either attempted or actual fraud attacks in 2025

Business email compromise (BEC) is the most prevalent fraud vector



BEC affected 74% of organizations in 2025, representing a significant increase from 2023 and 2024. Fraudsters primarily impersonate vendors or executives to request changes to payment instructions, making email the dominant channel for payments fraud regardless of organization size. Additionally, 39% of organizations continue to receive genuine emails that have been intercepted by fraudsters.

Treasury plays a central role in payments fraud detection, reporting and recovery

Treasury is most frequently cited as the business unit discovering both attempted fraud (83%) and actual fraud (55%), underscoring its critical risk management role in monitoring bank activity, managing controls and coordinating recovery efforts – often in close collaboration with Accounts Payable and banking/vendor partners.

Payments fraud impacts U.S. businesses of all revenue categories with varying consequences

Nearly half of organizations (48%) with annual revenue less than $1 billion that experienced payments fraud in 2025 incurred a loss, and 24% of these companies were unsuccessful in recouping any funds lost. Two-thirds (66%) of larger organizations with annual revenue of at least $1 billion faced a financial loss due to fraud, and 19% were unable to recoup funds lost.

Smaller organizations experience payments fraud less frequently, but when fraud succeeds, they are far more likely to absorb the full financial loss. While larger organizations face more frequent attacks, they recover those losses more effectively due to stronger detection, escalation and recovery infrastructure.

PAYMENTS FRAUD OVERVIEW

PAYMENTS FRAUD TRENDS

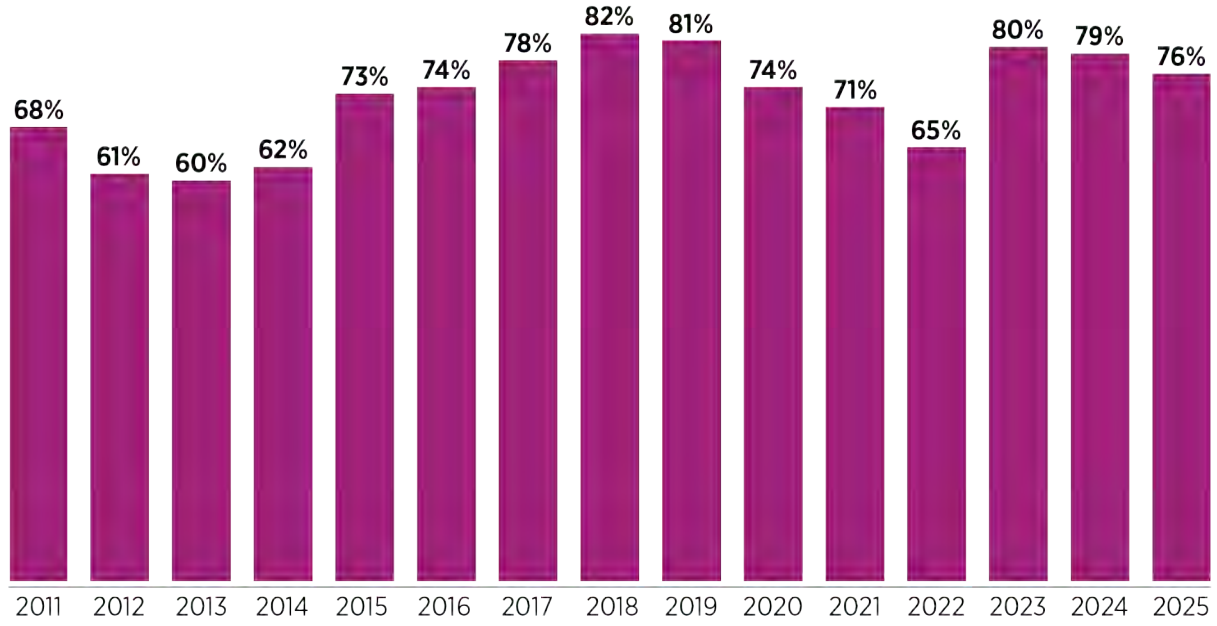
Payments Fraud Attacks on Organizations Continue to Be Elevated

Despite ongoing investments in controls and prevention, payments fraud remains widespread and persistent. Seventy-six percent of organizations report that they experienced actual or attempted payments fraud activity in 2025 – continuing the slight downward trend noted in 2024 but still well above pre-2023 levels.

Larger organizations – defined as those with annual revenue of at least $1 billion – report higher exposure to payments fraud; 81% experienced an attack compared with 67% of organizations with less than $1 billion in annual revenue. Organizations with annual revenue of at least $1 billion and fewer than 26 payment accounts experienced more payments fraud than did those organizations with annual revenue of at least $1 billion and more than 100 payment accounts (83% versus 74%).

A scammer took over the email box of one of our key vendors and started to send fake invoices to our operations; those bogus invoices were processed in the normal way with all approval steps. At the same time, the fraudster requested bank account information be changed which was entered into the system before Treasury could confirm the same.

Prevalence of Attempted/Actual Payments Fraud, 2011-2025
(Percent of Organizations)



Prevalence of Attempted/Actual Payments Fraud in 2025
(Percent of Organizations)

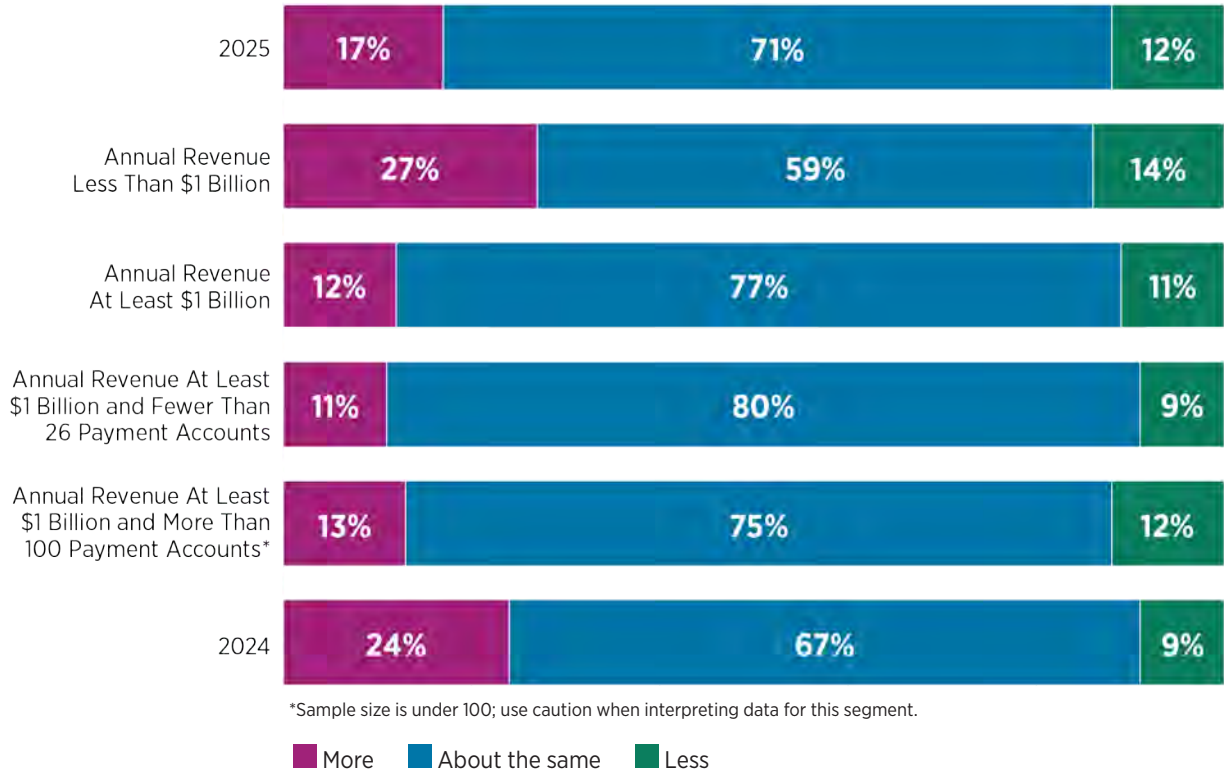
*Sample size is under 100; use caution when interpreting data for this segment.

More Organizations Report Similar Year-over-Year Incidence

More than 7 out of 10 (71%) organizations report that the incidence of payments fraud in 2025 was about the same as in the previous year; 17% indicate that there was more fraud and 12% indicate there was less. Compared with 2024, the share reporting an increase in fraud declined (from 24% to 17%), alongside a modest rise in reports of similar rates (67% to 71%) and a slight uptick in declines (9% to 12%). Results vary by organization size: respondents from organizations with annual revenue less than $1 billion are more likely to report increased fraud (27%) than are those from companies with annual revenue of at least $1 billion (12%).

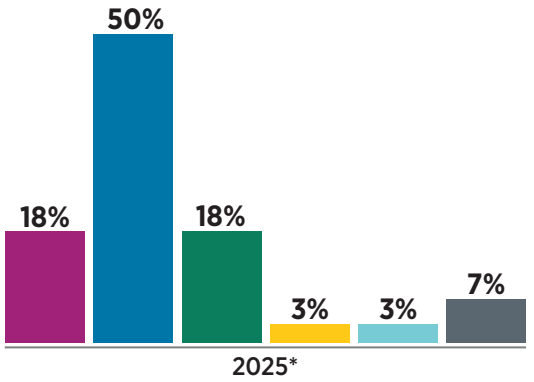
For the 17% of organizations experiencing an increase in payments fraud activity from 2024-2025, the increases are usually moderate: 50% of respondents report a *10%–25% increase,* 18% report *increases of less than 10%* and 18% report an *increase in fraud of 26%–50%.* Larger increases remained uncommon, with just 3% of respondents reporting a *51%–75% increase* and another 3% of respondents reporting an *increase of more than 75%.* The 7-percentage-point decline in the share of respondents selecting *Unsure* suggests organizations have a greater ability to estimate the incidence of payments fraud.

Change in Incidence of Payments Fraud in 2025
(Percentage Distribution of Organizations Experiencing Payments Fraud)



*Sample size is under 100; use caution when interpreting data for this segment.

Increase in Payments Fraud Compared to Previous Year
(Percentage Distribution of Organizations Reporting More Payments Fraud Attempts in 2025 than in 2024)



*Sample size is under 100; use caution when interpreting data for this segment.

PAYMENT METHODS IMPACTED BY FRAUD

Checks and ACH Debits Remain Most Susceptible to Payments Fraud

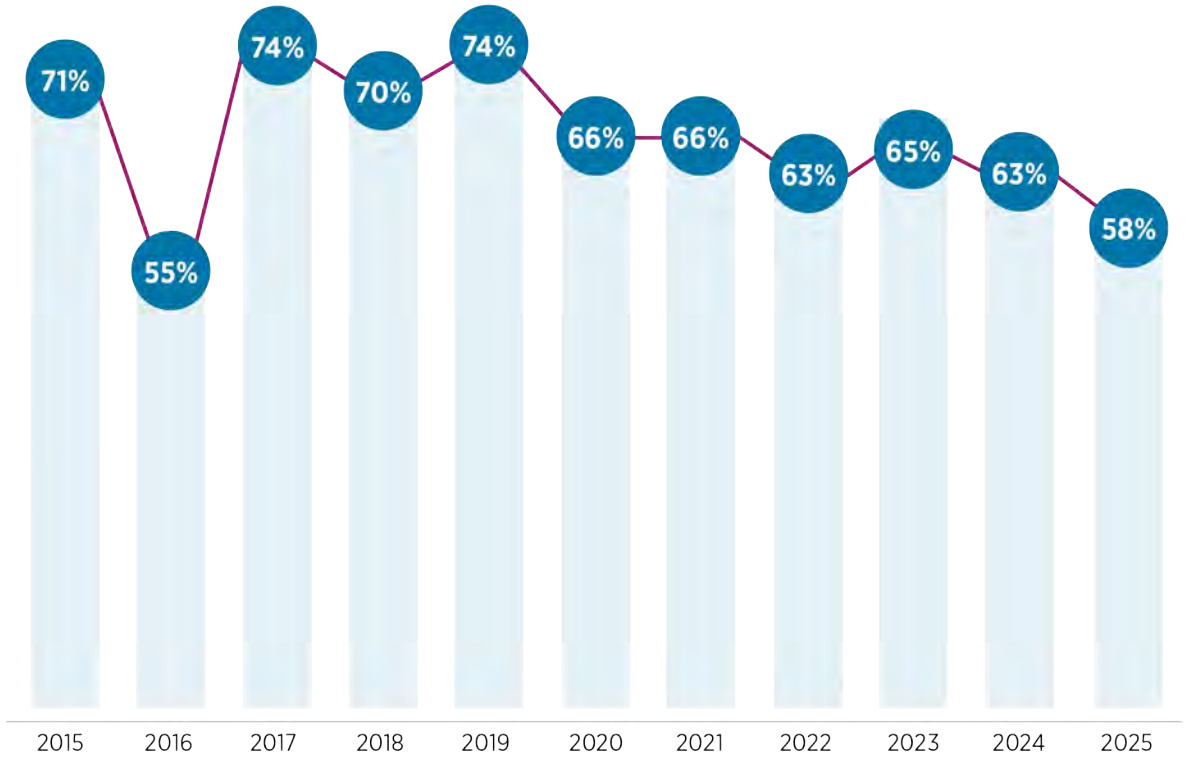
In 2025, checks and ACH debits remained the payment methods most impacted by fraud activity. Checks were the most frequently reported payment method subject to fraud (58% of organizations), followed by ACH debits (30%) and wire transfers (25%). Corporate/commercial credit cards (21%) and ACH credits (18%) accounted for a secondary tier of exposure, while newer or less widely used methods such as faster payments (1%), cryptocurrency (1%), and mobile wallets (2%) were cited less often.

Differences in fraud exposure are seen when considering organizational revenue. Organizations with annual revenue of at least $1 billion experienced a higher incidence of fraud for all payments methods (except for virtual cards) than organizations with annual revenue less than $1 billion.

Fraud involving ACH debits (reported by 30% of organizations) and wire transfers (25%) declined year-over-year, Wire transfers continued to be disproportionately targeted at larger organizations, particularly those with more than 100 payment accounts. Lower value and emerging payment methods – such as corporate cards, virtual cards, mobile wallets, and cash – remained comparatively infrequent targets.

The 10-year trend shows an overall decline in check fraud activity. Over the past decade, payments fraud via checks has trended downward, albeit with some bumps along the way. The decline observed in recent years is likely due to a reduction in the number of checks issued, as organizations increasingly adopt digital payment methods. Still widespread, the use of checks continues to represent the primary area of fraud vulnerability for organizations; this year's survey results reveal that over 87% of organizations use checks. Even as fraudsters adopt new technologies, the continued use of paper checks sustains long-standing fraud schemes. Mail-theft-enabled check fraud is a large persistent problem (see the side bar on this topic in the Checks and ACH section on page 35).

Check Fraud Activity: Trends
(Percent of Organizations)



PAYMENT METHODS IMPACTED BY FRAUD CONTINUED

According to the National Automated Clearing House Association (Nacha, which governs the ACH Network), **total ACH payment volume rose 4.9%** to 35.19 billion transactions in 2025, equivalent to a value of $93 trillion. Despite the continued growth of ACH payment volume, survey respondents report lower levels of payments fraud via both ACH debt and ACH credit compared to 2024. ACH debit fraud in 2025 was down 8 percentage points (30%) from the previous year, while ACH credit fraud was down two percentage points (18%). These declines are likely because organizations are more effective at detecting ACH fraud, and they probably offer more focused training and education to reduce the risk.

