September 2026 Report

PREVENTION **FIRST**

Building a Smarter Defense Against Payments Fraud

PYMNTS INTELLIGENCE | Bottomline

PREVENTION FIRST

Building a Smarter Defense Against Payments Fraud

PYMNTS INTELLIGENCE | Bottomline

Prevention First: Building a Smarter Defense Against Payments Fraud was produced in collaboration with Bottomline, and PYMNTS Intelligence is grateful for the company's support and insight. PYMNTS Intelligence retains full editorial control over the following findings, methodology and data analysis.

TABLE OF CONTENTS

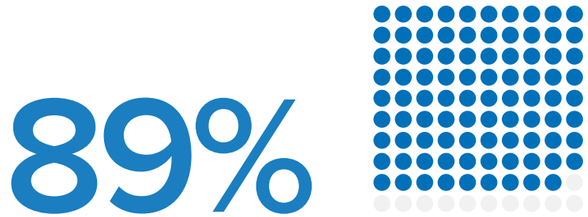
WHAT'S **AT STAKE**

An email lands in a finance team's inbox while the CFO is on vacation. It asks for a wire transfer to a new supplier account. While the request looks routine and the tone sounds right, the receiving account doesn't match the vendor's history. The right fraud protection tools can catch that kind of mismatch before anyone sends a payment.

In an ideal world, the fraud attempt fails without the finance team even noticing how close it came to succeeding.

As artificial intelligence makes vendor impersonation and business email compromise (BEC) fraud attempts more convincing, organizations are confronting a broader challenge: how to prevent fraudulent payment requests from going through while at the same time reducing the operational burden of protecting legitimate payments. **Half of firms say scam emails are the AI-enabled fraud tactic they encounter most often, while 89% of finance leaders say verifying vendors is a moderate or major burden.** At the same time, payments via paper checks remain a disproportionate source of exposure: 35% of firms report experiencing check fraud.

Today, effective fraud prevention requires investing in everything from payment modernization to vendor validation to building a full stack of AI-powered defense tools. The key is to build a payment environment that prevents fraud earlier and continuously adapts as threats evolve, all while improving operational efficiency.



of finance leaders

call verifying vendors before payment or onboarding a moderate or major burden.

These are just some of the findings detailed in Prevention First: Building a Smarter Defense Against Payments Fraud, a PYMNTS Intelligence and Bottomline collaboration. The report examines how organizations can build a fraud prevention strategy around payment modernization, supplier verification and layered controls, with AI as a key part of that stack. It draws on insights from a survey of 150 U.S. treasury and finance executives at firms with at least $100 million in annual revenue, fielded July 9–27, 2026.

This is what we learned.

KEY **FINDINGS**

01

THE THREAT LANDSCAPE

AI-written impersonation emails and check fraud exposure are the two biggest threats to outbound payments, and catching them takes a lot of work.

50%

of firms name AI-written vendor impersonation emails as their top threat, and 35% face check fraud.

02

ALL OR NOTHING

Organizations often deploy AI defenses as a full stack, using three or more complementary measures rather than relying on a single tool.

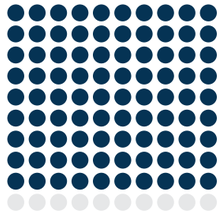
57%

of firms run no AI-powered defense processes at all, while 42% deploy three or more tools as a layered stack.

03

MULTIPRONGED DEFENSE

A full AI toolkit is one part of a successful fraud defense strategy.



90%

of fraud attempts are stopped before any loss occurs for the 6 in 10 firms using 3 or more AI tools.

04

GOOD ENOUGH?

Those that don't use AI fraud tools are holding off because they trust their manual reviews to do the job.

55%

of non-AI users say manual reviews already work well enough, a view they're 89% more likely to hold than AI users.

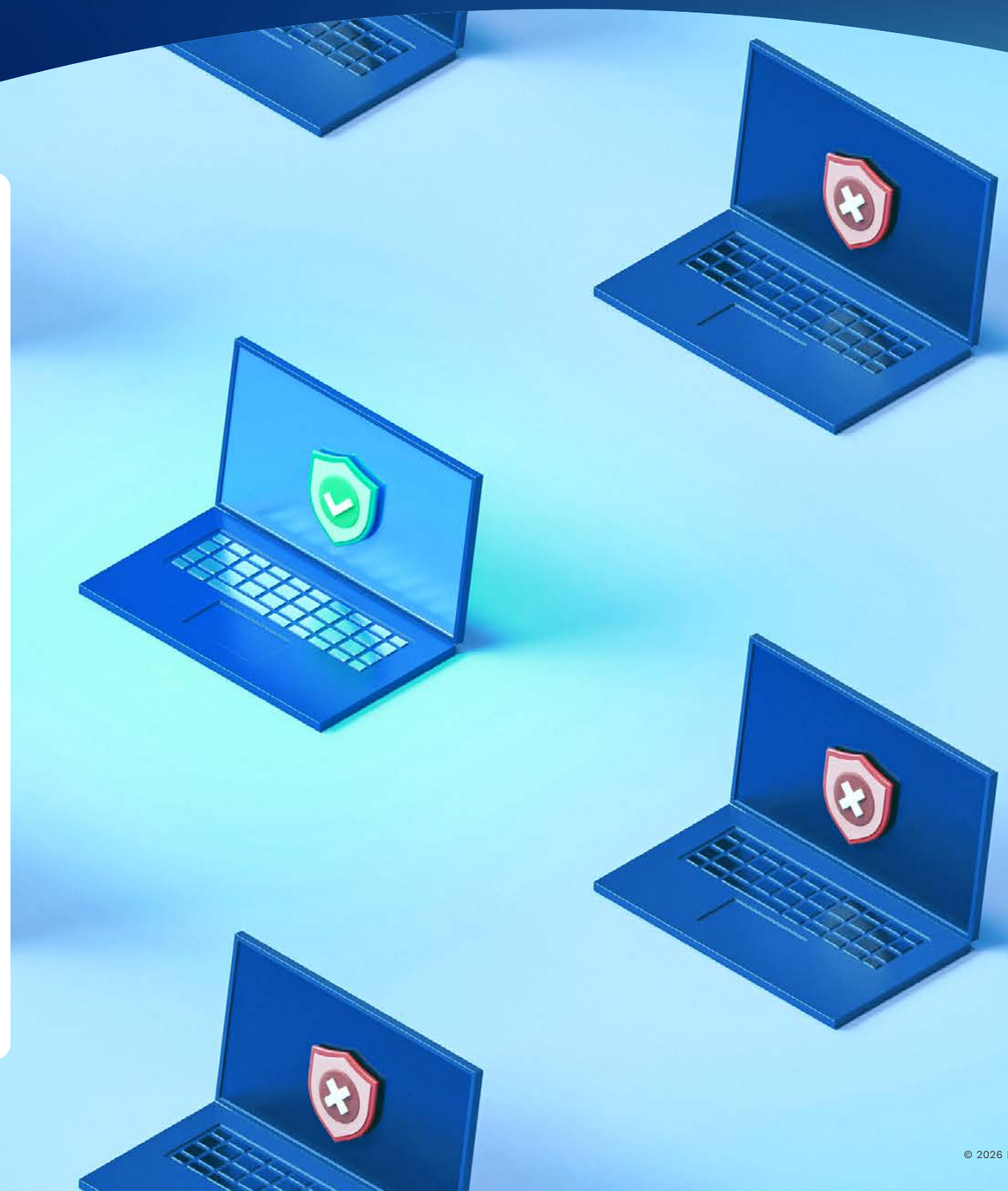
05

MODERNIZATION ROADMAP

Firms are upgrading their AI fraud protection, and even those that have held off until now expect to add these technologies soon.

