ASSOCIATION FOR FINANCIAL PROFESSIONALS

2026 AFP®

PAYMENTS FRAUD AND CONTROL SURVEY REPORT

Key Highlights

Underwritten by TRUIST

2026 AFP®

PAYMENTS FRAUD AND CONTROL SURVEY REPORT

Key Highlights

April 2026

This summary report includes highlights from the comprehensive *2026 AFP® Payments Fraud and Control Survey Report*. The comprehensive report comprising all findings and detailed analysis is exclusively available to AFP members.

Learn more about AFP membership.

Purchase the 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

TOPICS COVERED IN THE COMPREHENSIVE 2026 AFP® PAYMENTS FRAUD AND CONTROL SURVEY REPORT

PAYMENTS FRAUD OVERVIEW

- Payments Fraud Trends
- Payment Methods Impacted By Fraud
- Recovering Lost Funds
- Detecting Fraud Activity
- Sources Of Fraud
- Impact Of Deepfake Technology On Payment Systems
- Payments Fraud Experiences At Organizations

IMPOSTER FRAUD

- Impact Of Types Of Imposter Fraud
- Business Email Compromise (BEC)
- Fraud Via Organizations' Cell Phones/Phone Calls
- Key Perpetrators Of Fraud
- Payment Methods Used In Imposter Scams
- Departments Vulnerable To Imposter Fraud

CHECK USAGE

- Checks Continue To Be Issued Extensively

PAYMENTS AND FRAUD CONTROLS

- Business Email Compromise Prevention
- Check Fraud Controls
- ACH Debit Fraud And Controls
- Impact Of Artificial Intelligence (AI) On Payments Fraud Controls
- Measures For Improving Fraud Control

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.

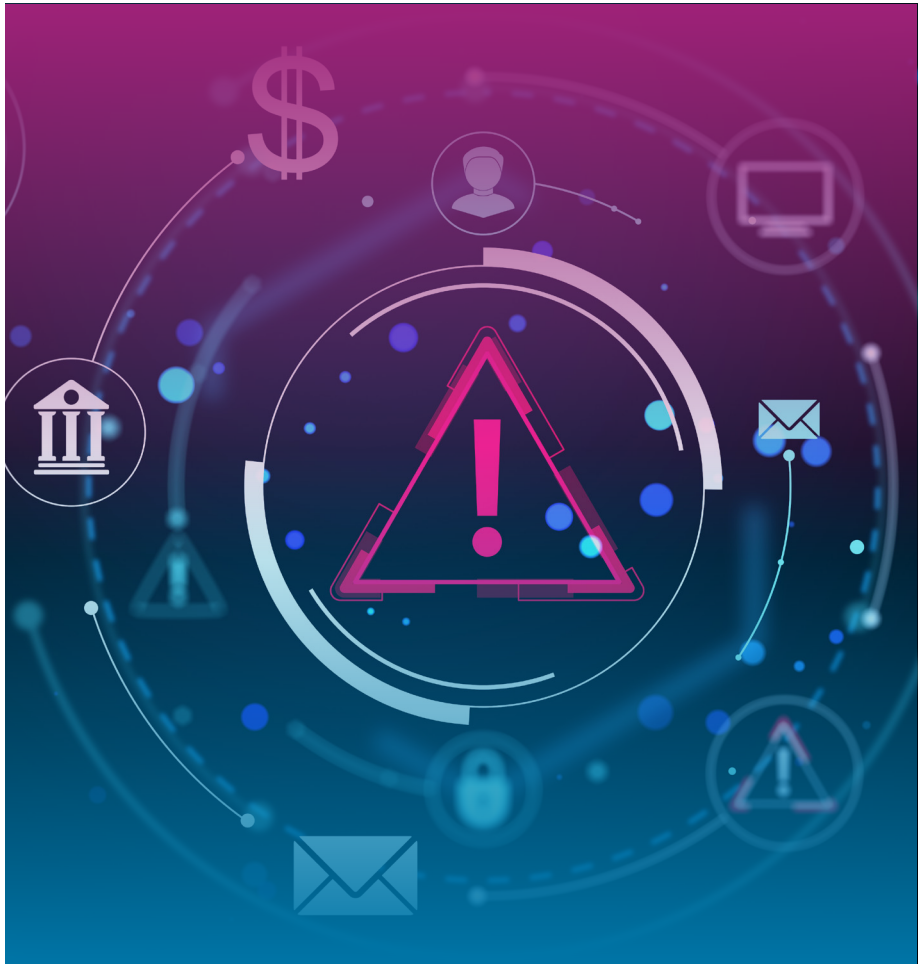
Businesses remain vulnerable to fraudulent activities, and those scams originating via email such as business email compromise (BEC) are widespread. Given the large volume of correspondence conducted via email, this channel is frequently exploited by fraudsters posing as vendors or employees to deceive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