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

	2025	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*	2024
Checks	58%	46%	65%	67%	56%	63%
ACH debits	30%	28%	32%	31%	33%	38%
Wire transfers	25%	21%	27%	25%	36%	30%
Corporate/commercial credit cards (e.g., purchasing, T&E, fleet)	21%	20%	22%	21%	21%	21%
ACH credits	18%	13%	22%	25%	10%	20%
Cash	5%	4%	5%	6%	4%	5%
Virtual cards	3%	3%	3%	2%	4%	5%
Mobile wallets (Venmo®, PayPal®, etc.)	2%	2%	3%	3%	3%	3%
Faster payments (RTP®, FedNow®, etc.)	1%	--	2%	1%	7%	2%
Cryptocurrency (Bitcoin, Ethereum®, etc.)	1%	1%	1%	2%	1%	1%

*Sample size is under 100; use caution when interpreting data for this segment.

PAYMENT METHODS IMPACTED BY FRAUD CONTINUED

Validation of Beneficiary Payment Information

Beneficiary payment account validation is the process of verifying a payment recipient's account details before a payment is executed to reduce the risk of fraud as well as mitigate transaction errors. Of those organizations that experienced payments fraud during 2025 via ACH credits or ACH debits, 63% continue to validate payment details manually, 18% use an external service to validate payment information, and 8% rely on a financial vendor/bank for validation.

Organizations That Validate Beneficiary Payment Information

(Percentage Distribution of Organizations Experiencing Attempted/Actual ACH Credit or ACH Debit Fraud)

	2025	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*
Organization validates payment details manually	63%	67%	60%	61%	64%
Organization uses an external service to validate payment information	18%	14%	21%	20%	24%
Organization relies on financial vendor/bank to do so	8%	11%	7%	6%	8%
Organization does not validate beneficiary payment information	3%	5%	3%	4%	--
Other	8%	5%	9%	9%	4%

*Sample size is under 100; use caution when interpreting data for this segment.

Other includes:

- Hybrid verification models combining external validation technology with manual checks
- Validation approach differs by payment type (e.g., domestic vs. international)
- Adding security enhancements to the validation workflow

LOSSES INCURRED DUE TO PAYMENTS FRAUD ATTACKS/ATTEMPTS

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

Financial loss remains the most severe outcome of payments fraud. Sixty percent of organizations that experienced payments fraud in 2025 report having incurred a dollar loss, reflecting continued fraud risk exposure among survey respondents. Losses were concentrated in the small to mid ranges, with the share of organizations reporting losses between up to $24,999 and $100,000–$249,999 rising from 42% in 2024 to 51% in 2025. A higher percentage of organizations with annual revenue less than $1 billion report they did not incur a loss compared to those companies with annual revenue of at least $1 billion (52% versus 34%).

Estimated Total Dollar Loss to Organization from Payments Fraud
(Percentage Distribution of Organizations Experiencing Payments Fraud)

	2025	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*	2024
No loss	40%	52%	34%	36%	29%	46%
Up to $24,999	24%	21%	26%	29%	20%	21%
$25,000-$49,999	11%	11%	10%	11%	12%	7%
$50,000-$99,999	9%	6%	10%	8%	18%	8%
$100,000-$249,999	7%	3%	10%	8%	10%	6%
$250,000 - $499,999	3%	2%	4%	5%	4%	4%
$500,000 - $999,999	2%	2%	2%	2%	0%	3%
$1,000,000 - $1,999,999	1%	1%	2%	1%	2%	3%
At Least $2 Million	2%	2%	2%	1%	6%	2%

*Sample size is under 100; use caution when interpreting data for this segment.

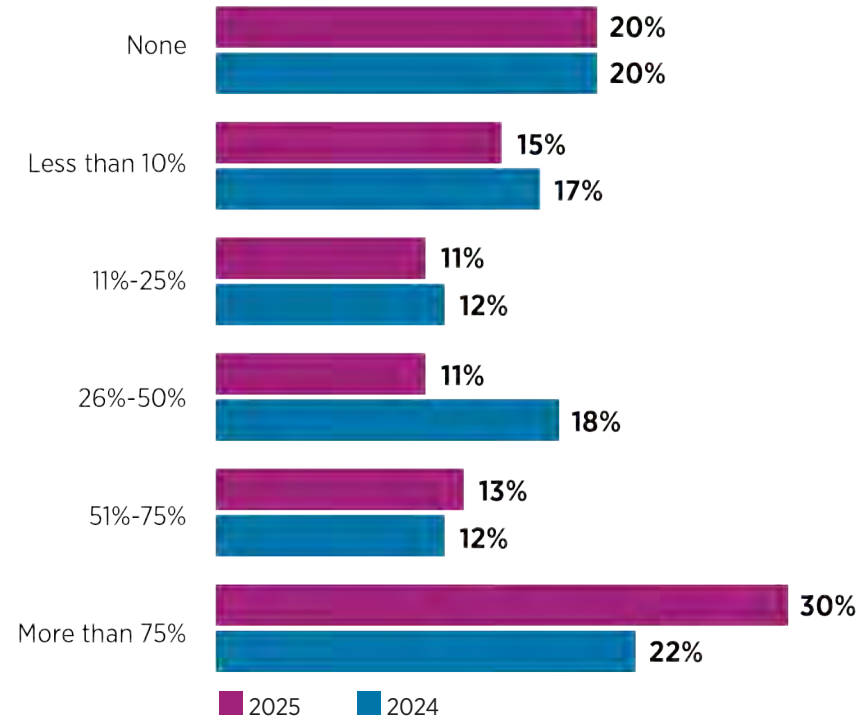
RECOVERING LOST FUNDS

Nearly One-third of Organizations Recovers More Than 75% of Lost Funds

Recovery outcomes among organizations experiencing payments fraud are mixed. While the largest share of organizations which experienced payments fraud in 2025 report recovering more than 75% of lost funds (30%), 20% report recovering none. The remaining 50% report partial recovery, underscoring a persistent recovery gap. Smaller organizations (those with annual revenue less than $1 billion) were more likely than larger ones to report very low recovery rates, with 24% recovering none and 24% recovering less than 10%. Among organizations with annual revenue of at least $1 billion, 19% report recovering none of lost funds and 12% indicate they recovered less than 10% of lost funds.

For every 100 attempts by a fraudster, 20 are successful; and some companies are unable to recover targeted funds. Organizations with annual revenue less than $1 billion are especially vulnerable since they lack more sophisticated payments fraud controls and so are more likely to be unsuccessful in recovering funds lost.

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



Someone posing as a client had been emailing our Sales and AP teams, and provided updated banking details. AP called the number on the email to confirm the banking details. The system did not update the banking details correctly, so we ended up paying the correct account. The fraudster reached out again and demanded payment. We sent the payment via wire, but the funds were returned because the fraudulent account was not set up to accept wire payments. At that point, we spoke with the actual client and confirmed it was fraud. No funds were lost, but a lot of lessons were learned.

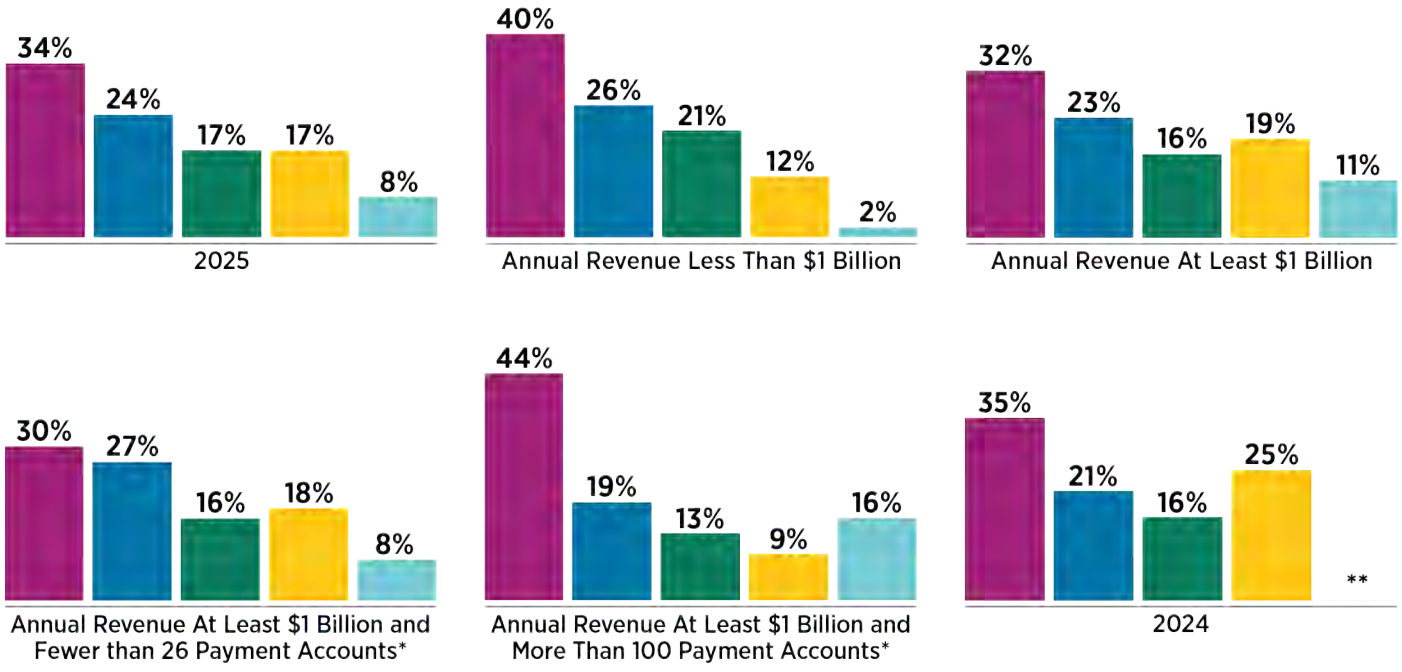
DETECTING FRAUD ACTIVITY

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

Among organizations that experienced actual losses due to payments fraud in 2025, most organizations detected the fraud within one month: 34% discovered the fraud in less than one week, 24% did so within 1–2 weeks and 17% within 3–4 weeks. Compared with 2024, the share of companies that took one month or more to uncover fraud declined from 25% to 17%, suggesting improvement in the detection process. 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. The longer it takes to identify fraud, the greater the possibility that the impact from the fraud could be detrimental. 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. Organizations that take longer to identify fraud may benefit from strengthening monitoring capabilities and reinforcing awareness among employees involved in payment processing, treasury and reconciliation activities. Artificial intelligence has the potential to enhance anomaly detection, particularly with micro transactions that may be used by fraudsters to verify active accounts. The forthcoming Nacha rules, which are discussed later in this report (see page 43), will outline how these measures will support both ACH processes and preventive fraud initiatives.

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



*Sample size is under 100; use caution when interpreting data for this segment. **Not an option for 2024

Other includes:

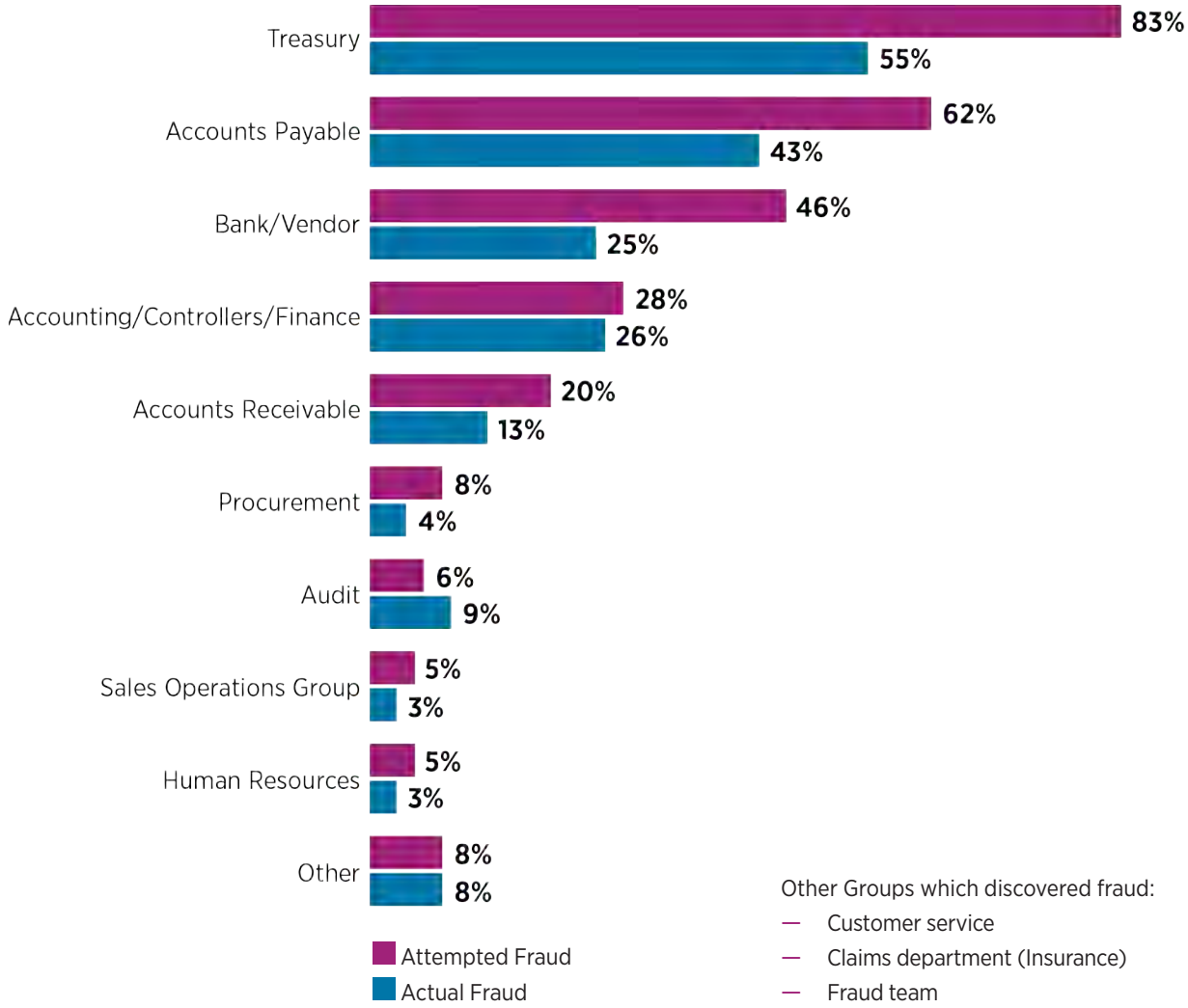
- Fraud detection time varies by fraud type. Discovery timeline is shorter for electronic payments and longer for check fraud
- Fraud is caught through routine operational controls (e.g., AP/payroll reconciliation, bank reporting, system flags)
- Vendor or customer notification triggers fraud discovery

Treasury Leads Payments Fraud Detection

Among organizations experiencing payments fraud, Treasury is most frequently cited as the department that discovers both attempted (83%) and actual (55%) fraud, followed by Accounts Payable (AP) at 62% and 43%, respectively. Banks and vendors also play a meaningful role, particularly in identifying attempted fraud (46%), while Accounting/Finance, Accounts Receivable, Audit, Procurement and other operational teams contribute to detection at lower levels.