58%

of non-users say they will implement AI fraud detection within 12 months.



THE FULL STORY

Fraud prevention and payment modernization are often described as two separate initiatives. The findings below suggest they are one story: How a payment gets sent, who gets verified before it goes out and what technology watches over the transaction all shape how exposed an organization is.

AI-written impersonation emails and check fraud exposure are the two biggest threats to outbound payments, and catching them takes a lot of work.

Half of respondents name AI-written scam emails impersonating a vendor as the most common AI-enabled fraud tactic they have encountered in the past year, and 88% say they see these emails at least a few times a year. Nearly one-third, 32%, see business email compromise (meaning a scam email designed to trick an employee into sending money to a fraudster) at least once a month.

Vendor impersonation emails rank as the most common tactic in every sector: tech (50%), services (51%) and goods (48%). Defenses such as account verification and payment controls need to be just as universal.

FIGURE 1:

Share of firms naming each AI-enabled fraud tactic as the one they encounter most often, overall and by industry

AI-enabled fraud tactic	Sample	Tech	Services	Goods
Vendor and supplier impersonation emails	50%	50%	51%	48%
Automated, high-volume attack attempts	15%	5%	12%	22%
AI-generated fabricated documents	14%	20%	16%	9%
AI-generated fake invoices	10%	10%	10%	9%
Synthetic video used to authorize transactions	4%	15%	4%	0%
Synthetic business identities	4%	0%	3%	7%
Fake call from vendor	3%	0%	3%	5%

Source: PYMNTS Intelligence
The Payments Fraud Defense, September 2026
N = 146: Firms reporting an AI fraud tactic, fielded July 9–27, 2026

50%

of firms **encounter emails impersonating vendors and suppliers.**

50%

name AI-written scam emails as the top tactic used by fraudsters.

88%

face AI-scam emails at least a few times a year.

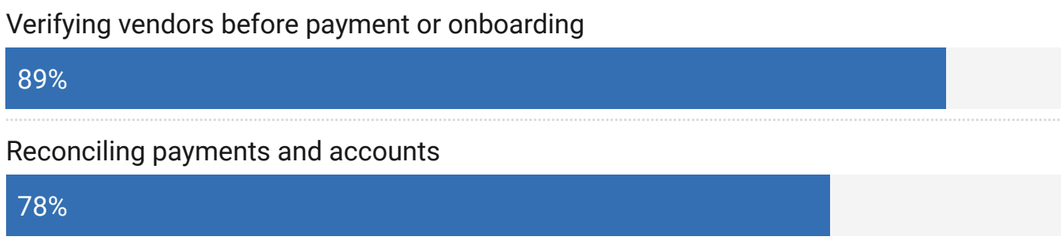
32%

encounter business email compromise at least monthly.

Catching these fraud attempts is hard work, costing firms time and money. Nearly nine in 10 finance leaders call verifying vendors a moderate or major burden. Additionally, nearly eight in 10 say the same of reconciling payments and accounts. These figures don't vary much based on whether a firm has adopted AI, suggesting that better detection tools alone have not been enough to lighten the load. Fraud prevention and operational efficiency are increasingly the same challenge: Every hour spent manually confirming a vendor's bank details is an hour not spent on higher-value work.

FIGURE 2:

Share of finance leaders calling manual payment tasks a moderate or major burden

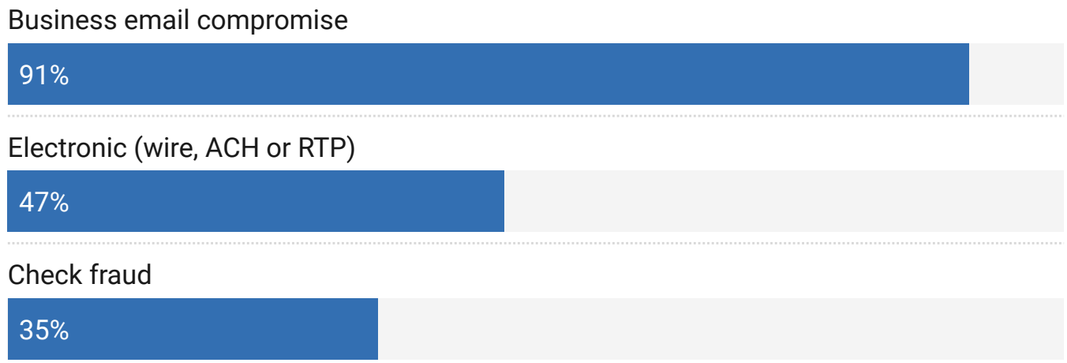


Source: PYMNTS Intelligence
The Payments Fraud Defense, September 2026
N = 150: Whole sample, fielded July 9–27, 2026

Even as firms shift more to electronic payment methods, check fraud continues to be a major issue: 35% of firms report encountering check fraud, and 48% say checks account for at least 10% of their outbound fraud losses. In fact, 15% tie more than one-quarter of fraud losses to checks. This vulnerability suggests that firms should consider reducing reliance on checks and other higher-risk payment methods if they're worried about fraud. Doing so could be as important a strategy as any detection tool layered on top. Payment modernization is one of the most direct ways to fight attacks.

FIGURE 3A:

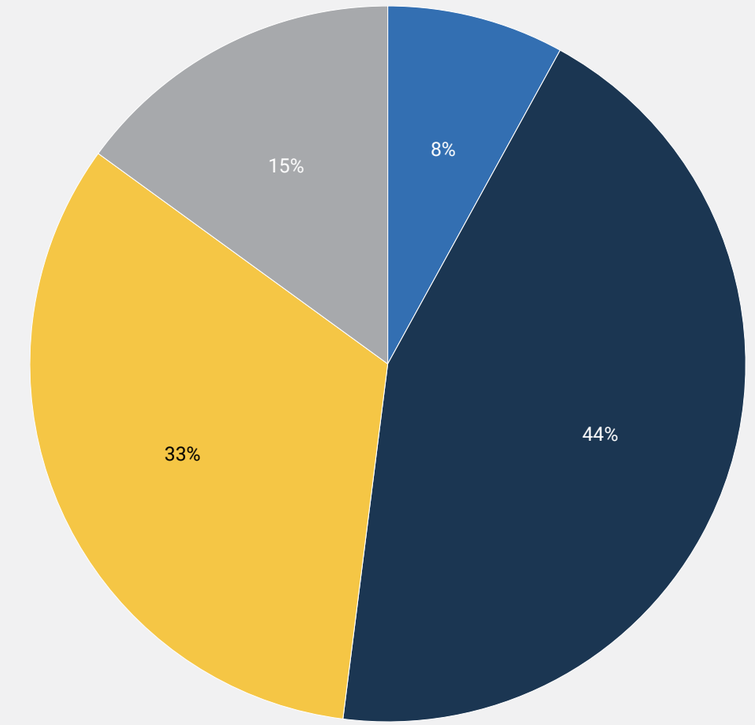
Share of firms experiencing each fraud type