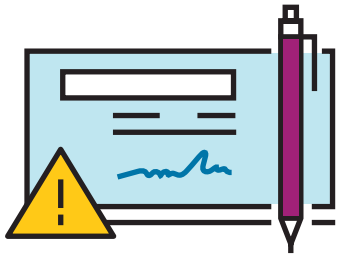
AFP® thanks Truist® for its underwriting support of the *2026 AFP® Payments Fraud and Control Survey*. Both questionnaire design and the final report, along with its content and conclusions, are the sole responsibilities of AFP's Research Department.

KEY FINDINGS

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

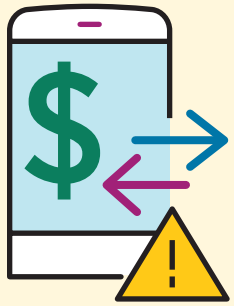
Few organizations (17%) report using AI to combat payments fraud. While adoption is higher among large organizations – i.e., those with annual revenue of at least $1 billion – most respondents cite immaturity of technology, cost and reliance on existing controls or banking partners as reasons for limited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

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



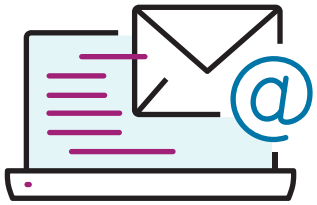
Despite declining fraud activity via their use, checks continue to be the most-often targeted method for fraud, reported by 58% of organizations in 2025 – outpacing fraud via ACH debits (30%) and wire transfers (25%). Check usage continues to be widespread; 68% of companies use checks for vendor payments 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 TRENDS

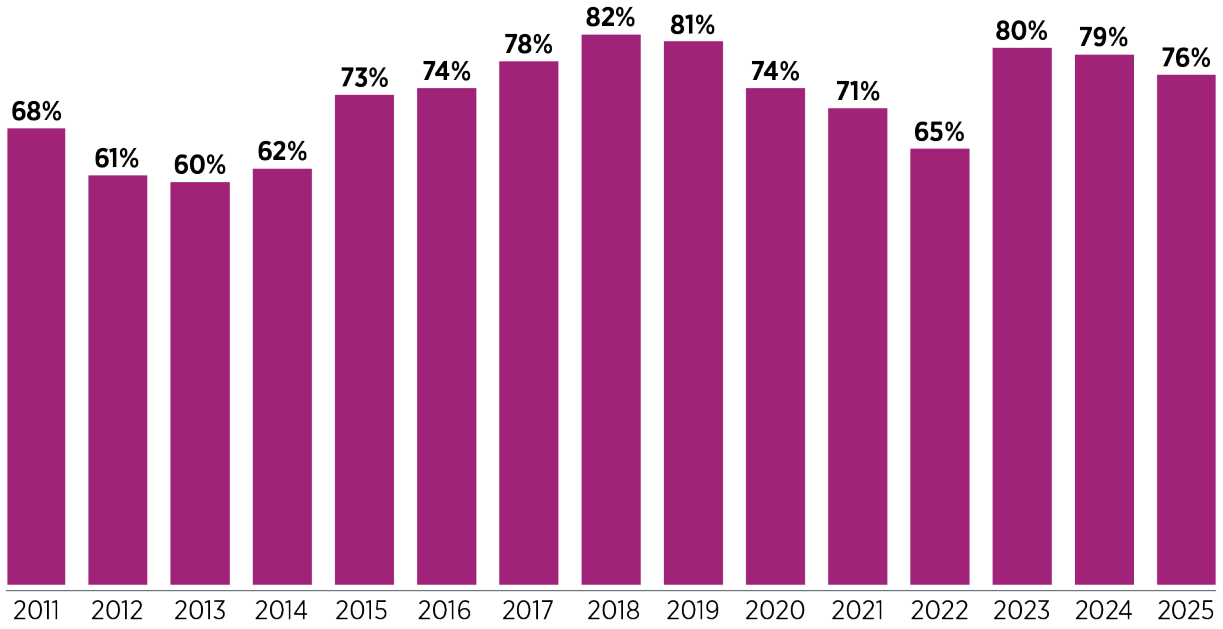
Payments Fraud Attacks on Organizations Continue to Be Elevated