The prominence of Treasury and AP in detecting payments fraud reflects their central role in initiating, releasing and monitoring payments. Treasury's regular review of bank account activity positions it to identify anomalies quickly, while AP's oversight of company liabilities, vendor payments and card activity supports earlier detection of irregularities. Effective fraud detection is strengthened when Treasury and AP operate in close coordination and apply consistent standards, controls and tools, while also incorporating signals from banks, vendors and other internal teams. More on this will be covered in the Payments Fraud Controls section of the report (see page 36).

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



Other Groups which discovered fraud:

- Customer service
- Claims department (Insurance)
- Fraud team
- Information technology
- Client services

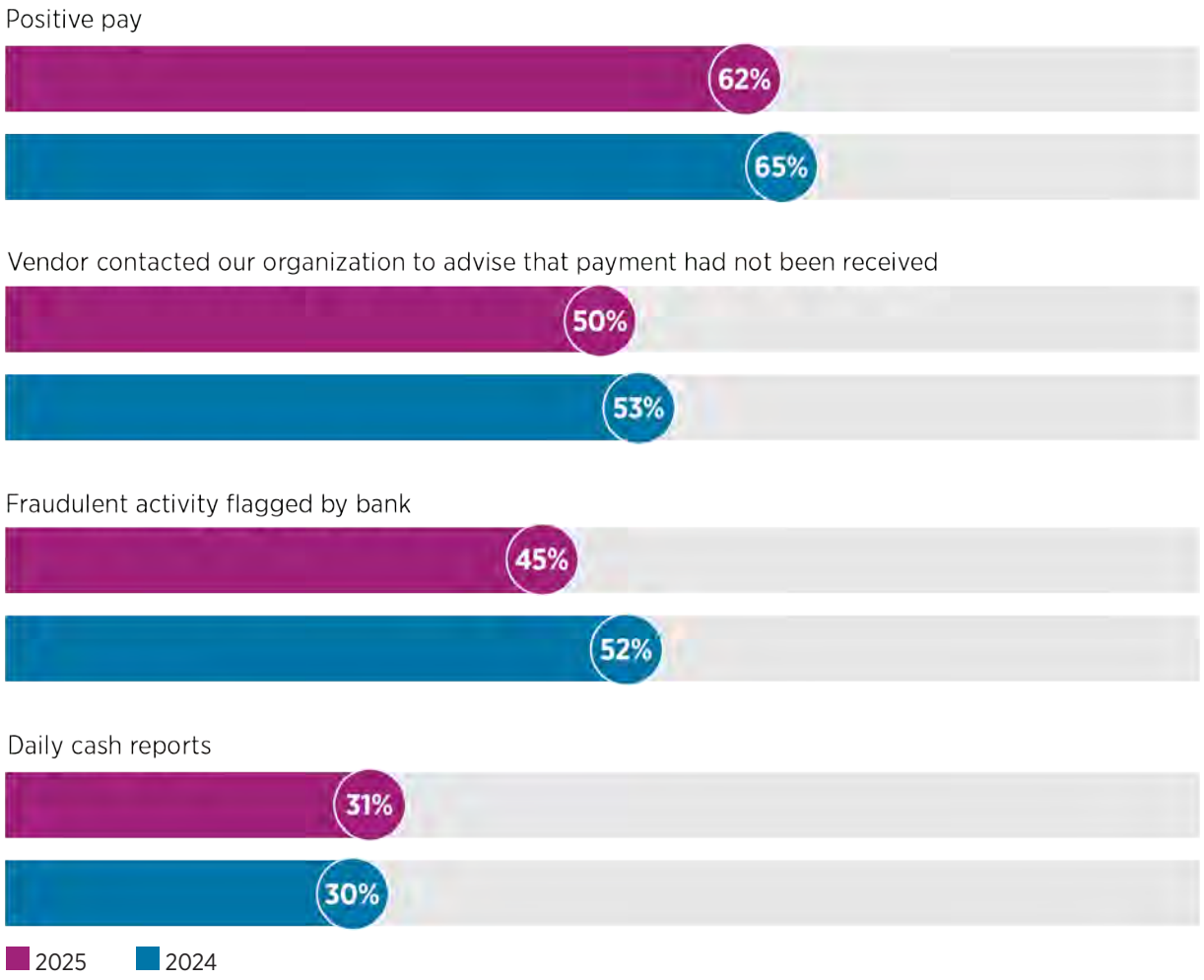
DETECTING FRAUD ACTIVITY CONTINUED

How Fraud is Discovered

Most payments fraud is discovered through a combination of bank-integrated controls and external alerts, with internal cash reporting providing a consistent back-up for discovery. Among organizations that experienced payments fraud in 2025, 62% report that discovery was most often triggered by positive pay, followed by vendor notification that a payment was not received (50%) and suspicious activity flagged by a bank (45%). Compared with 2024, the shares citing positive pay and bank flagging declined, while reliance on daily cash reports remained stable (31% in 2025 versus 30% in 2024). These results suggest that payments fraud is detected using a multi-pronged approach. Open-ended "Other" responses (16%) indicate additional fraud discovery pathways:

- Requests by vendor impersonators to update vendor banking details
- Customers reporting fraud activity
- Internal controls, reconciliation and review processes
- Wire fraud verification safeguards
- Employee-identified instance and general internal awareness

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



Treasury is Primarily Responsible for Managing Payments Fraud Reporting and Recovery Efforts

Managing payments fraud extends beyond detection to include timely reporting, coordinated response and recovery of lost funds. Survey respondents indicate that responsibility for these efforts is typically concentrated within finance and treasury operations but supported by a broader network of stakeholders. The anecdotal responses below highlight how organizations allocate ownership for fraud prevention, detection, reporting and recovery, and illustrate the degree to which responsibilities are centralized within Treasury or shared across Accounts Payable, Accounting, Risk, Legal, Technology and specialized fraud teams. Survey responses indicate that effective fraud management is commonly a cross functional effort, combining operational execution with oversight and technical support:

- Treasury is the primary owner of fraud prevention, detection, and recovery activities, consistently cited far more often than any other function.
- Accounts Payable plays a major operational role, especially in identifying vendor related payments fraud and managing disbursement controls.
- Accounting and Controller functions frequently support reconciliation, documentation review and financial reporting on fraud incidents.
- Legal, Compliance and Risk departments form a secondary layer of oversight, particularly in investigations, escalation and policy enforcement.
- IT, Cybersecurity and Security teams are key partners, especially for email compromise, system access and digital fraud attempts.
- Fraud specific teams (Special Investigation Unit, Fraud Prevention, , Financial Crimes) appear when organizations are large enough to have specialized units.
- Cross functional and shared responsibility models are common, with many responses describing joint ownership among Treasury, AP, IT, Risk and Legal.

We received a call from a fraudster posing as our banking partner, using the bank's correct phone number. The caller asked us to log into our bank account to review a suspected wire. The CFO transferred the call to a Treasury Manager and then separately contacted both the Treasurer and the Treasury Manager to share his concern that the call might be fraudulent. At the same time, the Treasurer contacted the bank directly and confirmed it was a fraud attempt. When the Treasury Manager told the caller that we were on the line with our bank, the caller immediately hung up.

SOURCES OF FRAUD

Fraud via Email Is Most Frequent

Fraudsters attempting to scam businesses resort to various ways to do so. Business email compromise (BEC) stands out as the most common threat, affecting 70% of organizations and between 62% and 76% of organizations across all company segments. External individuals employing tactics outside of email – such as forged checks, stolen cards or identity fraud – also constitute a significant source of fraud, with incidence rates at about 50%. Additional threats include manipulated ACH or wire transfer instructions, invoice fraud and interference from the U.S. Postal Service, each impacting a notable portion of organizations regardless of revenue or account complexity.

Less frequent but still concerning are attacks involving imposters posing as company representatives, unknown or undetermined sources, and fraud using spoofed communications or QR codes. Incidents involving third-party outsourcers, fraudulent live phone calls and account takeovers via system breaches or malware are also reported, albeit at lower rates. Notably, ransomware, malicious internal actors and organized crime rings, while less common, are persistent threats across all segments. Insiders at organizations responsible for committing fraud against their employers represent various departments, e.g., sales, customer service, treasury, etc. The "Other" category, which includes check and credit card fraud as well as counterfeit currency, rounds out the diverse landscape of fraud risks faced by organizations, underscoring the need for comprehensive and adaptive fraud prevention strategies.

The CEO's administrative assistant received an email that appeared to come from the CEO instructing her to have an invoice paid. The email thread showed what was a fraudulent dialogue between the CEO and the vendor. The CEO's administrative assistant sent an email request to Treasury for payment. Because this was a one-time payment for more than $5,000, we had additional controls in place; we require completion of an ACH/wire form so we can validate the banking information, a W-9, and the number of approvals increase from one individual to four. During the "pause" (request for additional information and approvals), the administrative assistant confirmed the payment request verbally with the CEO and discovered it was fraudulent. We then distributed details of the fraud across Finance.

SOURCES OF FRAUD CONTINUED

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

	2025	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)/Fraudulent email	70%	72%	75%	76%	70%
External individual using tactics other than email (e.g., forged checks, stolen cards, identity fraud)	51%	51%	52%	53%	47%
Manipulated ACH or wire transfer instructions	33%	33%	34%	35%	29%
Invoice fraud	26%	26%	26%	20%	40%
U.S. Postal Service office interference	20%	20%	20%	20%	16%
Imposter to a client posing as representative from your company	17%	12%	20%	21%	18%
Unknown or undetermined source	14%	14%	14%	16%	11%
Fraud via spoof/spam text on official mobile devices or fraudulent QR code	13%	15%	12%	10%	24%
Third-party or outsourcer (e.g., vendor, professional services provider, business trading partner)	13%	10%	14%	10%	33%
Fraudulent live phone calls on organization's phone/mobile lines.	8%	6%	10%	6%	13%
Account takeover via system breach or malware (e.g., spyware, social network-based attacks)	8%	7%	10%	9%	4%
Fraud via gateway credentials (fake messages are either emailed or texted impersonating a bank, to trick individuals to provide login credentials on a fake website)	8%	6%	10%	7%	18%
Deepfake attempt (e.g., voice and/or video swapping, "deep voice" technology, vishing)	7%	5%	8%	6%	13%
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)	5%	3%	6%	7%	4%
Ransomware	5%	7%	3%	2%	7%
Internal party (e.g., malicious insider)	3%	2%	4%	4%	4%
Other	8%	9%	7%	6%	9%

Other includes:
- Check-related fraud
- Credit card fraud
- Counterfeit currency

IMPACT OF DEEPFAKE TECHNOLOGY ON PAYMENT SYSTEMS

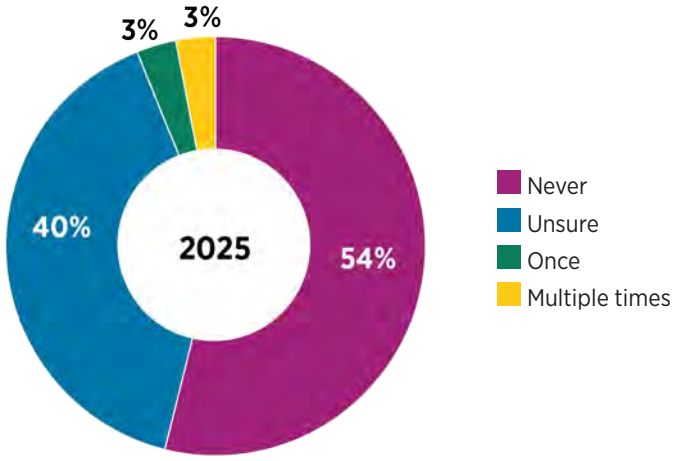
Deepfake Technology Not Yet Pervasive

Deepfake technology refers to the use of artificial intelligence, particularly deep learning algorithms, to create highly realistic but fake audio, video or image content. These manipulated media can convincingly mimic real people's voices, faces and mannerisms, making it difficult to distinguish between genuine and fabricated materials.

More than half of respondents indicate that their organizations' payment systems have not experienced any effects from deepfake technology, while 40% are uncertain if such incidents have occurred. Only a small fraction confirms a direct impact in 2025: 3% report multiple victimizations and another 3% indicate their organizations were targeted just once.

Among organizations that have encountered deepfake technology attacks, audio impersonation through voice cloning was the most frequently reported. In contrast, fewer cases involved advanced video impersonations of staff or vendors or the use of realistic images.

Impact of Deepfake Technology on Organizational Payment Systems in the Past Year
(Percentage Distribution of Organizations)



A recent fraud attempt involved a deepfake video call supposedly from the CFO asking for an urgent payment via WhatsApp. Our company's "Stop, Think, and Ask" policy required the individual to go through all the checks before realizing this video did not originate from the CFO.

REPORTING PAYMENTS FRAUD

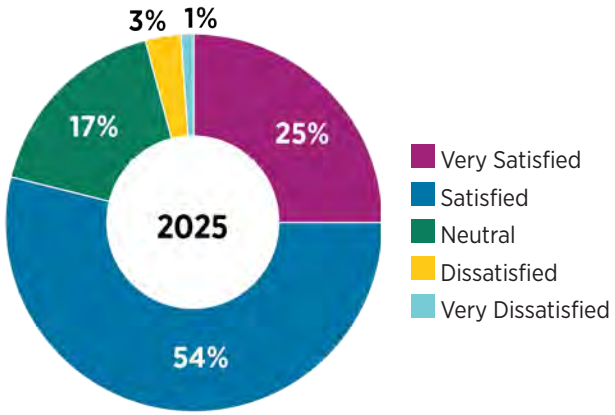
Financial Professionals Look to Banking Partners for Assistance

When organizations uncover fraud, more than three-quarters turn to their banking partners for support, and 66% notify their internal security or compliance teams. Additional measures taken to prevent payments fraud include filing a report with the police (reported by 39% of participants), notifying law enforcement agencies (37%), and only reporting fraud if there is evidence to support the claim (32%).

Large organizations with at least $1 billion in annual revenue are more likely to report fraud to their internal security or compliance teams than are smaller organizations, likely due to having dedicated resources for handling such incidents. These organizations also tend to involve law enforcement agencies such as the FBI more frequently, as larger-scale fraud attacks often require external assistance and the expertise of law enforcement agencies.

Eighty percent of respondents seeking assistance from their banking partners when targeted by fraud reports they are either very satisfied or satisfied with the fraud resolution provided by their partners.

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



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

	2025	ANNUAL REVENUE LESS THAN $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION AND FEWER THAN 26 PAYMENT ACCOUNTS	ANNUAL REVENUE AT LEAST $1 BILLION AND MORE THAN 100 PAYMENT ACCOUNTS
Seek assistance from our banking partner	78%	77%	79%	84%	66%
Inform internal security/ compliance team	66%	57%	72%	71%	66%
File report with police (Local, State or Federal)	39%	37%	40%	38%	43%
Inform law enforcement agencies (e.g., FBI)	37%	27%	42%	39%	46%
Report fraud only if fraud actually occurs	32%	36%	29%	30%	34%
Inform Federal Trade Commission (FTC)	8%	8%	8%	7%	7%
Other	4%	4%	4%	3%	7%

Other includes:

- Cybersecurity
- Insurance specialists, underwriters
- Suspicious Activity Report
- Treasury informs compliance
- Inform counterparty
- Operations manager and board

REPORTING PAYMENTS FRAUD

Respondents reported a variety of payments fraud types that fit into the following broad categories:

Withdrawal from the account and return request was raised via bank

- Vendor payment and banking instruction fraud
- Fraudsters impersonated vendors or infiltrated vendor email systems to request changes to banking instructions, leading to unauthorized payments or attempted payments. In some cases, AP teams failed to independently validate new instructions, resulting in losses; in other instances, controls such as call-backs or validation checks prevented fraud or enabled recovery of funds.
- Several incidents involved fake or altered bank letters and payment forms that appeared legitimate, requiring close inspection to detect anomalies.
- Some organizations improved their vendor account validation processes after experiencing these types of fraud attempts.