Source: PYMNTS Intelligence
The Payments Fraud Defense, September 2026
N = 150: Whole sample, fielded July 9–27, 2026

FIGURE 3B:

Share of outbound fraud losses tied to checks



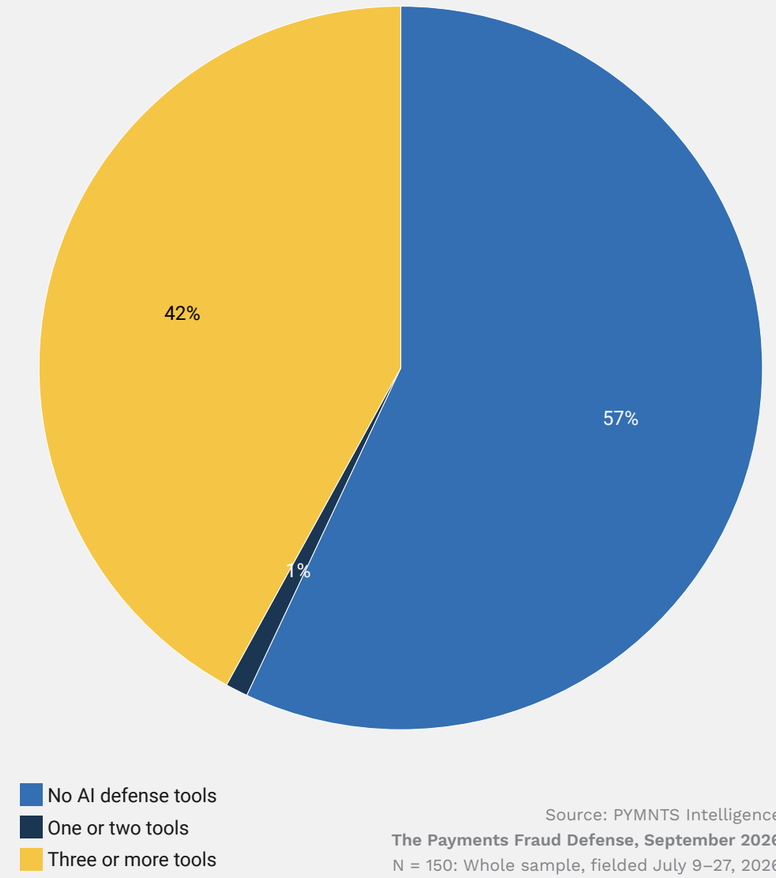
Source: PYMNTS Intelligence
The Payments Fraud Defense, September 2026
N = 150: Whole sample, fielded July 9–27, 2026

Organizations often deploy AI defenses as a full stack, using three or more complementary measures rather than relying on a single tool.

Most firms (57%) run no AI fraud-detection tools, while another 42% deploy three or more tools at once. Just 1% are somewhere in the middle. Firms are taking an all-or-nothing approach to AI fraud defense tools.

Among firms that have adopted AI, the tools they add first are linked to the types of fraud they see most, and many of those defenses double as verification tools. Eighty-three percent of firms deploy real-time predictive risk scoring, meaning software that scores a transaction's fraud risk as it happens, and 82% run automated document verification. Only 26% have implemented deepfake detection. Firms appear to be defending against the text-based threats they already face and building out verification capability alongside detection, rather than treating AI as a single-point solution.

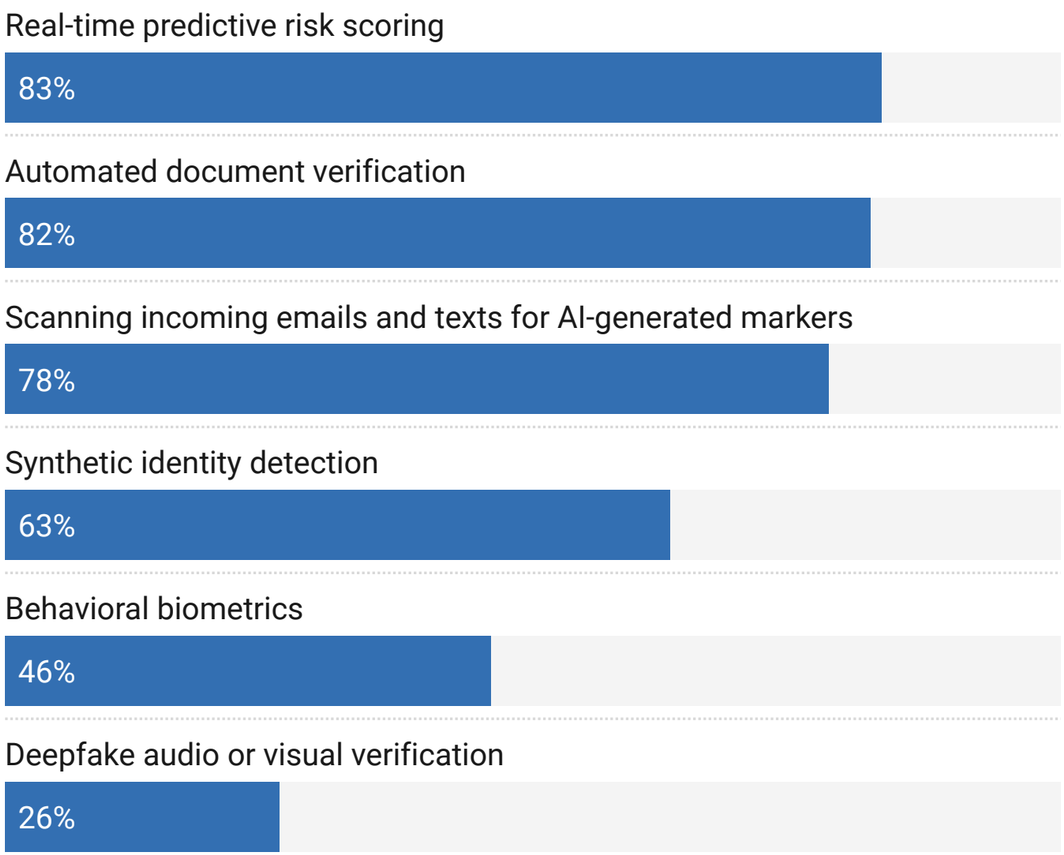
FIGURE 4:
Number of AI fraud-detection tools deployed



Source: PYMNTS Intelligence
The Payments Fraud Defense, September 2026
N = 150: Whole sample, fielded July 9–27, 2026

FIGURE 5:

Where AI fraud-detection users apply AI across their fraud-defense stack

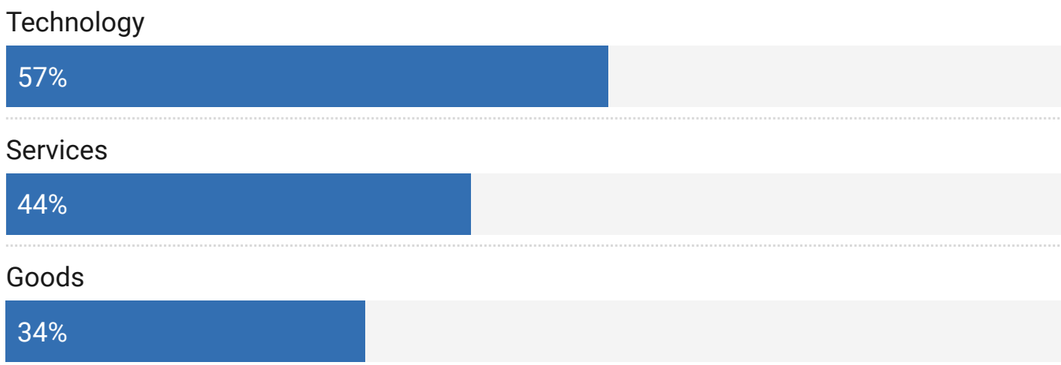


Source: PYMNTS Intelligence
The Payments Fraud Defense, September 2026
N = 65: Firms using AI or machine learning for fraud detection, fielded July 9–27, 2026

Different sectors are running at different speeds. Fifty-seven percent of tech firms run a full toolkit of three or more tools, compared with just 34% in the goods industry. Goods firms also stop the least fraud before loss, at 41%, making the sector the one with the widest gap between the threat it faces and the defense it has built.

FIGURE 6:

Share of firms running a full AI toolkit of three or more fraud-detection tools, by industry



Source: PYMNTS Intelligence
The Payments Fraud Defense, September 2026
N = 150: Whole sample, fielded July 9–27, 2026

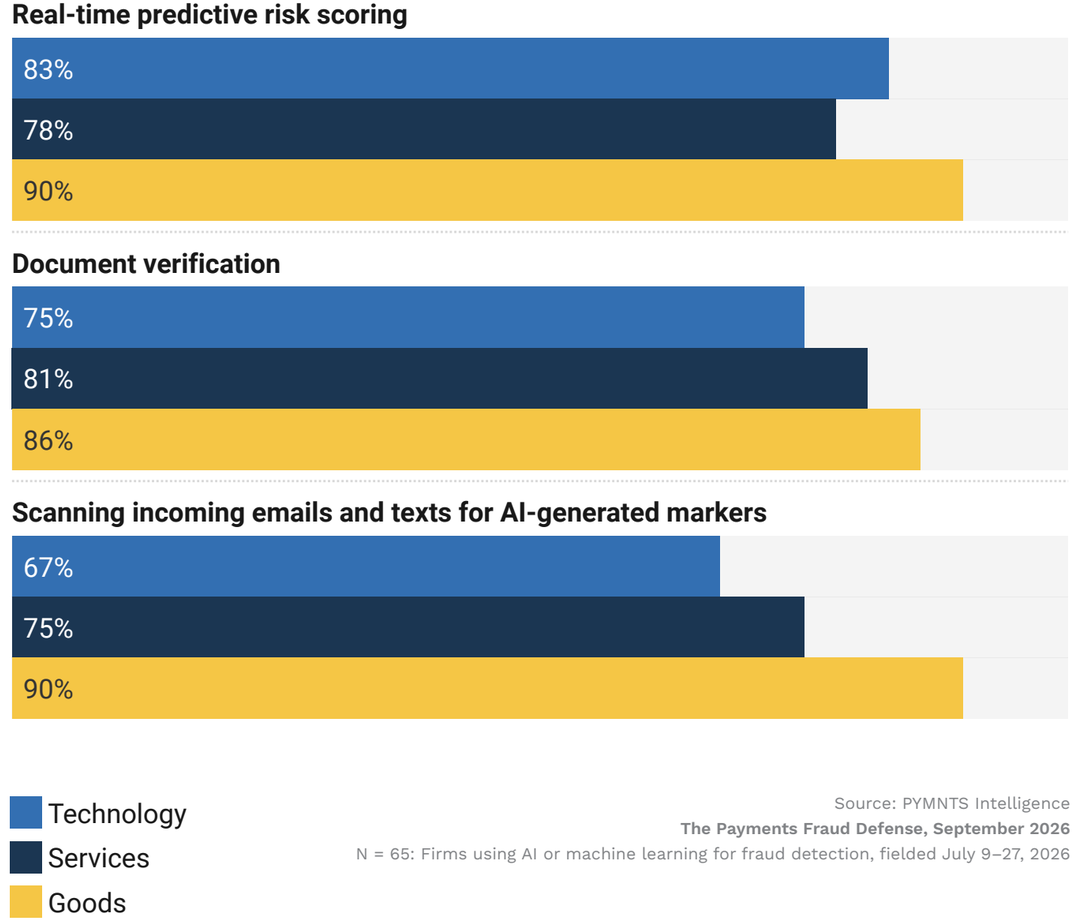
Where firms have adopted AI, the specific tools they favor stay fairly consistent by sector. Tech firms lean hardest on real-time risk scoring (83% of AI users), followed by document verification (75%) and email scanning for AI-generated markers (67%). Services firms flip the order slightly, leading with document verification (81%). Goods firms lean most heavily on real-time risk scoring and email scanning, both at 90%. Across sectors, firms are combining the same core set of tools with the verification processes they already run, rather than treating AI as a standalone fix.

90%

of goods-sector **AI users run both real-time risk scoring and email scanning for AI-generated markers,** the heaviest use of either tool in any sector.

FIGURE 7:

Share of AI fraud-detection users applying each tool, by industry



Source: PYMNTS Intelligence
The Payments Fraud Defense, September 2026
N = 65: Firms using AI or machine learning for fraud detection, fielded July 9–27, 2026

A full AI toolkit is one part of a successful fraud defense strategy.

Catching fraud attempts rarely comes down to AI working alone. One firm caught a wire request to a new partner because account validation flagged a mismatch on a request that arrived while the CFO was traveling. Another firm's anomaly monitoring flagged an attempt to reroute an ACH payment after it diverged from a vendor's usual pattern. A third stopped an AI-written email impersonating a vendor by verifying the requested banking details against its trusted supplier records before the payment went out.

Selected examples of AI-enabled payables fraud attempts reported by finance leaders and how each one was caught

Business email compromise asking for a wire transfer to a new partner

"A polished BEC email came in during our CFO's travel window asking for a wire to a new partner. Our ML flagged the payee account, and we caught it."

—Executive of a transportation and logistics company

HAS AI DEFENSE

Attempt to reroute ACH payment

"We detected an attempt to reroute an ACH payment after anomaly monitoring flagged activity that differed from the vendor's normal payment pattern."