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.

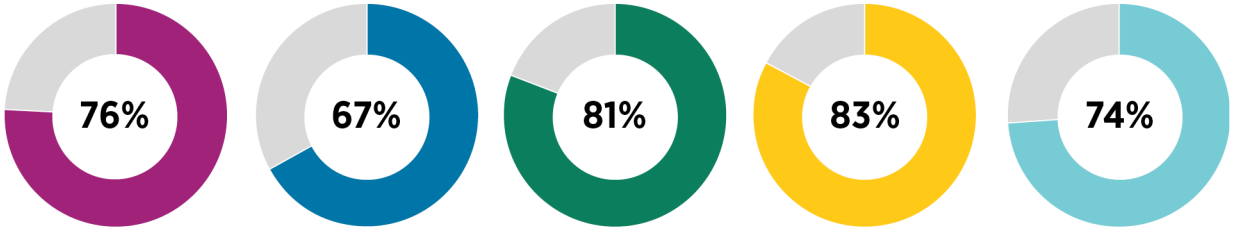
Larger organizations – defined as those with annual revenue of at least $1 billion – report higher exposure to payments fraud; 81% experienced an attack compared with 67% of organizations with less than $1 billion in annual revenue. Organizations with annual revenue of at least $1 billion and fewer than 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.

PAYMENT METHODS IMPACTED BY FRAUD

Checks and ACH Debits Remain Most Susceptible to Payments Fraud

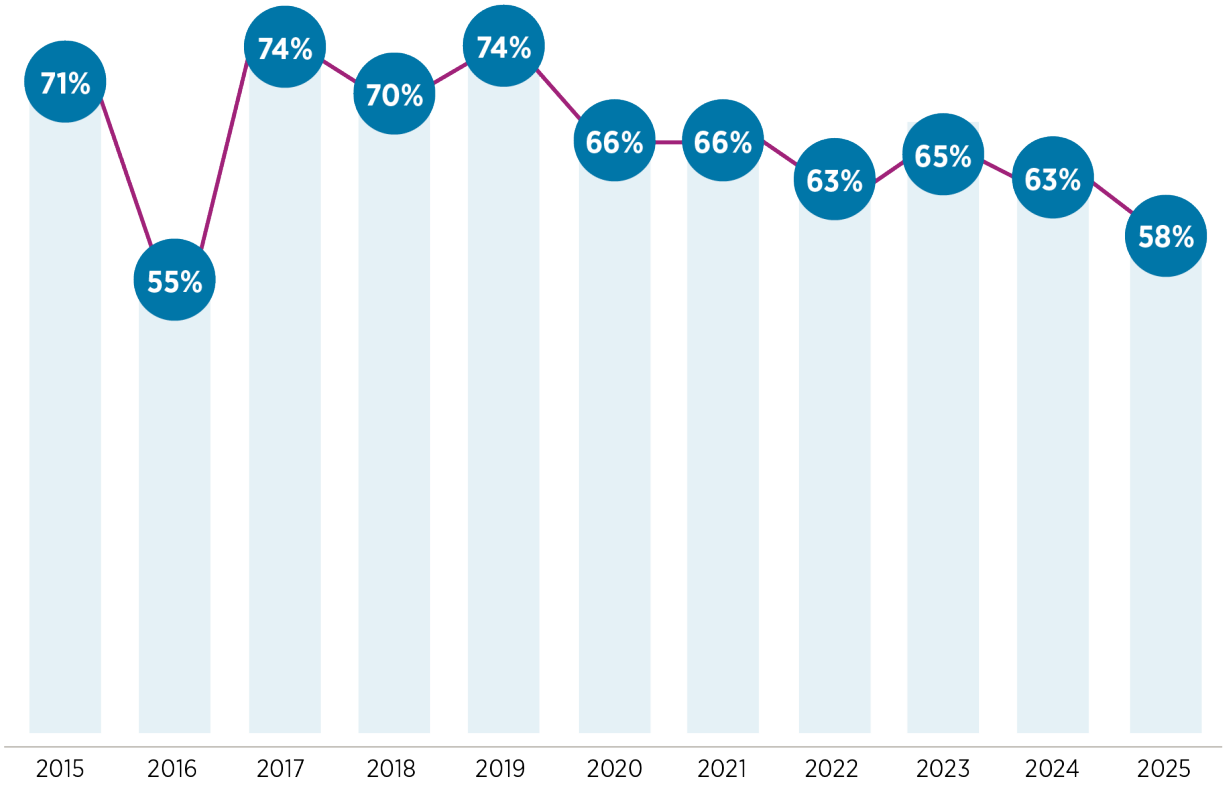
In 2025, checks and ACH debits remained the payment methods most impacted by fraud activity. Checks were the most frequently reported payment method subject to fraud (58% of organizations), followed by ACH debits (30%) and wire transfers (25%). Corporate/commercial credit cards (21%) and ACH credits (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.