Check Fraud and Check Washing

- Numerous cases involved checks being intercepted during mailing, altered (washed) to change payee names or amounts, and then cashed or attempted to be cashed by unauthorized parties. Positive pay and payee validation were frequently cited as effective controls in detecting and stopping fraudulent checks, although some losses still occurred when these controls were not in place or exceptions were mishandled.
- Some checks were duplicated or used for unauthorized ACH transactions using the banking information obtained from intercepted checks.

Email Impersonation and Business Email Compromise (BEC)

- Fraudsters impersonated company executives or vendors via email, requesting urgent payments or changes to payment details. In several cases, internal controls requiring multi-step validation, verbal confirmation or additional approvals prevented losses; in other instances, failure to follow these protocols resulted in fraudulent payments.

Deepfake Technology

- Deepfake video call supposedly from the CFO requested an urgent payment via WhatsApp. The organization's "Stop, Think, and Ask" policy required the individual reviewing the request to go through all the checks before realizing the video did not originate from the CFO.

ACH and Wire Fraud

- Attempts to fraudulently debit accounts via ACH or redirect wire transfers were reported. ACH debit blocks, bank filters and strict approval processes helped prevent unauthorized transactions or facilitated recovery of funds.
- Some incidents involved the manipulation of employee payroll details or customer payment instructions, sometimes due to compromised email accounts or insufficient verification.

Credit Card and Payment Card Fraud

- Fraudsters used stolen or hacked credit card information for unauthorized purchases. Banks often blocked cards and reissued new ones, minimizing losses. Some incidents involved virtual cards, and disputed transactions were managed through established protocols.

Internal Controls and Recovery Efforts

- Positive pay, payee validation, call-back verification and multi-step approval processes were frequently cited as effective controls in preventing or mitigating losses from fraud attempts.
- Organizations routinely collaborated with banks, law enforcement and internal audit or compliance teams to investigate incidents, recover funds and enhance controls.
- Education and communication across departments were emphasized to maintain vigilance and improve fraud detection.

Emerging Trends and Lessons Learned

- Fraud attempts are increasingly sophisticated, leveraging technology such as deepfakes and exploiting lapses in verification procedures.
- Organizations are moving toward electronic payments (e.g., ACH) and reinforcing validation protocols to reduce reliance on checks and limit exposure to check fraud.
- Some losses were unrecoverable, highlighting the importance of robust preventive measures and timely detection.

IMPOSTER FRAUD

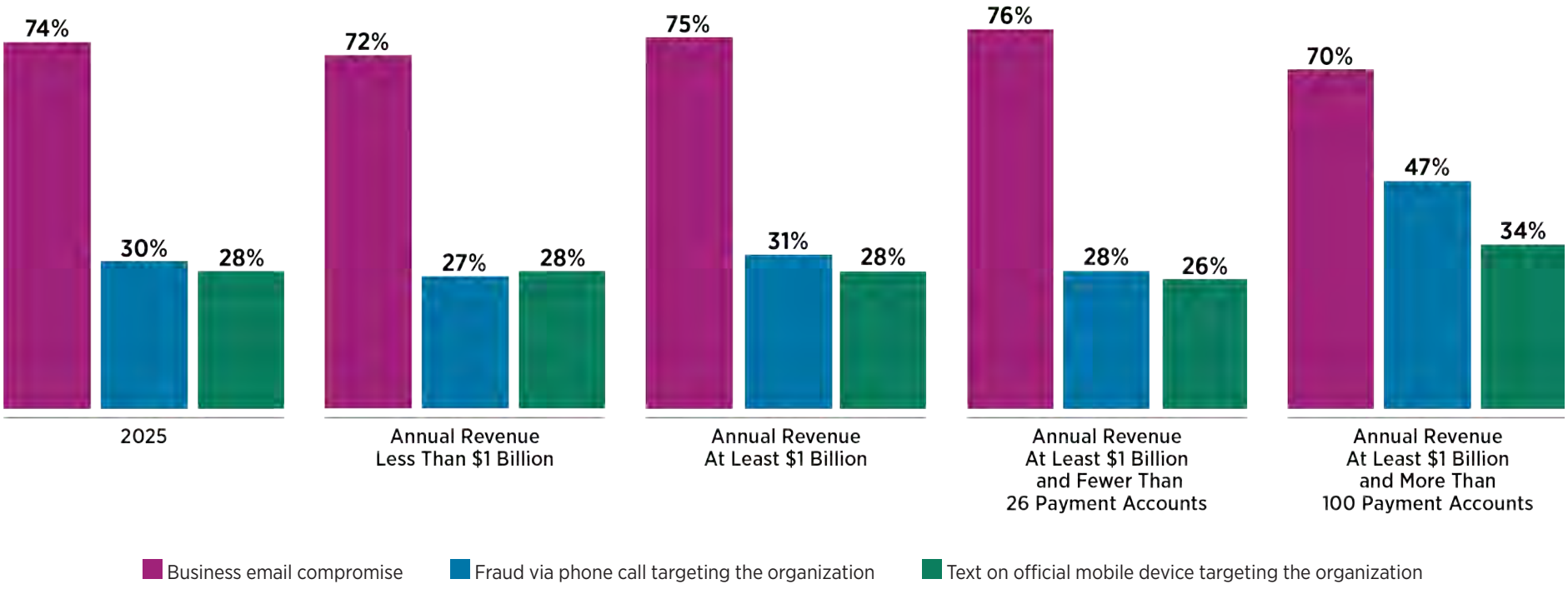
IMPACT OF TYPES OF IMPOSTER FRAUD

Business Email Compromise (BEC) Used Frequently by Imposters

Imposter fraud occurs when a criminal impersonates a trusted individual or entity – such as a company executive, vendor or government agency – to deceive employees and manipulate them into making unauthorized payments or sharing sensitive information. These schemes often use emails, phone calls or texts that appear legitimate in order to trick victims into complying with fraudulent requests. Recognizing and verifying communications before taking action is essential in preventing imposter fraud.

In 2025, nearly 75% of organizations experienced email or BEC fraud, 30% were targeted by fraudulent phone calls, and 28% received scam texts on company mobile devices. Organizations with at least $1 billion in annual revenue and more than 100 payment accounts report higher rates of phone and text fraud targeting their payment systems compared to others.

Types of Fraud Attacks Experienced by Organizations in 2025
(Percent of Organizations Experiencing Payments Fraud)



BUSINESS EMAIL COMPROMISE (BEC)

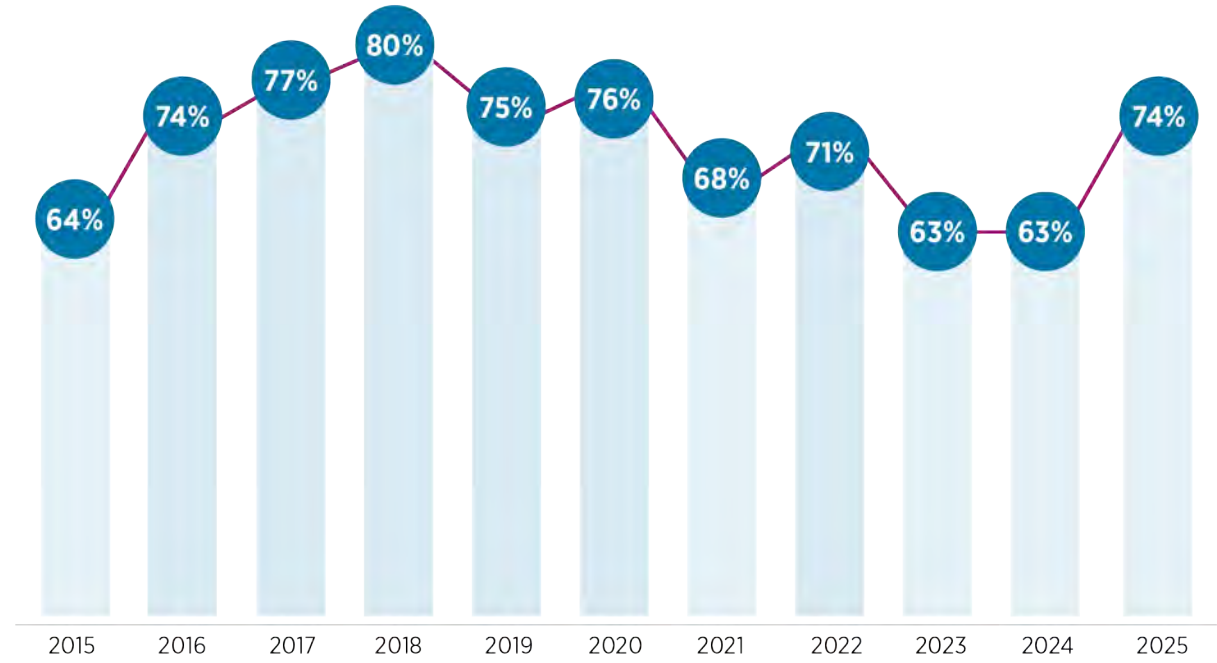
An Uptick in Email Fraud

Business email compromise (BEC) is a sophisticated scam targeting both businesses and individuals performing a transfer of funds. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques resulting in an unauthorized transfer of funds.

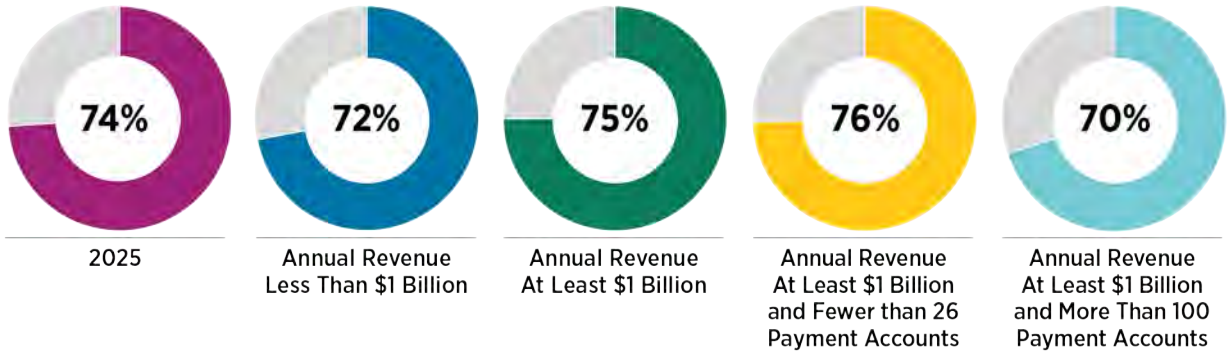
In 2025, organizations experienced a marked increase in fraud attacks conducted through email, with 74% reporting incidents – a 13-percentage-point increase from 2023 and 2024, but similar to the 71% in 2022. Regardless of organizational revenue or the number of payment accounts, at least 70% of entities report being targeted by fraud attempts or attacks via email.

Fraud via email continues to be prevalent because email remains the main communication tool at organizations, making it a prime target for cybercriminals. Scammers use email to pose as trusted contacts like company executives or vendors, convincing recipients to share sensitive information or approve fake payments and often with a heightened sense of urgency. With more employees working remotely or in hybrid setups, it's harder to confirm emails face-to-face, which creates more opportunities for scams. The frequent exchange of emails, easy exploitation, and risk of human mistakes all help drive the ongoing rise in email-originated fraud incidents.

Organizations that Experienced Business Email Compromise (BEC) (2015-2025)
(Percent of Organizations Experiencing Payments Fraud)



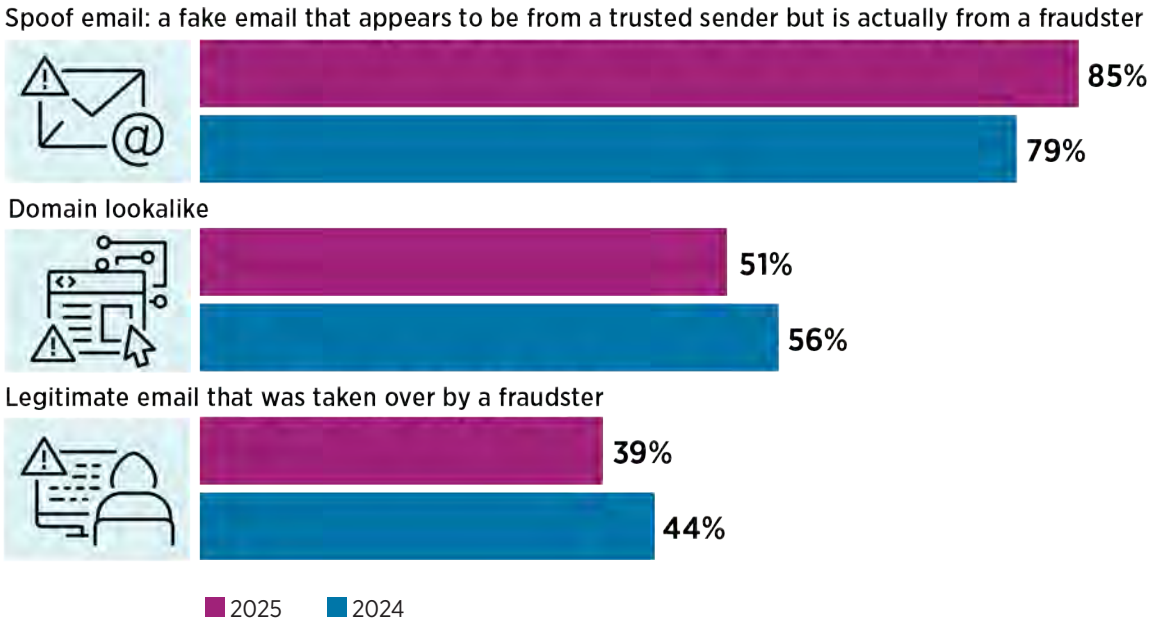
Organizations that Experienced Business Email Compromise
(Percent of Organizations)



BUSINESS EMAIL COMPROMISE (BEC) CONTINUED

Fraudsters often use spoofed emails to scam organizations, sending fake messages that seem to come from trusted senders or vendors. In fact, 85% of organizations received such emails in 2025, an increase from 79% in 2024 and 77% in 2023. More than half of respondents indicate that their companies received emails from domains that looked almost identical to legitimate ones, with only minor differences in a letter or two. Additionally, 39% of organizations continued to receive emails that have been intercepted by fraudsters.

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



A fraudster compromised a client's email and sent new wire instructions. Our teams are supposed to verify such instructions independently, but in this instance, they neglected to do. As such, a fraudulent wire went out. We reported this as an incident within our organization, reported it to the bank to assist, reported it to the local authorities, and reported it to our insurance company and other authorities. Eventually, we implemented new processes to tighten our controls. Furthermore, our bank was able to get the funds returned but it took about 8 months.