—Executive of a transportation and logistics company

HAS AI DEFENSE

Business email compromise impersonating a vendor

"An AI-written email impersonating a vendor requested updated banking information, but our account validation process flagged the change and prevented the payment from being sent."

—Executive of a technology and software company

HAS AI DEFENSE

The six-figure near miss

"A supplier account takeover attempt nearly redirected a six-figure payment, but a mismatch in payment instructions triggered an alert, and we froze the transaction immediately."

—Executive of a wholesale trade company

NO AI DEFENSE

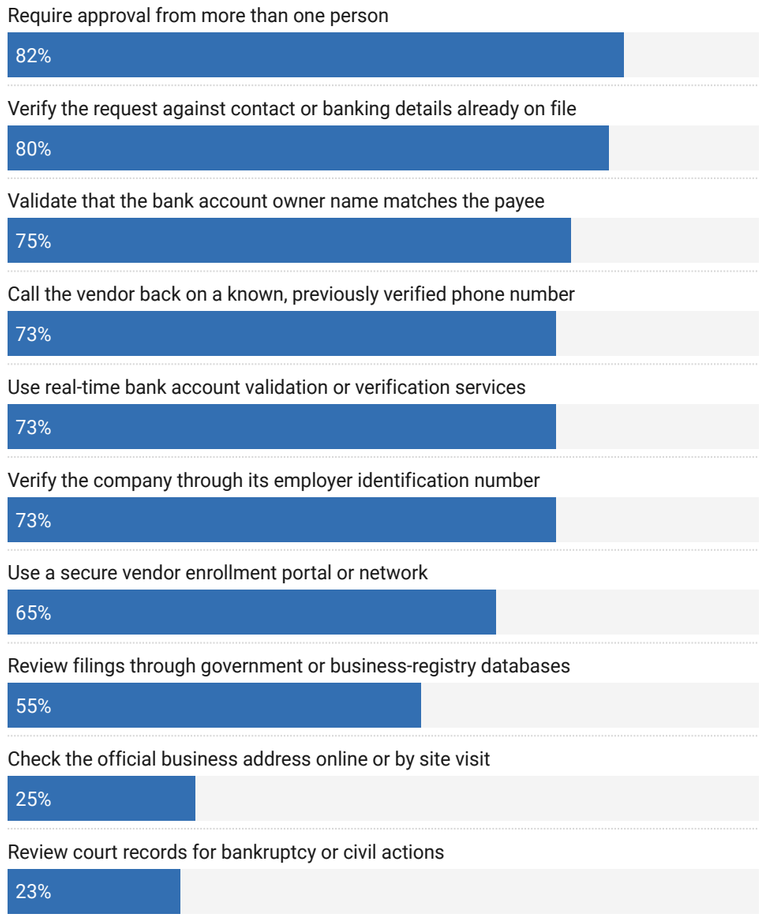
Strong verification processes let businesses confirm who they are paying; they are a core part of any defense against fraud. Most firms require approval from more than one person (82%) and check requests against contact or banking details already on file (80%). Nearly two in three firms (65%) use a secure vendor enrollment portal or network to verify a vendor before adding them or changing their bank details. Additionally, 75% check that the bank account name matches the payee, and 73% use real-time bank account validation.

82%

of firms **require approval from more than one person before adding a vendor or changing bank details,** the most widely used verification step of any.

FIGURE 8:

Share of firms using selected methods to verify a vendor before adding one or changing bank details

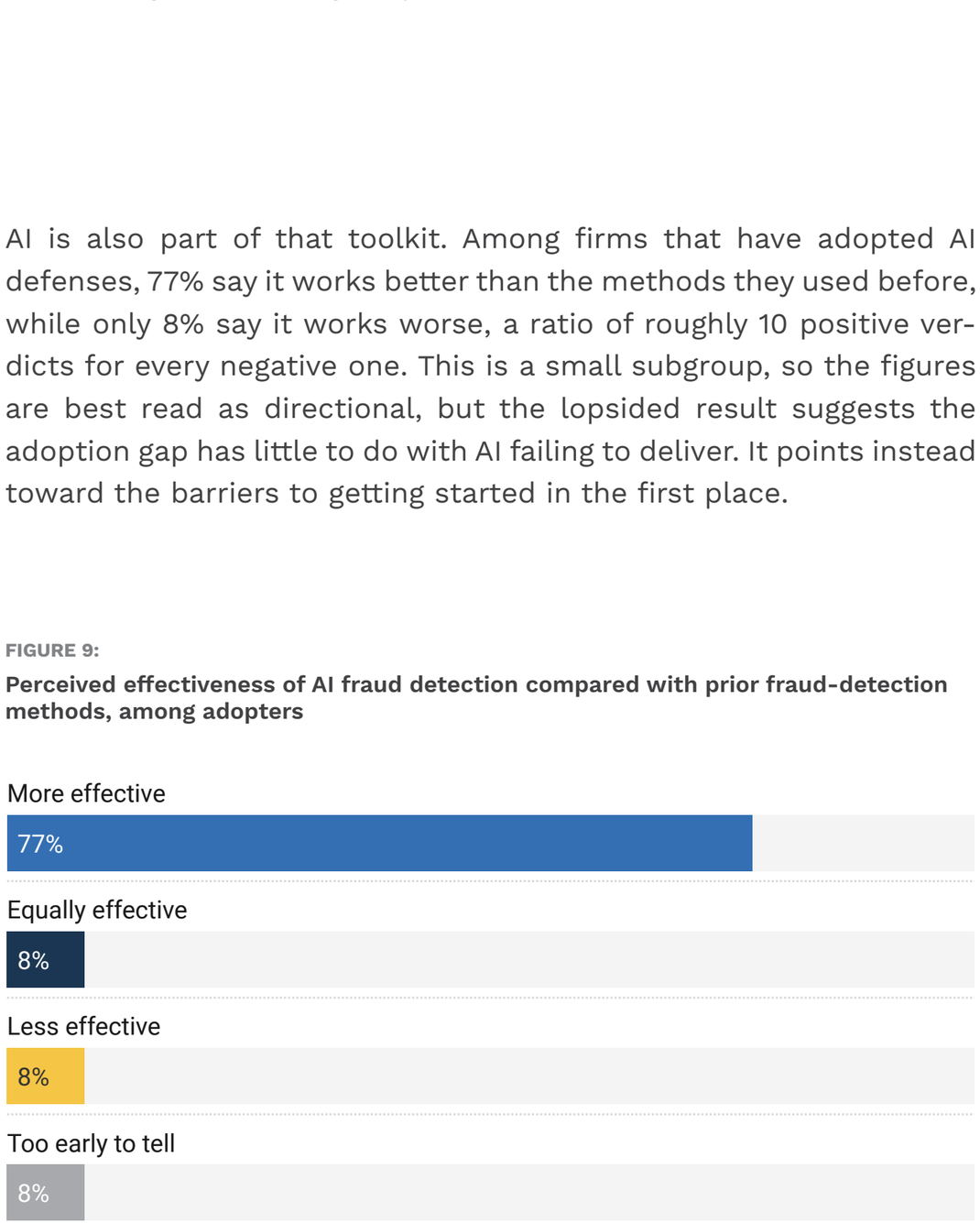


Source: PYMNTS Intelligence
The Payments Fraud Defense, September 2026
N = 150: Whole sample, fielded July 9–27, 2026

AI is also part of that toolkit. Among firms that have adopted AI defenses, 77% say it works better than the methods they used before, while only 8% say it works worse, a ratio of roughly 10 positive verdicts for every negative one. This is a small subgroup, so the figures are best read as directional, but the lopsided result suggests the adoption gap has little to do with AI failing to deliver. It points instead toward the barriers to getting started in the first place.