Check Fraud Activity: Trends
(Percent of Organizations)



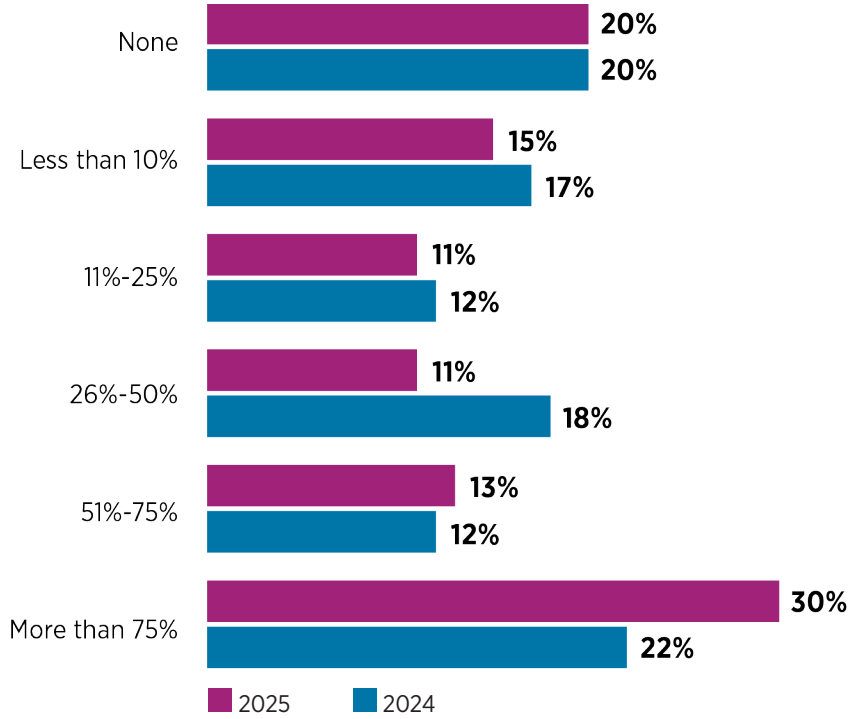
RECOVERING LOST FUNDS

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.