FRAUD VIA ORGANIZATIONS' CELL PHONES/PHONE CALLS

Vigilance Needed When Engaging with Text Messages

Spoofed text messages were the leading sources of mobile/cell-phone fraud in 2025, with 92% of organizations reporting such messages on company phones. More than a third received fraudulent texts from compromised known numbers. Use of fraudulent QR codes, while less common, was reported by 11% of organizations.

Although fraud via mobile devices is less common than email-originated fraud, organizations frequently issue mobile phones to employees for official purposes. The widespread sharing of these phone numbers increases their exposure to potentially fraudulent activity. To mitigate risks, organizations should ensure that employees remain vigilant regarding text messages received on company-provided devices, and refrain from engaging with messages that may pose security threats.

Most Prevalent Types of Mobile Device Fraud Targeting Organizations
(Percent of Organizations Experiencing Payments Fraud)

92%
Spoof text message: a fake text that appears to be from a trusted sender but is actually from a fraudster targeting the organization

36%
Text message from a compromised mobile device, i.e., from a known number

11%
Fraudulent QR Code

Fraud Via Phone Calls Targeting Organizations

Besides scamming targets through email and mobile text messaging, fraudsters are now also calling employees at organizations via phones. They often pose as vendors or customers and attempt to redirect funds into fake accounts. For example, fraud over the phone can include several types:

- **Impersonation of financial institutions:** Calls from individuals pretending to represent entities such as American Express® or banks, requesting sensitive account information or attempting to validate banking details.
- **Impersonation of company executives and employees:** Use of deepfake technology and voice impersonation to mimic executives like the CEO, as well as general employee impersonation to gain trust and information.
- **Attempts to change bank account details:** Fraudsters calling to request changes to bank accounts or payment methods, often under the guise of expedited processes or payment issues.
- **Phishing for organizational structure and Personnel Information:** Calls seeking information about company structure, financial personnel or payment processes to facilitate future fraud attempts.
- **Vendor and customer impersonation:** Individuals pretending to be legitimate vendors or customers, claiming issues with payments or ordering services fraudulently.
- **Fake payment and transaction requests:** Calls to Accounts Payable (AP) lines requesting confirmation of transactions or urging payments to fraudulent accounts.
- **Attempts to instruct employees to download malicious apps:** Calls instructing company personnel to download apps onto company phones under the pretense of resolving fraudulent charges.
- **Repeated payment requests after fraudulent activity:** Persistent follow-up calls from fraudsters after a payment was made correctly, seeking additional payments.
- **General attempts to obtain unauthorized information:** Calls aiming to gather any information not normally available to the caller, with the intention of committing payment fraud.

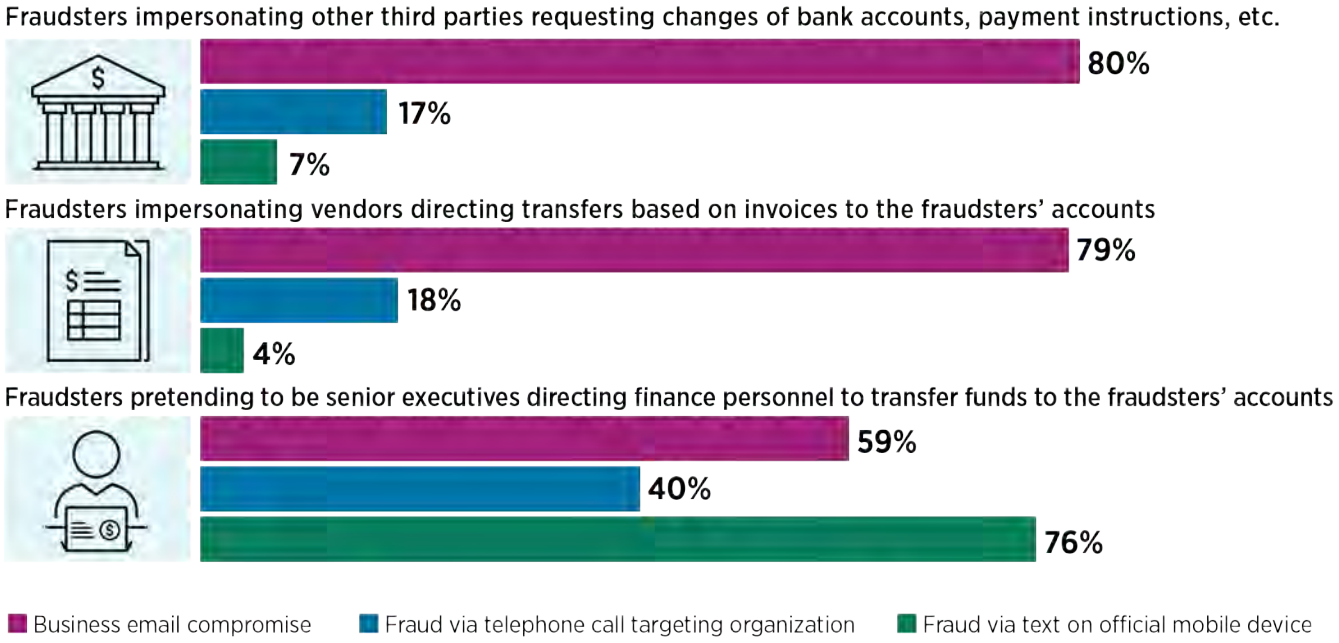
These fraudulent calls targeted various departments including Treasury, Accounts Payable and call centers, often leveraging social engineering techniques and exploiting gaps in verification procedures. Enhanced controls, staff education and vigilant protocols helped identify and mitigate these threats.

KEY PERPETRATORS OF FRAUD

Impersonation Most Often Used to Scam Targets

Payments fraud often involves perpetrators using email, phone calls or text messages to impersonate third parties, vendors or senior executives. About 80% of email scams request changes to bank accounts or payment instructions by fraudsters impersonating third parties/vendors, and nearly 60% of organizations report having received emails from imposters posing as senior executives to redirect funds in 2025. Phone scams primarily involve impersonating executives to persuade finance staff to transfer money. Although scams through cell phones are less common, most text message scams involve fraudulent requests from supposed executives for company fund transfers.

Fraud Perpetrators
(Percent of Organizations Experiencing Payments Fraud)



A fraudster posed as member of bank service team requesting a payment be executed through our banking portal. An employee executed the payment. As a result, we have instituted a global review process for banking portal capabilities, and have documented which banking portals do not meet our standards for segregated payment input, review and release.

PAYMENT METHODS USED IN IMPOSTOR SCAMS

Business Email Compromise

Various payment methods continue to be vulnerable to BEC; 49% of fraud via email in 2025 were made using wire transfers, a decline from 63% in 2024, but higher than in 2023 and 2022. About one-third of organizations reports that the payment methods used by fraudsters were ACH debits (34%), checks (33%). The use of ACH credits for BEC, at 31%, is significantly lower than the 50% reported last year. For a third consecutive year, real-time payments were one of the payment methods impacted by BEC. Overall, 6% of respondents indicate real-time payments were targeted via BEC.

Telephone Calls

Fraudsters mainly used checks (40%) in phone scams, with wire transfers (35%) and ACH credits (33%) close behind.

Fraud Via Text (Mobile Devices)

Few organizations report payments were made through fraudulent texts, but checks, ACH credits and gift cards were the second most-common methods used in fraud in 2025.

Payment Methods Utilized in Fraud Attacks via Email, Telephone Calls and Text Messages
(Percentage Distribution of Organizations Experiencing Payments Fraud)

	BUSINESS EMAIL COMPROMISE		FRAUD VIA TELEPHONE CALL TARGETING ORGANIZATION	FRAUD VIA TEXT ON OFFICIAL MOBILE DEVICE
	2025	2024	2025	2025
Wire transfers	49%	63%	35%	20%
ACH debits	34%	26%	27%	20%
Checks	33%	26%	40%	30%
ACH credits	31%	50%	33%	30%
Corporate/commercial credit cards (e.g., purchasing, T&E, Fleet)	10%	11%	17%	35%
Third-party payouts (e.g., Venmo®, PayPal®, Zelle®, etc.)	7%	9%	17%	20%
Real-time payments (RTP®, FedNow®)	6%	3%	10%	10%
Gift cards	6%	6%	13%	30%
Cash	6%	8%	10%	15%
Cryptocurrency (Bitcoin, Ethereum®, etc.)	2%	3%	8%	15%
Virtual cards	2%	–	13%	35%

DEPARTMENTS VULNERABLE TO IMPOSTER FRAUD

Business Email Compromise

Survey results suggest that 80% of respondents view Accounts Payable as highly vulnerable to BEC attacks. In half of the organizations surveyed, treasury departments are also seen as easy targets for email-based fraud. Approximately one-third of organizations report that procurement, sourcing departments and the C -Suite are vulnerable to fraudulent emails. Accounts Receivable and Customer Service receive scam emails in about one-fourth of organizations.

Telephone Calls

Almost 60% of those surveyed say imposters often target their Accounts Payable teams with fraudulent phone calls. Meanwhile, 36% note that their treasury departments are also at risk of receiving scams via phone calls. Additionally, customer service teams are frequently targeted, with 28% reporting fraud attempts by phone.

Fraud Via Text (Mobile Devices)

The three areas at organizations most-often-targeted by fraudulent text messages are Accounts Payable (51%), Treasury (37%) and C-Suite Executives (35%).

Departments Most Vulnerable to Targeting by Imposter Scams
(Percentage Distribution of Organizations Experiencing Payments Fraud)

	BUSINESS EMAIL COMPROMISE		FRAUD VIA TELEPHONE CALL TARGETING ORGANIZATION	FRAUD VIA TEXT ON OFFICIAL MOBILE DEVICE
	2025	2024	2025	2025
Accounts Payable	80%	56%	59%	51%
Treasury	50%	9%	36%	37%
Procurement/Sourcing	32%	8%	23%	19%
CEO, COO, CFO, or other C-Suite Executives	32%	9%	24%	35%
Accounts Receivable	26%	4%	20%	12%
Customer Service	23%	--	28%	18%
Human Resources/Payroll Department	21%	1%	13%	12%

CHECK USAGE

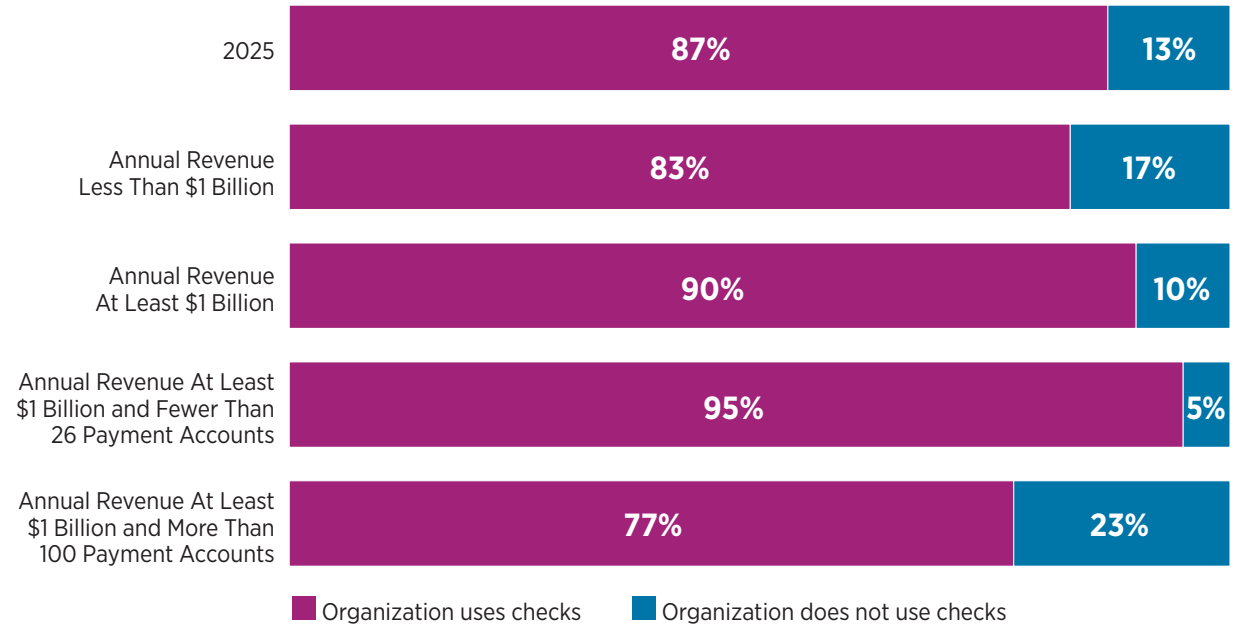
CHECKS CONTINUE TO BE ISSUED EXTENSIVELY

Despite being the payment method most vulnerable to payments fraud, check usage at businesses is widespread: 87% of organizations report using checks in 2025.

Among organizations with annual revenue of at least $1 billion, the number of payment accounts managed appears to influence check usage. For those with up to 25 payment accounts, 95% report using checks, compared with 77% of organizations with more than 100 payment accounts. This pattern suggests that as payment operations become more complex, organizations move away from checks.

Check usage is more prevalent in the lower-use bands. In 2025, 72% of organizations that use checks report that checks accounted for 25% or less of their payments (42% use checks for 10% or less of payments and 30% use checks for 11%–25% of payments). Use patterns vary within larger organizations: among those with annual revenue of at least $1 billion, the percentage of organizations using checks for more than 50% of payments was 10% overall, 6% for organizations with fewer than 26 payment accounts, and rises to 19% for those with more than 100 payment accounts.

Check Usage at Organizations
(Percentage Distribution of Organizations)



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

	2025	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	42%	43%	41%	40%	40%
11%-25%	30%	24%	33%	37%	21%
26%-50%	18%	21%	16%	17%	19%
Over 50%	10%	11%	10%	6%	19%

CHECKS CONTINUE TO BE ISSUED EXTENSIVELY CONTINUED

Reasons for Continuing Check Use

Organizations Compelled to Use Checks Due to Vendor/Customer Requests

Despite well documented fraud risks and operational inefficiencies, there are several use cases still requiring payment via check. Many organizations continue to rely on checks due to practical, regulatory and counterparty driven constraints. Check use often persists for those vendors or customers who require it, when working with smaller organizations that lack electronic payment capabilities, or in situations such as refund processing and certain tax payments where alternatives are limited. In addition, some organizations face internal barriers – including legacy systems and the difficulties of system change – that slow the transition away from checks.