FIGURE 9:

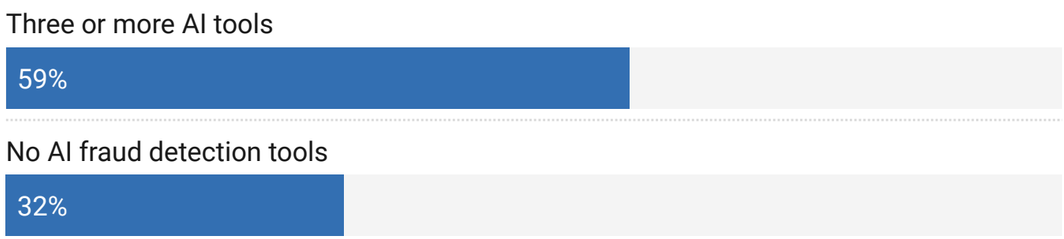
Perceived effectiveness of AI fraud detection compared with prior fraud-detection methods, among adopters



Source: PYMNTS Intelligence
The Payments Fraud Defense, September 2026
N = 65: Firms using AI or machine learning for fraud detection, fielded July 9–27, 2026

FIGURE 10:

Share of firms stopping 90% or more of fraud attempts before any loss, by number of AI tools deployed



Source: PYMNTS Intelligence
The Payments Fraud Defense, September 2026
N = 150: Whole sample, fielded July 9–27, 2026

In fact, most firms with a full AI toolkit (59%) stop 90% or more of fraud attempts before any loss occurs. Among firms running no AI defense, only 32% clear that bar. By industry, tech firms stop the most fraud before loss at 52%, followed by services at 44%, while the goods industry trails at 41%, tracking closely with how heavily each sector has adopted AI.

Firms with a fuller AI defense stack are catching more fraud before it turns into a loss. Tool adoption can serve as a signal of an organization's risk-management maturity.

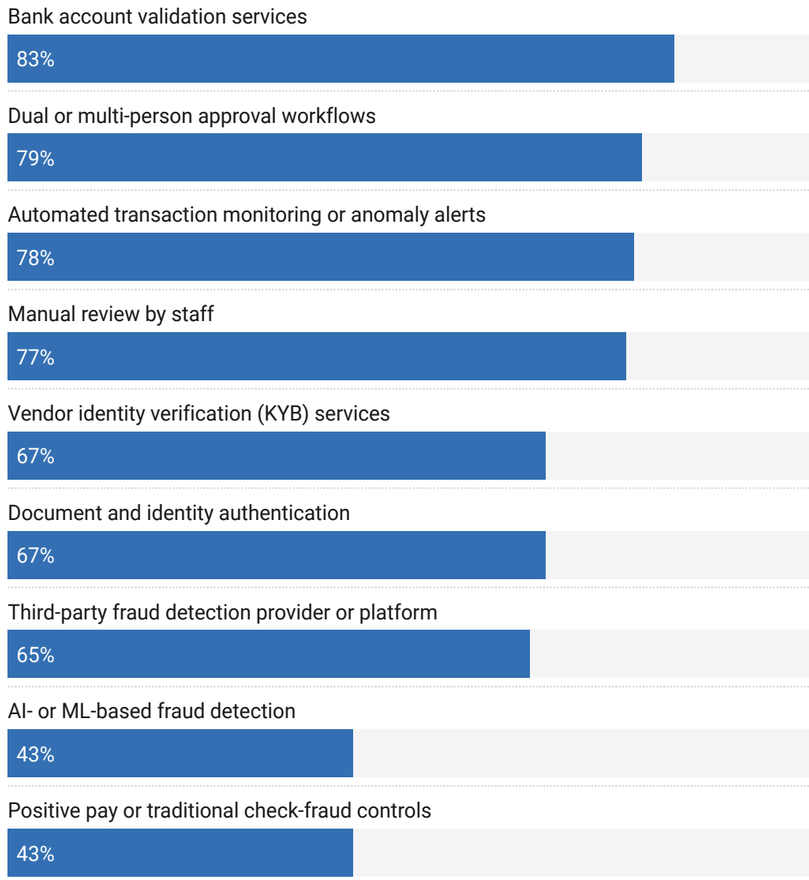
While AI is linked with catching fraud attempts, it is also just one part of an effective defense, and far from the most common one. Eighty-three percent of firms use bank account validation to identify fraud, 77% use manual review and 65% use a third-party fraud detection provider or platform. Only 43% use AI- or machine learning (ML)-based fraud detection. Fraud protection requires a variety of tools and levers, and AI provides an added layer of defense.

83%

of firms **use bank account validation to identify fraud,** nearly twice the share using AI or ML.

FIGURE 11:

Share of firms using selected methods to identify or detect payment fraud



Source: PYMNTS Intelligence
The Payments Fraud Defense, September 2026
N = 150: Whole sample, fielded July 9–27, 2026

Those that haven't adopted AI fraud tools are holding off because they trust their manual reviews to do the job.

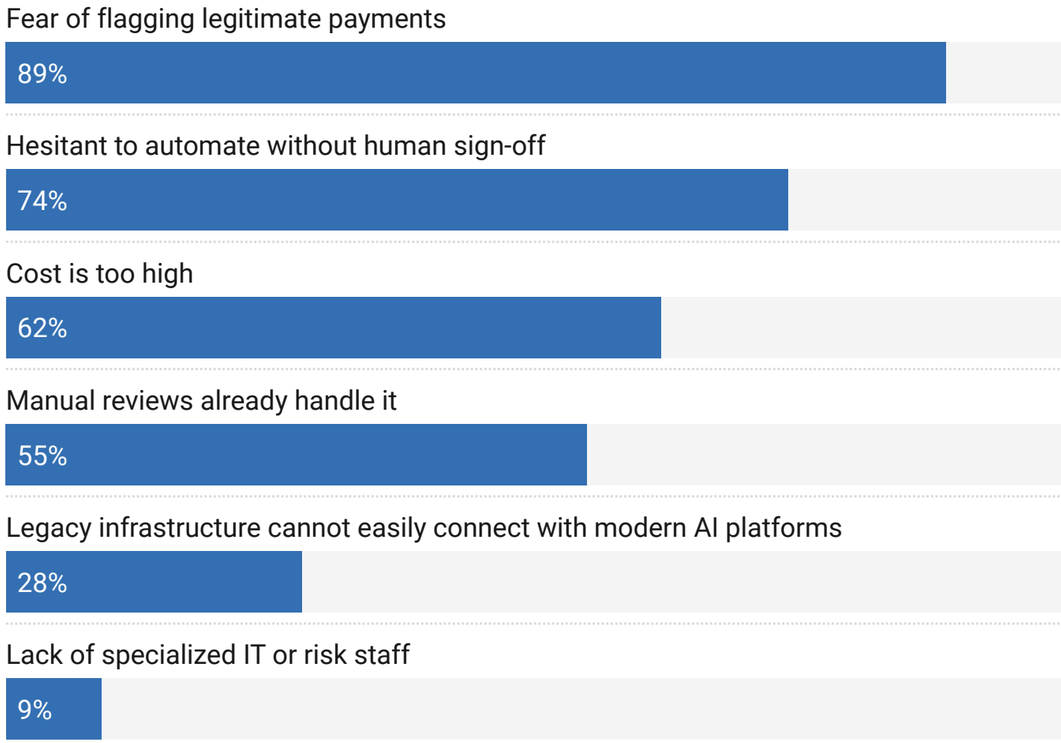
AI adopters may be convinced that their investment is paying off, but more than half of businesses are still holding out. That's because they're satisfied with the systems they have in place.