SOURCES OF FRAUD

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

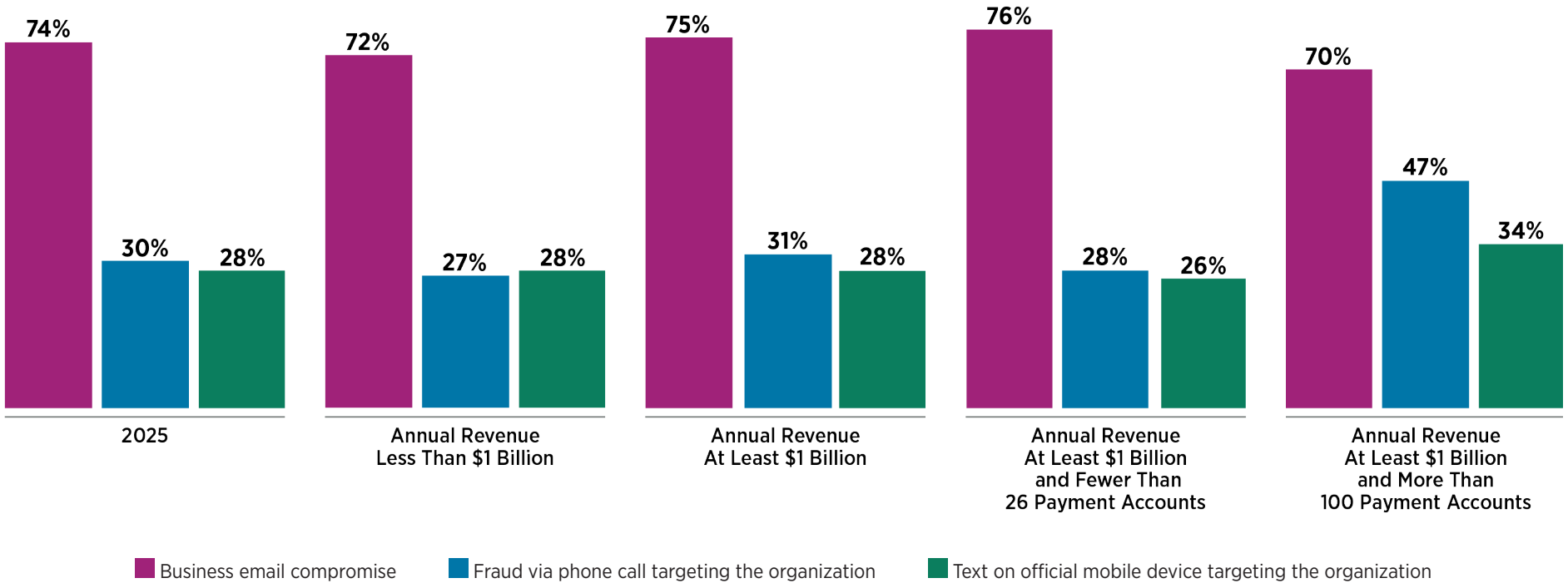
IMPACT OF TYPES OF IMPOSTER FRAUD

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)



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.