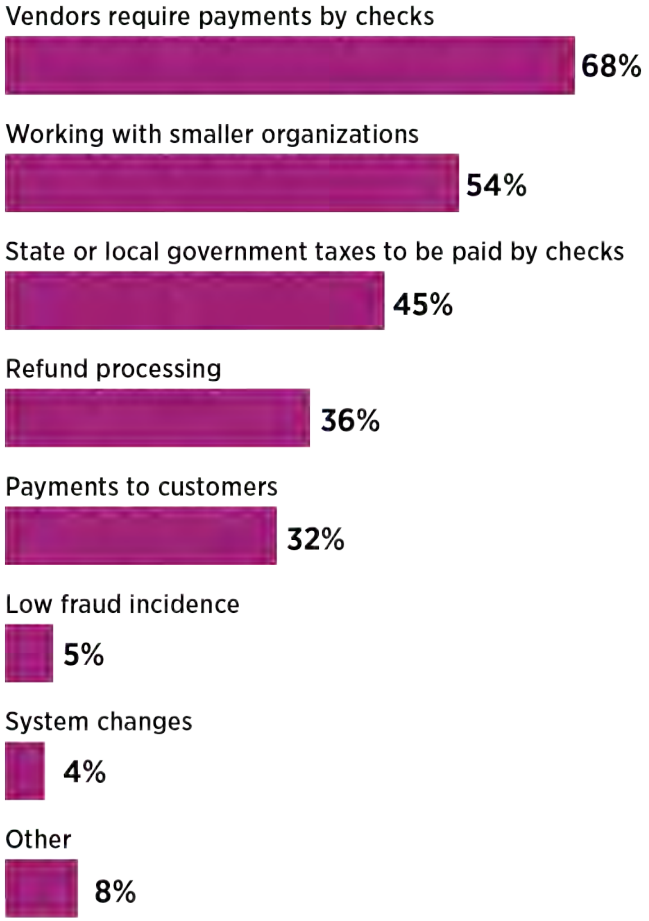
For organizations without plans to eliminate the use of checks, external factors account for the top three reasons. Over two-thirds (68%) of organizations that are not planning to eliminate the use of checks indicate that a requirement for checks by vendors is a reason to continue check use. Additional reasons include:

- **Working with smaller organizations** (cited by 54% of those organizations not planning to eliminate the use of checks)
- **State or local government taxes to be paid by checks** (36%)
- **Payments/refunds to customers** (32%)

Responses in the "Other" category indicate that organizations have additional use cases outside of the predefined response options. The major themes of these responses include:

- Some vendors, government agencies and utility companies only accept checks and do not support electronic payments such as ACH.
- There are difficulties in setting up vendors for ACH such as outdated ERP systems that cannot generate ACH files or incomplete banking information from clients or vendors.
- Checks are preferred in scenarios where immediate payment verification of electronic instructions is not possible, such as for consumer refunds, true-up payments to former employees or when waiting to verify vendor wiring instructions.
- Management preferences and resistance to change, along with lack of executive support for check elimination initiatives, can slow the transition to electronic payments.
- Specific business models (e.g., those involving retirees or talent management teams) require the flexibility and speed of issuing checks.
- Checks enable float on funds, providing additional time before funds are withdrawn from the payer's account.
- Complex payment scenarios, such as payments to multiple parties (split beneficiaries, two-party checks or insurance premium refunds), are often easier to manage with checks.
- Checks are sometimes used temporarily until electronic payment methods can be securely established and verified.

Reasons Organizations Continue to Use Checks
(Percent of Organizations Not Planning to Eliminate Use of Checks)



CHECKS CONTINUE TO BE ISSUED EXTENSIVELY CONTINUED

Reasons for Eliminating Check Use

Fraud Leading Reason Organizations Plan to Stop Issuing Checks

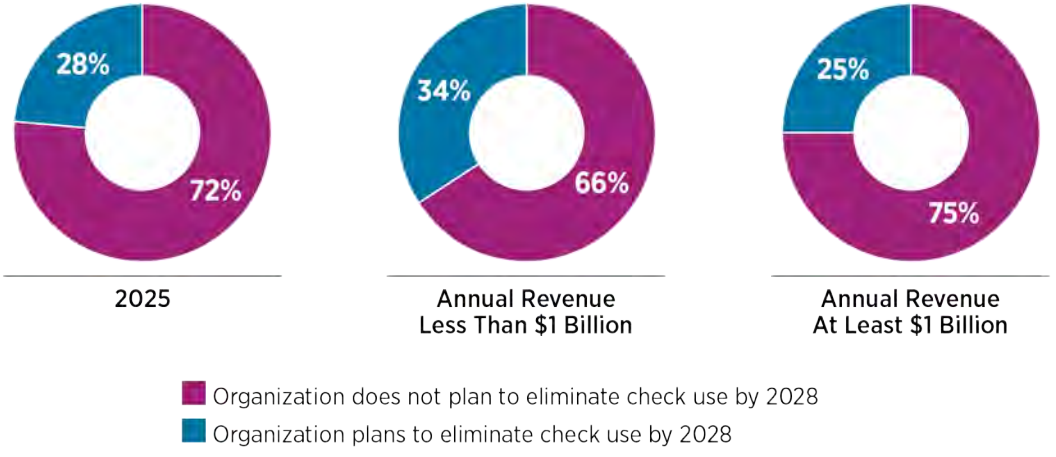
The cons of check use continue to motivate organizations to move away from checks, however. Of those organizations currently using checks, 28% plan to eliminate check use within the next two years.

Survey respondents indicate a variety of reasons in support of eliminating check use. The most-often cited reason is checks' vulnerability to fraud (cited by 75% of respondents from organizations planning to eliminate the use of checks). Other reasons reported by a majority of respondents include:

- **Manual process** (68%)
- **Administrative burden** (64%)
- **Administrative and labor costs** (54%)

The top four reasons for considering the elimination of checks are unchanged from 2024, but their order has shifted for 2025.

Intent to Eliminate the Use of Checks by 2028
(Percentage Distribution of Organizations Using Checks)



Reasons for Considering Eliminating the Use of Checks
(Percent of Organizations Planning to Eliminate Use of Checks)

	2025
Vulnerability to fraud	75%
Manual process	68%
Administrative burden	64%
Administrative and labor costs	54%
Escheatment process	34%
Float time	20%
Executive Order mandating the transition to electronics payments for all Federal disbursements and receipts	6%
Other	2%

Other includes:
- Requirement from vendor
- Cost

CHECKS CONTINUE TO BE ISSUED EXTENSIVELY CONTINUED

Disbursing Checks

How organizations disburse checks has important implications for both cash flow management and fraud exposure. Despite well known risks associated with their use, checks continue to offer a tangible audit trail, relatively low transaction fees and accommodation of customer and vendor preferences, all of which helps explain checks' continued use. In 2025, 70% of organizations disbursed checks via USPS without tracking, while 47% used commercial carriers such as FedEx®, UPS® or DHL®, and 27% include USPS tracking. Forty-two percent of organizations using checks also rely on banks or third party vendors to print and mail checks, while fewer organizations use hand or courier delivery (14%).

The continued reliance on untracked mail underscores the ongoing risk of mail theft related check fraud. When checks are intercepted, fraudsters most commonly alter and deposit the original check, use the check as a template to create counterfeits, or fraudulently endorse and deposit the check. Although many organizations employ more secure delivery methods – such as commercial carriers or tracked mail – the prevalence of general mail usage indicates that exposure to these fraud scenarios remains a persistent concern.

Methods for Disbursing Checks
(Percent of Organizations Using Checks)

	2025
USPS general mail (without tracking)	70%
Commercial carrier (FedEx®, UPS®, DHL®, etc.)	47%
Checks are printed and sent by bank or third-party vendors	42%
USPS with tracking	27%
Hand/Courier delivery	14%

Check Fraud via USPS

Independent reporting and federal regulators point to the same conclusion: mail theft related check fraud remains a persistent and high impact risk. A January 2026 **Forbes personal finance article** describes how fraudsters routinely steal checks from mailboxes and postal collection points, alter or replicate them using readily available technology, and deposit them before victims or financial institutions can intervene. The article emphasizes that what appears to be an "old" crime has been modernized through chemical check washing, high quality printers, and remote deposit methods that minimize human review.

Federal data reinforce this assessment. In a September 2024 **Financial Trend Analysis**, the Financial Crimes Enforcement Network (FinCEN) reported that mail theft related check fraud was linked to more than $688 million in suspicious activity over a six month period, based on over 15,000 Bank Secrecy Act filings from 841 financial institutions nationwide. FinCEN found that stolen checks were most commonly altered and deposited or used as templates for counterfeits.

Similarly, the FBI and U.S. Postal Inspection Service issued a 2025 **Public Service Announcement** warning that mail theft enabled check fraud is increasing, citing a sharp rise in related suspicious activity reports and highlighting how fraudsters exploit funds availability timelines to move money before fraud is detected.

Taken together, these sources underscore that continued reliance on paper checks sustains long standing fraud schemes, even as criminals adopt modern tools and techniques. For more information, check out these articles:

- **February 2025:** A USPS employee and co-conspirator in Alabama managed to steal more than $17 million in high-value checks en route to their business PO Boxes
- **May 2025:** Four individuals charged in $63 million mail theft conspiracy, including two postal employees
- **December 2025:** A USPS employee in Connecticut was sentenced to 30 months in prison for stealing mail for the purpose obtaining checks that were payable to other individuals. The checks totaled more than $285,000
- **February 2026:** Checks pulled from mail in Gage County [NE], washed, and cashed elsewhere, deputies say

PAYMENTS FRAUD CONTROLS

BUSINESS EMAIL COMPROMISE PREVENTION

Organizations are adopting comprehensive policies to assist employees in identifying fraudulent emails and establishing systems that alert staff to potential threats before such messages reach their inboxes. These proactive measures significantly reduce the risk and impact of email-based payments fraud. Clicking on malicious links or opening suspicious attachments can result in considerable harm to an organization. To mitigate these risks, many organizations are diligently developing and implementing targeted procedures and controls aimed at preventing payments fraud, particularly through business email compromise (BEC).

Survey findings show that top-ranked measures include established policies for verifying changes to invoices, bank deposits and contact details. These policies have been implemented at 96% of organizations, and 91% of respondents believe they are effective in safeguarding organizations from falling victim to a fraudulent email. End-user education and training on identifying fraudulent emails and spear phishing attempts is also widely adopted, with 96% of organizations implementing it; 84% of survey participants consider it an effective way to reduce email scams.

Ninety-four percent of companies have implemented company policies for verifying fund transfer requests by calling an authorized contact at the payee organization using a phone number from official records, not from email. This approach appears to have been effective in controlling BEC as reported by 94% of respondents. At 94% of organizations, employees are required to get an authorized signoff from senior management for transactions over a certain threshold, a policy found to be effective by 84% of respondents

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

- **Stronger internal controls prohibiting payment initiation based on emails or other less secure messaging systems** (implemented at 91% of organizations)
- **Providing additional training to/reprimanding employees who repeatedly fail simulated testing or open phishing emails** (84%)
- **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** (35%)

Clicking on scam attachments or links can seriously harm organizations. Employees may accidentally fall for fraudulent emails, especially with advanced AI-based scams that are hard to spot. Consequently, organizations need to ensure they are equipping their employees with the necessary safeguards to prevent them from falling for these crimes and putting their organizations at risk by implementing safeguards to block fraudulent emails, and encourage verification practices even in remote and hybrid settings.

We received an invoice from a company with which we don't normally do business. The invoice referenced both a location our company hasn't had in many years as well as an employee who hasn't been with our company for a while. The invoice was sent to us by email and the email looked suspicious to me. A staff member had called the vendor and was convinced the invoice was real; she wasn't aware of the practices surrounding business email compromise (BEC) or deepfakes such as call centers that handle calls inquiring about fake invoices. I was able to prove the invoice was fake. Subsequently, I set up an education presentation for all our employees about BEC and invoice fraud. Now our employees are educated on a consistent basis on fraud.

BUSINESS EMAIL COMPROMISE PREVENTION 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
Established policies to verify changes to invoices, bank deposits and contact details	**96%**	58%	33%	8%	1%	--
End-user education and training on identifying fraudulent emails and spear phishing attempts	**96%**	42%	42%	14%	1%	1%
Verifying fund transfer requests by calling an authorized contact at the payee organization using a phone number from official records, not from email	**94%**	63%	31%	6%	--	--
Requiring authorized signoff of senior management for transactions over a certain threshold	**94%**	52%	32%	10%	4%	1%
Stronger internal controls prohibiting payment initiation based on emails or other less secure messaging systems	**91%**	53%	35%	10%	1%	1%
Providing additional training to/reprimanding employees who repeatedly fail simulated testing or open phishing emails	**84%**	36%	42%	18%	3%	1%
Using passcodes known only to both parties in a proposed wire transaction (not contained in an email)	**42%**	52%	26%	16%	5%	1%
Terminating employees who repeatedly fail simulated testing or open phishing emails.	**35%**	29%	32%	24%	9%	6%

BUSINESS EMAIL COMPROMISE PREVENTION – SECURITY AND COMPLIANCE MEASURES

Organizations are also safeguarding their payment systems from email attacks 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 90% of respondents as an effective measure to combat BEC fraud. Two-factor authentication is used at 91% of organizations in their efforts to mitigate payments fraud via email.

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 77% of organizations)
- **Intrusion detecting systems that flag emails with extensions similar to company emails** (example: where "rn" could be in the place of an "m," etc.) (67%)
- **Prohibiting, or at least quickly detecting, emails where the "reply" email address is different than the "from" email address shown** (66%)
- **Using a bank or vendor system where beneficiaries manage their own refund or return information** (63%)
- **Color-coded emails with colored banners or other methods of distinction, etc., indicating they are external** (44%)
- **Implementing TLS keys, between sender and bank in lieu of encrypted email or password protected document to validate payment information via email** (42%)

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 payment initiation	**91%**	57%	33%	8%	1%	--
Review of email forwarded from outside of your organization	**77%**	32%	39%	26%	2%	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.)	**67%**	39%	41%	18%	2%	1%
Prohibiting, or at least quickly flagging, emails where the "reply" email address is different than the "from" email address shown	**66%**	41%	40%	16%	3%	--
Color-coded emails with colored banners or other methods of distinction etc. indicating they are external	**63%**	35%	35%	24%	5%	1%
Using a bank or vendor system where beneficiaries manage their own refund or return information	**44%**	38%	35%	24%	2%	1%
Implementing Transport Layer Security (TLS) keys, between sender and bank in lieu of encrypted email or password protected document to validate payment information via email	**42%**	39%	40%	15%	2%	3%

CHECK FRAUD CONTROLS

Due to the extensive use of checks at organizations, check fraud remains a persistent threat to businesses, financial institutions and individuals. Effective controls are essential to mitigating risk, protecting financial assets and maintaining trust in payment systems. As a result, organizations must prioritize robust measures to detect and prevent fraudulent activity. Given that a large majority of organizations continues to use checks, safeguarding against check fraud remains a critical concern for treasury professionals.

Treasury practitioners are well aware of checks' vulnerability to fraud, and most of their organizations have implemented controls designed to provide strong protection against check-related losses. Ninety-six percent of respondents report their organizations have implemented positive pay to curb check fraud. Other measures implemented include:

- **Daily reconciliation and other internal processes** (cited by 94% of respondents)
- **Payee positive pay** (93%)
- **Segregation of accounts by function for single purpose** (89%)
- **Tamper resistant features on checks** (83%)

These measures are also viewed as highly effective, with positive pay (95%) and payee positive pay (97%) most frequently rated *effective* or *very effective*. The data, however, suggest an implementation gap for some controls: reverse positive pay is rated highly (88% effective/very effective) but is implemented by fewer organizations (57%), indicating potential operational or adoption barriers. Reverse positive pay, according to AFP's *Essentials of Treasury, 7th Edition*, is a process in which a bank sends a daily or intraday file of checks presented for payment, and the company reviews the file against issued checks and directs the bank to return any exceptions. Overall, the concentration of responses in the top effectiveness categories indicates that organizations prioritize and value controls that strengthen verification and exception handling in check processing. In contrast, 83% of organizations utilize tamper resistant features on checks, but only 55% of organizations rank them *effective/very effective*.