Among firms with no AI fraud detection, 55% say their manual reviews already handle fraud well enough, a view 89% more common among these non-users than among firms that have already adopted AI. Goods-focused firms are most likely to be satisfied with manual processes, and those in the tech sector are least likely, at 54% versus 33%.

This confidence may reflect years of hands-on vendor relationships rather than a rejection of new technology, which suggests the fastest path forward could be formalizing those relationships into structured, verified supplier networks rather than replacing them outright.

FIGURE 12:

Barriers to adopting AI fraud detection among non-users



Source: PYMNTS Intelligence
The Payments Fraud Defense, September 2026
N = 85: Firms not using AI for fraud detection, fielded July 9–27, 2026

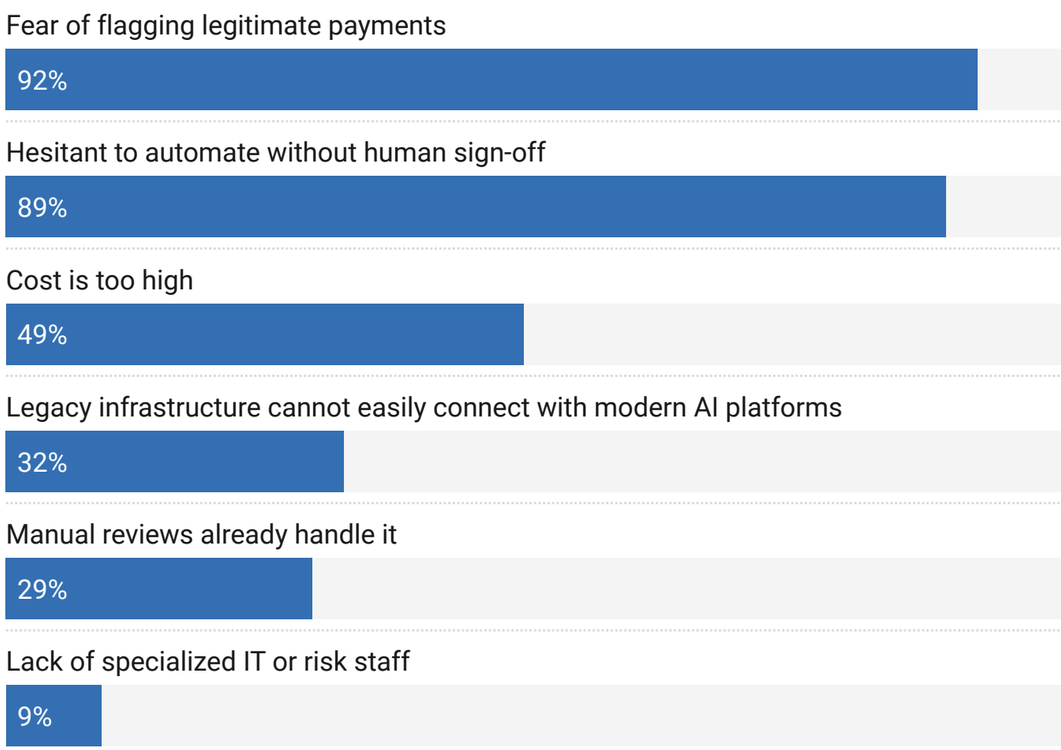
49%

of AI adopters **say cost made adoption difficult, and 32% struggled with legacy systems.** Practical barriers, not doubt about AI, separated the adopters from the holdouts.

Firms that have already adopted AI are facing a different set of roadblocks. Roughly half (49%) say cost has made adoption difficult, and 32% have struggled with legacy systems that could not connect to new tools. Only 29% of AI users say manual reviews alone would have sufficed. One concern does unite both groups: 92% of AI users say that concerns about wrongly flagging a legitimate payment have made adoption harder. Trust in the technology's accuracy tops both lists, but the practical barriers of cost and legacy systems, not doubt about AI's effectiveness, are what have separated the adopters from the holdouts.

FIGURE 13:

Barriers that made AI fraud-detection adoption difficult among current users



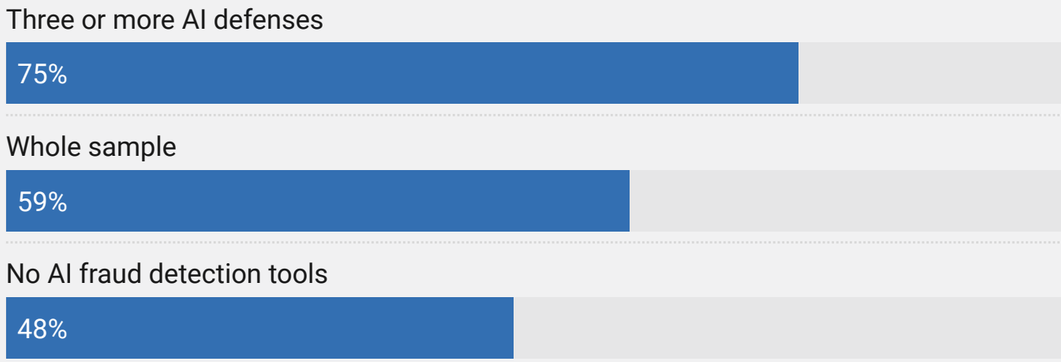
Source: PYMNTS Intelligence
The Payments Fraud Defense, September 2026
N = 65: Firms using AI or machine learning for fraud detection, fielded July 9–27, 2026

Firms are upgrading their AI fraud protection. Even those that have held off until now expect to add these technologies soon.

Across the full sample, 59% of firms say they are very or extremely likely to invest in new payment-security tools within the next 12 months. That appetite is strongest among firms that have already adopted AI: 75% of firms with a full toolkit plan to continue investing, compared with 48% of not using AI fraud tools.