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%

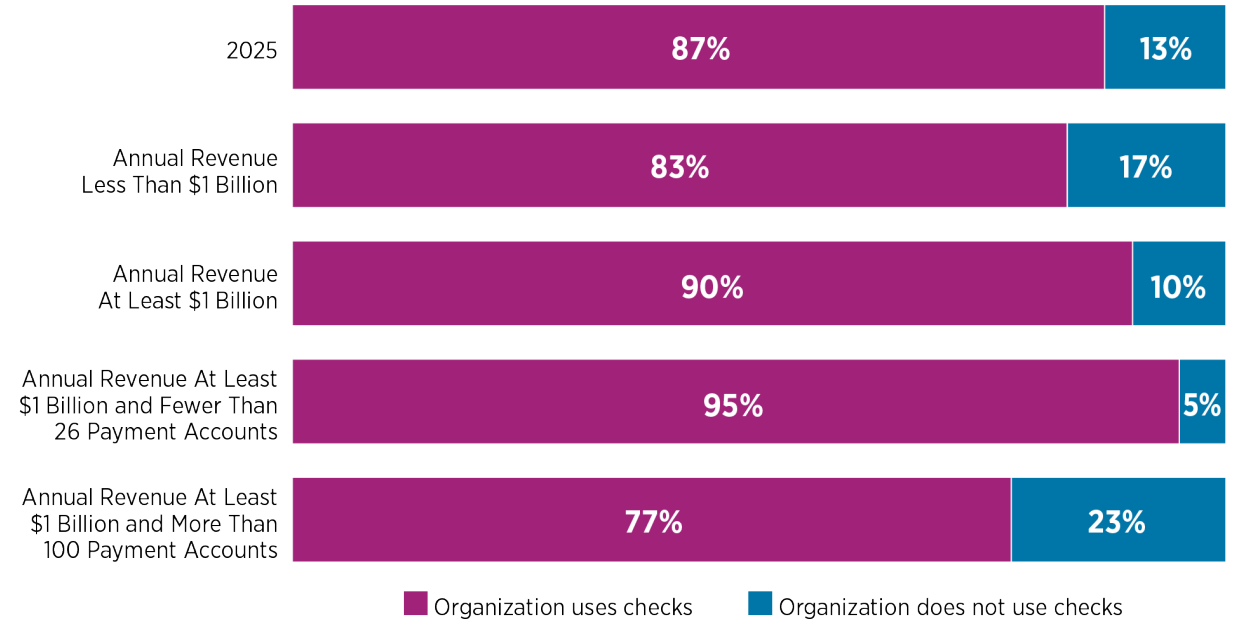
CHECKS CONTINUE TO BE ISSUED EXTENSIVELY

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%

BUSINESS EMAIL COMPROMISE PREVENTION

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%

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

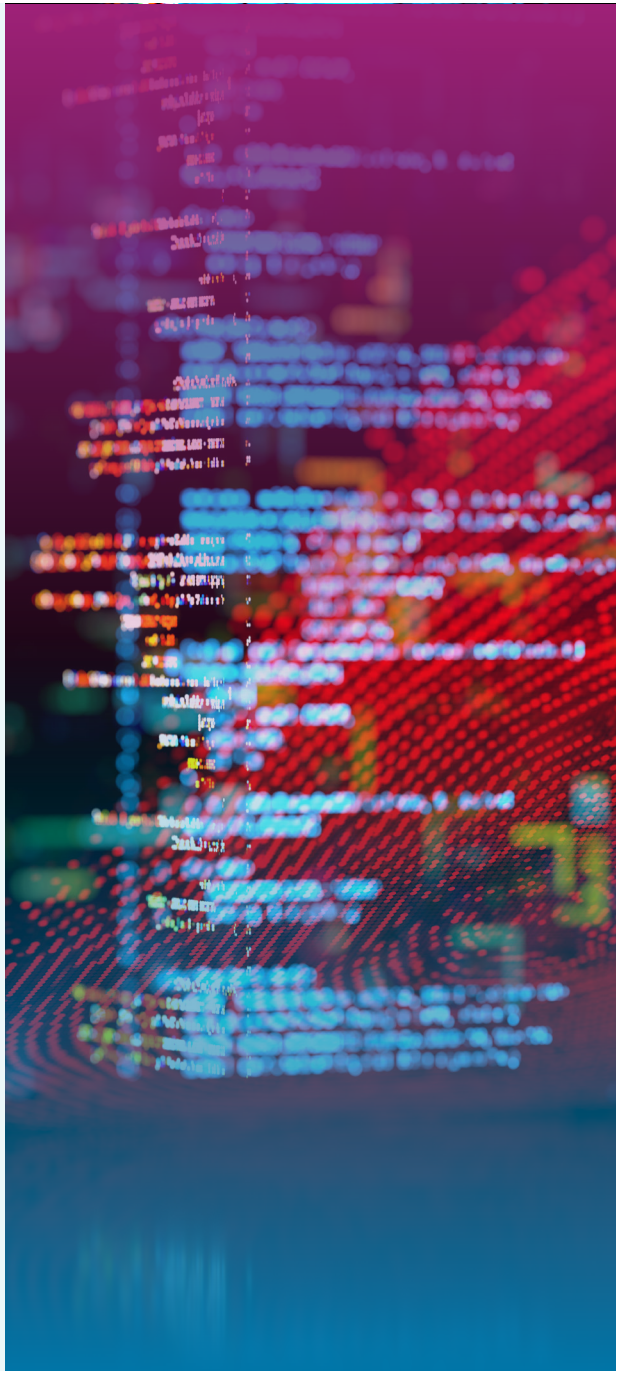
March 17, 2028

- 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.)



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.