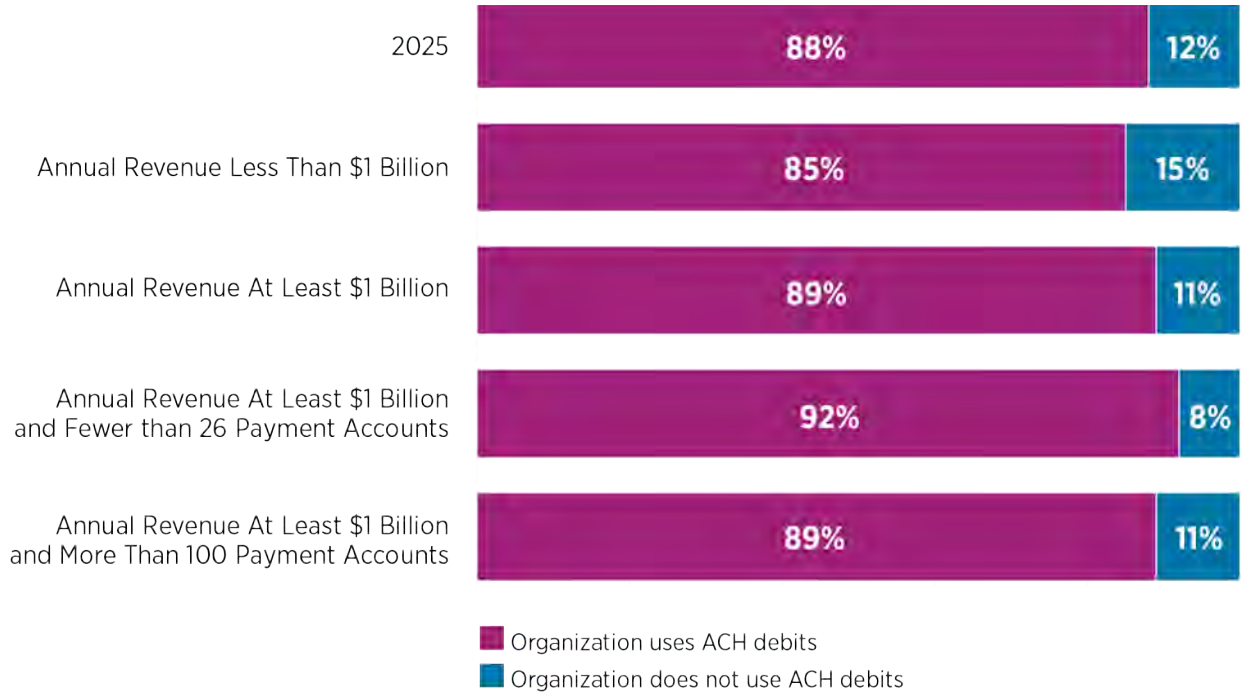
Effectiveness of Fraud Control Procedures and Services used to Protect Against Check Fraud
(Percent of Organizations Using Checks)

	IMPLEMENTED	VERY EFFECTIVE	EFFECTIVE	SOMEWHAT EFFECTIVE	NOT VERY EFFECTIVE	VERY INEFFECTIVE
Positive pay	**96%**	71%	24%	4%	1%	--
Daily reconciliation and other internal processes	**94%**	54%	29%	15%	1%	--
Payee positive pay	**93%**	79%	18%	3%	--	--
Segregation of accounts by function for single purpose	**89%**	48%	35%	15%	2%	--
Tamper resistant features on checks	**83%**	33%	32%	24%	8%	3%
"Post no checks" restriction on depository accounts	**77%**	67%	24%	7%	2%	--
Reverse positive pay	**57%**	55%	33%	10%	1%	2%
Non-bank fraud control services	**52%**	38%	36%	23%	3%	1%

ACH DEBIT FRAUD AND CONTROLS

Organizations continue to use ACH debits extensively. Eighty-eight percent of companies used ACH debits in 2025 – unchanged from 2024.

ACH Debit Usage
(Percentage Distribution of Organizations)



An imposter called the AP general line pretending to be from our bank. AP staff knew to reach out to Treasury which then reached out to our banker for confirmation that the call was not legit. Our banker and the bank's support team erroneously insisted it was a legitimate call, and only after continued persistence did they agree to research the case further, ultimately confirming (days later) that the call had not been legitimate. No information was shared with the imposter.

ACH DEBIT FRAUD AND CONTROLS CONTINUED

More than 90% of organizations use both *daily account reconciliation to identify and return unauthorized ACH debits*, as well as the practice of *blocking all ACH debits except on designated accounts with an ACH debit filter*. At least 90% of respondents consider these controls effective.

While 70% of organizations control ACH debit fraud by placing debit blocks on consumer items with debit filters on commercial ACH debits, 94% believe this method is effective. Fewer than 60% block ACH debits on all accounts, but 92% find this approach effective.

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	**95%**	80%	17%	3%	--	--
Reconcile accounts daily to identify and return unauthorized ACH debits	**92%**	63%	28%	8%	1%	--
Debit block on all consumer items with debit filter on commercial ACH debits	**70%**	72%	22%	5%	1%	--
Block ACH debits on all accounts	**57%**	72%	20%	7%	1%	--

Nacha Rules Rolling out to Combat ACH Fraud:

The 2026 Nacha fraud monitoring rules mandate risk-based, proactive fraud detection for both ACH debits and credits across the network, targeting schemes like BEC. Compliance rolls out in two phases: larger participants first, everyone by June 2026.

Summary of Upcoming Rule Changes

Source: Summary of Upcoming Rule Changes | Nacha

March 20, 2026

- Fraud Monitoring by ODFIs (Originating Depository Financial Institution- where the transaction is initiated)
- Fraud Monitoring by large Originators, TPSPs, and TPSs (Phase 1) (Third Party Service Providers, Third Party Senders or Originators from a non-Financial Institution)
- ACH Credit Monitoring by large RDFIs (Phase 1) (Receiving Depository Institution)
- New Company Entry Descriptions – PAYROLL and PURCHASE

June 22, 2026

- Fraud Monitoring by all other Originators, TPSP, and TPS
- ACH Credit Monitoring by all other RDF

September 18, 2026

- Definition of IAT entries (for international ACH Transactions)
- Funds Availability Requirements for Non-Same Day ACH Credit Entries

January 1, 2027

- Registration of IAT Contacts in the ACH Contact Registry

March 19, 2027

- Optional Date of Birth Field for IAT Entries
- Non-Bank Foreign Financial Agencies in IAT Entries

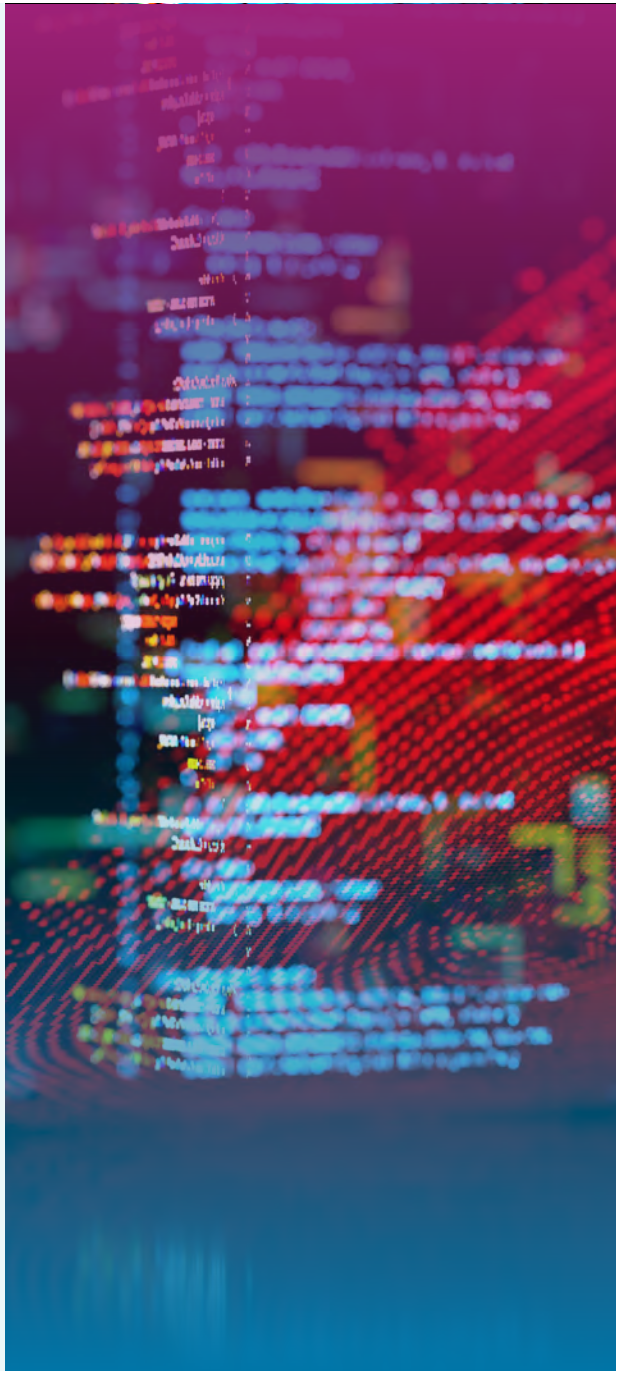
March 17, 2028

- New Return Reason Code (R90) for Sanctions Compliance Obligations

Implications for Treasury Departments

Your bank or vendor might have reached out to you already to discuss the changes. If not, it is worth proactively reaching out to them and discussing (in addition to internal departments as needed):

- How the bank/vendor will carry out the rule changes
- Potential impacts to your origination process
- ACH formats and beneficiaries most likely impacted in your mix of activity
- Understand pricing implications
- Credit implications for ACH support
- Solutions in place for exceptions (like ACH positive pay)
- Policies, process and control changes that require documentation updates
- Informing other ACH originating departments in the company
- Any third-party senders used for other types of ACH payments at the company (payroll, refunds, travel/expenses, etc.)



IMPACT OF ARTIFICIAL INTELLIGENCE (AI) ON PAYMENTS FRAUD CONTROLS

Organizations Yet to Embrace AI for Fraud Control

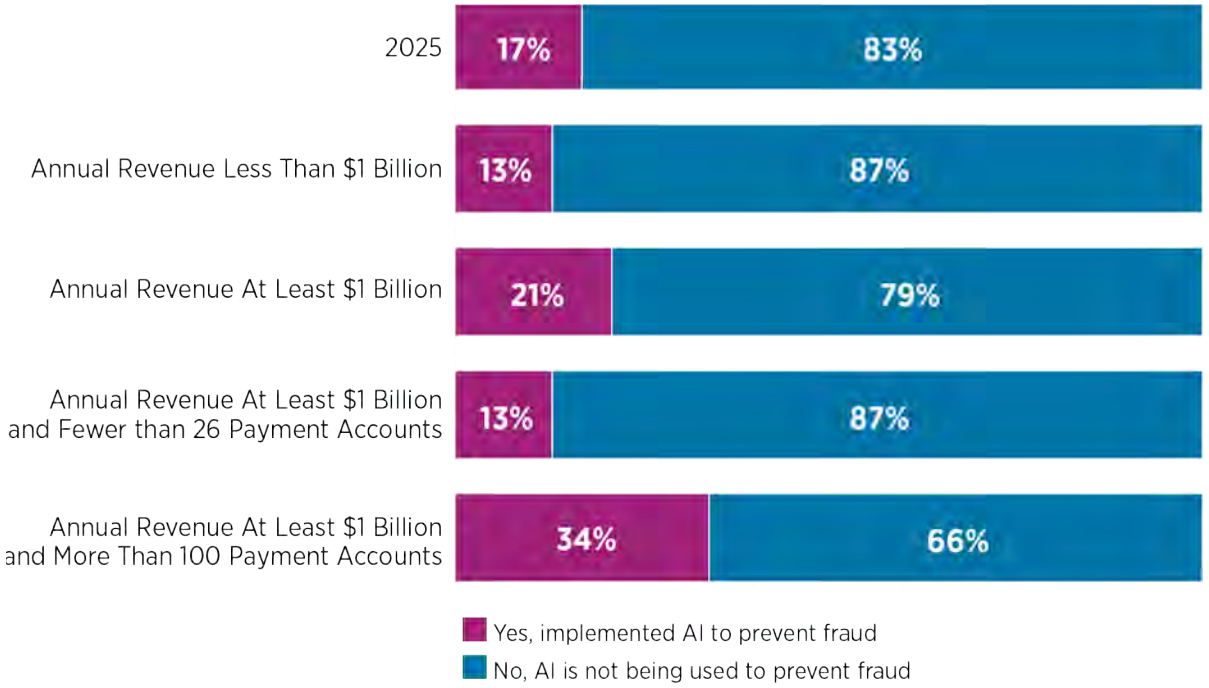
AI can help prevent payments fraud by analyzing large volumes of transaction data in real time through a Treasury Management System (TMS), Enterprise Resource Planning (ERP), payment gateway or a standalone solution in addition to your bank/vendor monitoring to detect unusual patterns or behaviors that may indicate fraudulent activity for payments but also invoices. Machine learning algorithms continuously learn from historical fraud cases, allowing them to flag suspicious transactions more accurately, provide risk scoring and reduce false positives. Additionally, AI can automate the monitoring process, making it easier for organizations to identify potential threats quickly and respond before losses occur.

By leveraging AI, companies can enhance their fraud prevention strategies, especially as fraudsters use increasingly sophisticated methods. AI-powered systems can adapt to new tactics, identify anomalies, and provide early warnings, which is particularly valuable for organizations with high transaction volumes or complex payment structures.

Report findings indicate that most organizations have been slow to adopt AI for fraud prevention, as just 17% of respondents say their companies rely on AI to combat fraud. Larger companies – those with annual revenue of at least $1 billion and more than 100 payments – are more likely than others to use AI to reduce payments fraud. It is advisable to inquire with your provider whether artificial intelligence is employed in fraud monitoring across all payment types.

Respondents cite several factors contributing to their organization's reluctance to implement AI in payments fraud prevention initiatives. A lack of adequate infrastructure, resources, and the substantial financial investment required are all cited as barriers. Additionally, limited familiarity with AI technology and uncertainty regarding its effectiveness in preventing payments fraud have contributed to hesitancy. Some organizations are currently evaluating AI solutions for fraud control and determining their applicability.

AI Implementation for Payments Fraud Prevention
(Percentage Distribution of Organizations)



IMPACT OF AI ON PAYMENTS FRAUD CONTROLS CONTINUED

Organizations utilizing AI to combat payments fraud have experienced enhanced efficiency in fraud reporting (49%), improved detection of deepfake technology (45%) and real-time identification capabilities (43%). The benefits associated with adoption of AI are evident; however, broader implementation is necessary for organizations to fully realize these advantages.

Impact of AI on Payments Fraud Prevention*
(Percent of Organizations)

	2025
Increased efficiency in controlling fraud	49%
Detection of deepfake technology	45%
Real-time detection	43%
Biometric authentication	35%
Reduction in false positives	31%
Other	9%

*Sample size is under 100; use caution when interpreting data for this segment.

Other includes:

- Email scanning
- Hoping AI will confirm anomalies before releasing payment
- Used a third-party company for email scanning

Reasons Organizations Have Not Implemented AI to Enhance Fraud Controls

As noted earlier, few organizations have taken steps to implement AI to prevent fraud. The reasons for reluctance are varied. Survey respondents note a variety of reasons to explain why their employers are not using AI to mitigate fraud.

- **Immaturity and risk concerns:** Many organizations view AI as an emerging or unproven technology. They are cautious due to perceived risks, the need for human oversight, and uncertainty about its effectiveness in fraud prevention.
- **Lack of knowledge and awareness:** There is widespread uncertainty about available AI tools, use cases, and how to implement them. Some organizations are simply unaware of relevant solutions or have not yet explored the technology.
- **Resource and cost constraints:** Limited IT resources, staff bandwidth, and financial constraints are major barriers. Many cite high costs – both for acquisition and training – as reasons for delay.
- **Competing priorities and organizational readiness:** Other projects and priorities often take precedence. Some organizations are in early exploratory or planning stages, while others are waiting for AI technology to mature or become more widely adopted.
- **Technical limitations:** Outdated systems, lack of infrastructure, and decentralized software environments hinder the implementation of AI solutions.
- **Executive and cultural hesitation:** Resistance to change, lack of executive support, and concerns about privacy or industry regulations (e.g., government contractor restrictions) slow adoption.
- **Existing controls and low perceived need:** Some organizations believe their current fraud controls are sufficient or that their volume of payments and fraud incidents does not justify AI investment.
- **Reliance on third parties:** Several organizations depend on their banks or vendors for fraud prevention, assuming that those partners are already leveraging AI technologies on their behalf.

Overall, the lack of AI adoption for fraud mitigation is typically due to a combination of technological, financial, organizational and strategic factors rather than outright resistance to innovation.

MEASURES FOR IMPROVING FRAUD CONTROL

Measures Taken in 2025 to Improve Fraud Control

To stay ahead of fraudsters, organizations have to ensure they are enhancing measures to safeguard against fraud and be less vulnerable to attacks. In 2025, organizations implemented a broad range of measures to strengthen payments fraud controls, focusing on governance, technology, process improvements and employee training. Key initiatives included:

- **Enhanced internal controls:** Organizations improved segregation of duties and approval workflows, ensuring multiple reviews and sign-offs for payment transactions. This included dual and multi-level authorization, especially for higher-value payments.
- **Vendor verification and validation:** Companies adopted stricter vendor verification processes, such as call-back procedures to known contacts, use of third-party services for bank account validation, and requiring vendors to confirm previous transactions or supply additional information before processing changes.
- **Reduction of check usage:** Many organizations actively reduced or phased out the use of paper checks, moving towards ACH and other electronic payments to minimize the risk associated with check fraud.
- **Adoption of advanced technologies:** There was increased implementation of fraud detection and prevention tools, including AI and machine learning modules, automated treasury management systems, positive payee services, and enhanced system monitoring for suspicious activities.
- **Employee training and awareness:** Regular and targeted fraud and cybersecurity training programs were delivered, with emphasis on identifying fraudulent emails (phishing), business email compromise (BEC) scams and proper escalation protocols. Some organizations conducted testing and awareness campaigns to reinforce vigilance.
- **Policy and procedure updates:** Internal control policies and procedures were updated and aligned with current regulations and industry best practices. Routine internal and external audits were conducted to assess and enhance fraud controls.
- **Collaboration with banking partners:** Organizations worked closely with banks to implement available fraud controls such as ACH positive pay, debit blocks, account validation services and payment automation solutions.
- **Increased monitoring and automation:** Enhanced daily reconciliation, automated review of emails, and continuous monitoring of payment systems helped in the early detection of anomalies and potential fraud attempts.
- **Ongoing education and communication:** Internal communication channels were used to disseminate information on new fraud trends and ensure all staff remained informed about evolving threats and prevention strategies.

Overall, the measures taken in 2025 reflect a proactive and multi-layered approach, combining technology, process rigor and human vigilance to mitigate payment fraud risks across organizations.

MEASURES FOR IMPROVING FRAUD CONTROL CONTINUED

Recommended Further Improvements for Payments Fraud Controls in 2026

Respondents recommend that to continue strengthening payments fraud controls in 2026, they would like their employers to consider advancing their existing measures with the following targeted improvements:

1. Expand Real-Time Fraud Detection and Response

- Implement real-time monitoring across all payment channels, leveraging AI and machine learning to flag unusual patterns instantly.
- Automate alerts and escalation protocols to ensure immediate investigation and response to suspicious activity.
- Integrate fraud detection tools directly with ERP and treasury systems for seamless oversight and faster action.

2. Strengthen Vendor Onboarding and Change Controls

- Require multi-factor authentication and biometric verification for all vendor onboarding and banking information changes.
- Adopt secure vendor portals that enforce encrypted communications and documentation for sensitive account updates.
- Increase periodic audits of vendor databases, cross-referencing with external validation services to eliminate outdated or fraudulent records.

3. Advance Employee Training and Simulation

- Introduce AI-powered fraud awareness simulations tailored to specific roles (e.g., Accounting, Treasury, AP/AR).
- Implement quarterly mandatory training updates, including real-world case studies and interactive phishing tests.
- Develop a centralized repository for reporting suspected fraud attempts and sharing best practices across teams.

4. Enhance Payment Method Security

- Accelerate migration away from checks to fully digital payment platforms, with comprehensive controls for ACH, wire and card transactions.
- Adopt tokenization and end-to-end encryption for all payment data transmissions.
- Utilize blockchain-based payment verification for high-value or international transactions to ensure authenticity and traceability.

5. Deepen Collaboration and Information Sharing

- Establish formal partnerships with financial institutions to access shared fraud intelligence and participate in industry-wide threat alert networks.
- Regularly review and update fraud control protocols in collaboration with banking partners, leveraging new tools and services as they become available.
- Join multi-company forums to exchange information on emerging fraud tactics and successful prevention strategies.

CONCLUSION

Payments fraud continues to affect a large proportion of organizations, even as efforts to strengthen controls and prevention measures persist. While there has been a modest downward trend in the number of reported fraud incidents, the overall rate remains elevated compared to previous years. Most organizations experienced similar levels of fraud in 2025 as before, although some report increases or decreases in activity.

Traditional payment methods such as checks and ACH debits are most frequently targeted, with checks being especially vulnerable. Financial losses due to payments fraud remain a significant concern, and many organizations report experiencing these losses within a range that is notable but not extreme. Treasury departments are most often responsible for detecting both attempted and actual fraud, but Accounts Payable, banks, vendors and other operational teams also play important roles in identifying and responding to incidents.

Managing payments fraud involves more than just detection; it requires coordinated efforts in reporting, response and recovery. These responsibilities are typically concentrated in Treasury, but effective management depends on collaboration across multiple departments including Risk, Legal, Technology and specialized fraud teams.

Business email compromise remains the most common threat, but organizations also report fraud involving tactics such as forged checks, stolen cards and identity theft. Other threats include manipulated payment instructions, invoice fraud and various forms of interference, including those from postal services. Less frequent but still concerning are attacks involving imposters, spoofed communications, QR codes, ransomware, insiders and organized crime.

Deepfake technology has not yet had a widespread direct impact on payment systems, although some organizations have encountered attacks using audio impersonation or, less often, video or image manipulation. Email- and phone-based fraud attempts have increased, especially among larger organizations with more complex payment operations.

Despite the high risk of fraud, checks remain a commonly used payment method, especially for smaller transactions or in environments where alternatives are limited by partner requirements, regulatory constraints or legacy systems. The continued reliance on checks underlines the need for comprehensive, adaptive fraud prevention strategies that address both traditional and emerging threats.

Most organizations have been slow to adopt AI for fraud prevention, with only a minority of surveyed practitioners relying on artificial intelligence to combat fraud. Organizations that use AI to fight payments fraud have observed greater efficiency in fraud reporting, improved abilities to detect deepfake technology, and enhanced real-time identification of threats. The advantages of adopting AI are clear, yet wider implementation is needed for organizations to fully benefit from these improvements.

In summary, payments fraud remains a persistent and evolving challenge for organizations, demanding both ongoing vigilance and adaptive strategies. While progress has been made in reducing incident rates and strengthening controls, the continued prevalence of fraud – especially through traditional methods like checks and ACH debits, via business email compromise and newer threats such as deepfake technology – underscores the importance of a multi-layered, cross-functional approach. Organizations should set clear policies for standard payment turnaround times: time can work both for and against a fraudster. Allowing more time before making a payment can help prevent fraud, while immediate or emergency payments should be closely examined. As payment systems and fraud tactics grow more complex, organizations must prioritize collaboration across departments and invest in robust prevention, detection, and recovery efforts to safeguard their financial operations and maintain trust in their payment processes.

DEMOGRAPHICS

ABOUT THE SURVEY PARTICIPANTS

In January 2026, the Research Department of the Association for Financial Professionals (AFP®) distributed the survey to 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 465 responses were received from practitioners, which form the basis of the report.

AFP thanks Truist® for underwriting the *2026 AFP® Payments Fraud and Control Survey*. Responsibility for the survey questionnaire, as well as the final report and its content and conclusions, rests solely with the AFP Research Department. The tables below present a profile of the survey respondents, including the payment types they use and accept.

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

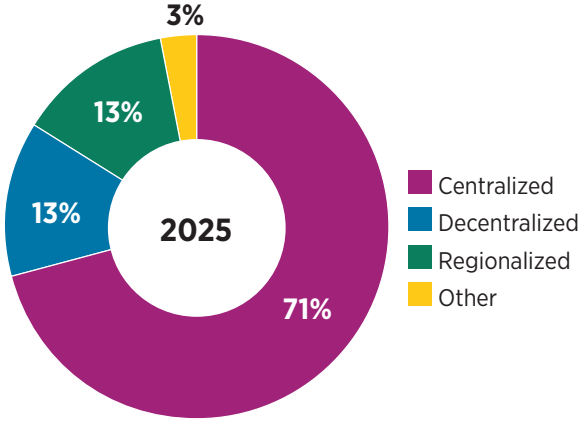
	PRIMARILY CONSUMERS	SPLIT BETWEEN CONSUMERS AND BUSINESSES	PRIMARILY BUSINESSES
When making payments	4%	27%	69%
When receiving payments	16%	33%	51%

Number of Payment Accounts Maintained
(Percentage Distribution of Organizations)

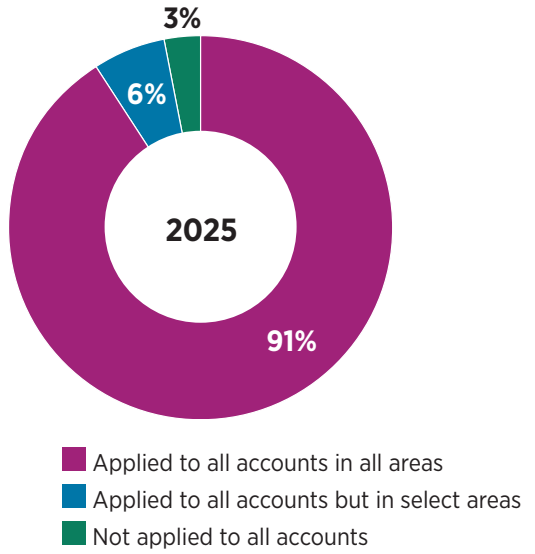
	2025	ANNUAL REVENUE LESS THAN $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION AND FEWER THAN 26 PAYMENT ACCOUNTS	ANNUAL REVENUE AT LEAST $1 BILLION AND MORE THAN 100 PAYMENT ACCOUNTS *
Fewer than 5	25%	34%	20%	34%	--
5-9	17%	19%	16%	28%	--
10-25	18%	13%	21%	37%	--
26-50	9%	12%	8%	--	--
51-100	9%	8%	10%	--	--
More than 100	22%	15%	25%	--	100%

*Sample size is under 100; use caution when interpreting data for this segment.

Methods to Maintain Payments Accounts
(Percentage Distribution of Organizations)

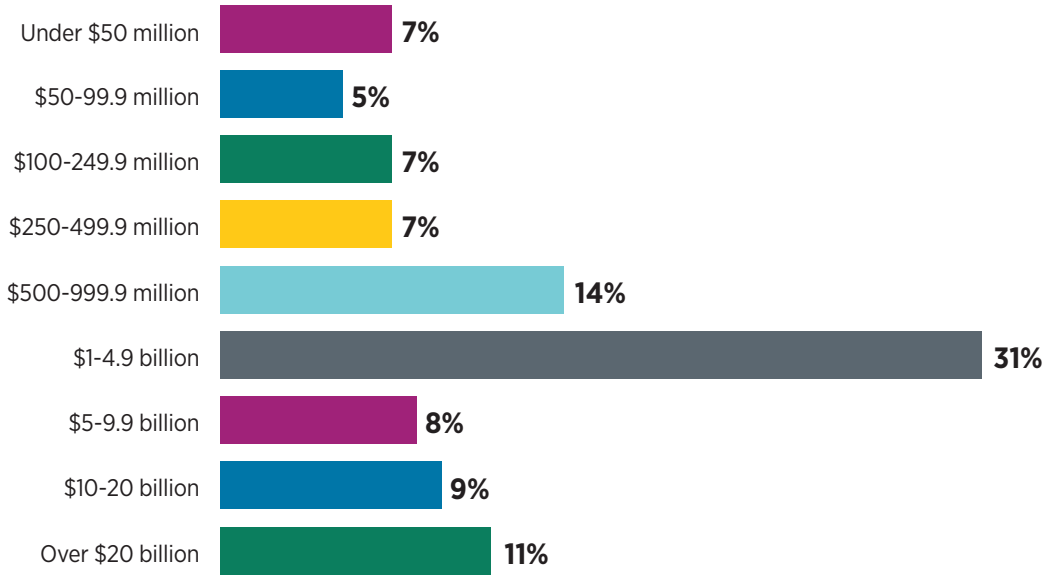


Application of Account Controls
(Percentage Distribution of Organizations)



Annual Revenue (USD)

(Percentage Distribution of Organizations)



Organization's Ownership Type

(Percentage Distribution of Organizations)

	2025	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	34%	14%	47%	42%	50%
Privately held	45%	61%	34%	34%	40%
Nonprofit (not-for-profit)	14%	17%	11%	16%	4%
Government (or government-owned entity)	8%	9%	7%	8%	6%

*Sample size is under 100; use caution when interpreting data for this segment.

Industry Classification

(Percentage Distribution of Organizations)

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

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.financialprofessionals.org

2026 AFP® Payments Fraud and Control Survey Report
Copyright©2026 by the Association for Financial Professionals® (AFP).
All Rights Reserved.

This work is intended solely for the personal and noncommercial use of the reader. All other uses of this work, or the information included therein, is strictly prohibited absent prior express written consent of the Association for Financial Professionals. The *2026 AFP® Payments Fraud and Control Survey Report* and the information included therein, may not be reproduced, publicly displayed, or transmitted in any form or by any means, electronic or mechanical, including but not limited to photocopy, recording, dissemination through online networks or through any other information storage or retrieval system known now or in the future, without the express written permission of the Association for Financial Professionals. In addition, this work may not be embedded in or distributed through commercial software or applications without appropriate licensing agreements with the Association for Financial Professionals.

Each violation of this copyright notice or the copyright owner's other rights, may result in legal action by the copyright owner and enforcement of the owner's rights to the full extent permitted by law, which may include financial penalties of up to $150,000 per violation.

This publication is **not** intended to offer or provide accounting, legal or other professional advice. The Association for Financial Professionals recommends that you seek accounting, legal or other professional advice as may be necessary based on your knowledge of the subject matter.

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@financialprofessionals.org
Web: www.financialprofessionals.org

TRUIST

Keep your organization safer.

Get custom fraud solutions built for your business.

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

Talk to us about custom fraud solutions that are built for simplicity, speed and safety.

Truist.com/FraudProtection

© 2026 Truist Financial Corporation. TRUIST, the Truist logo and Truist Purple are service marks of Truist Financial Corporation. All rights reserved.