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)

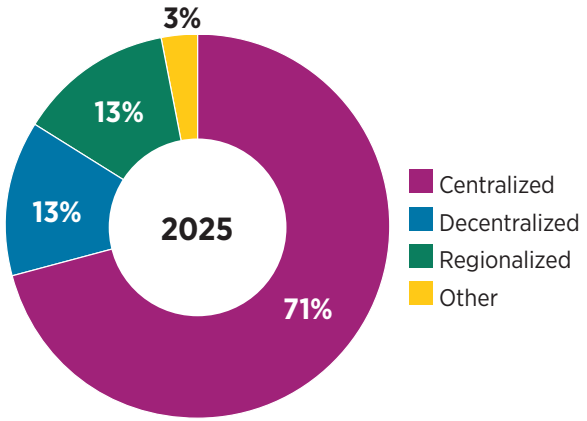
	PRIMARILY CONSUMERS	SPLIT BETWEEN CONSUMERS AND BUSINESSES	PRIMARILY BUSINESSES
When making payments	4%	27%	69%
When receiving payments	16%	33%	51%

Number of Payment Accounts Maintained
(Percentage Distribution of Organizations)

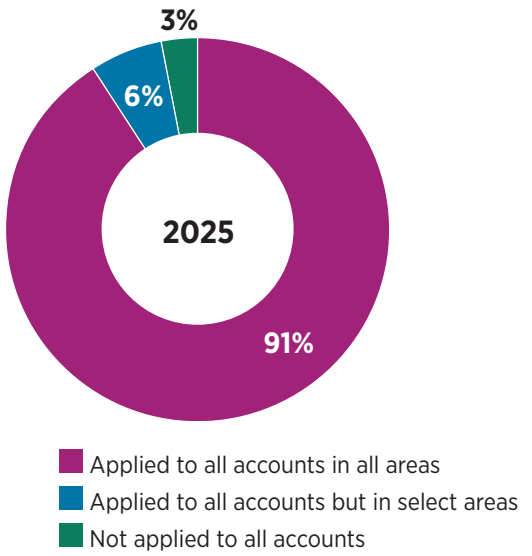
	2025	ANNUAL REVENUE LESS THAN $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION AND FEWER THAN 26 PAYMENT ACCOUNTS	ANNUAL REVENUE AT LEAST $1 BILLION AND MORE THAN 100 PAYMENT ACCOUNTS *
Fewer than 5	25%	34%	20%	34%	--
5-9	17%	19%	16%	28%	--
10-25	18%	13%	21%	37%	--
26-50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

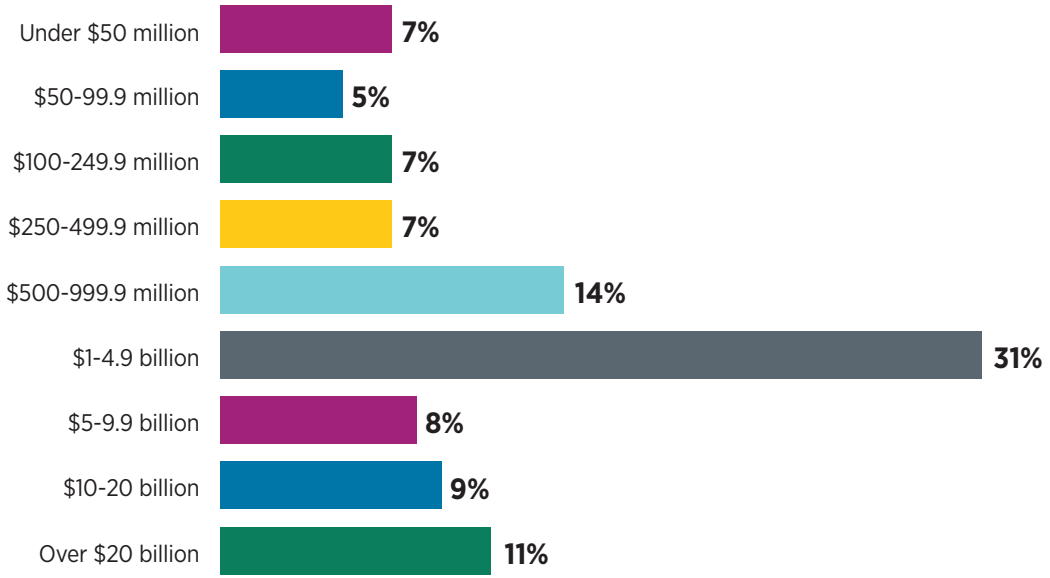


Application of Account Controls
(Percentage Distribution of Organizations)



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

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