FIGURE 14:

Firms very or extremely likely to invest in new payment-security tools in the next 12 months, by AI-defense depth



Source: PYMNTS Intelligence
The Payments Fraud Defense, September 2026
N = 150: Whole sample, fielded July 9–27, 2026

Most firms not yet using AI are prepared to adopt it soon. Approximately one in four (24%) say they are implementing AI fraud detection right now, 9% plan to do so within six months and another 25% within 12 months. Those figures add up to 58% of non-users making the move within a year, while just 2% say they have no plans to adopt it at all.

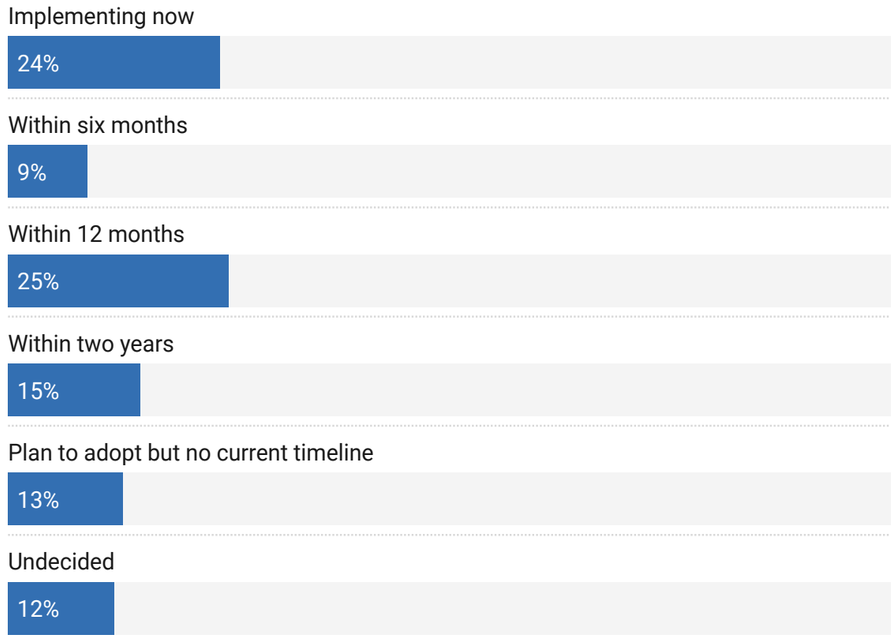
Just **2%**

of firms not yet using AI

say they have no plans to adopt it.

FIGURE 15:

AI adoption timeline among firms not yet using AI fraud detection



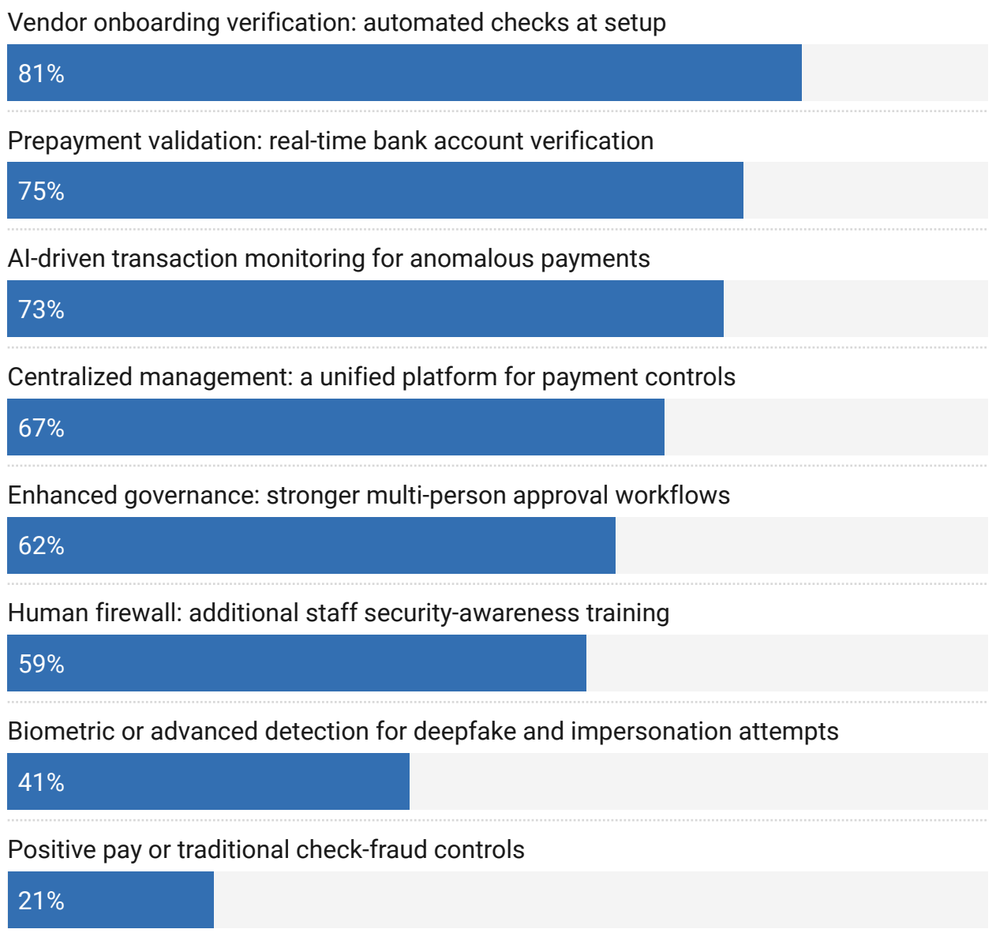
Source: PYMNTS Intelligence

The Payments Fraud Defense, September 2026

N = 85: Firms not yet using AI for fraud detection, fielded July 9–27, 2026

FIGURE 16:

Share of firms saying they are likely to adopt or improve selected capabilities in the next 12 months



Source: PYMNTS Intelligence
The Payments Fraud Defense, September 2026
N = 150: Whole sample, fielded July 9–27, 2026

Yet while most firms plan to invest in AI, it does not top the list of innovation priorities. Instead, when asked what capabilities they will adopt or improve in the next year, firms ranked vendor verification first, with 81% saying they will invest in a more secure onboarding process. The next-most common priority is prepayment bank account validation, at 75%, with AI-driven transaction monitoring ranking third at 73%. Businesses are more focused right now on improving prevention than detection.

Taken together, these findings suggest that organizations are best served by reducing reliance on higher-risk payment methods, increasing adoption of secure electronic payments, strengthening supplier validation and trusted vendor relationships, applying AI-powered controls on top and continuously monitoring for new tactics as they emerge. In short, fraud prevention requires a multipronged approach and ongoing modernization.

ACTIONABLE **INSIGHTS**

Modernize payments

Build a trusted supplier network

Validate accounts/ payees

Implement strong payment controls

Build an AI detection stack

Monitor continuously

01

Spend against the threat you face. Half of finance leaders say the fraud they encounter most is an email impersonating a supplier, and 88% see one at least a few times a year. Fabricated videos appear in just 4% of cases. The picture barely moves across industries, making this a common threat rather than a sector problem.

02

Budget for a set of defenses, not a trial. Companies fall into two camps: 57% run no AI fraud tools at all, and 42% run three or more. Just 1% stop halfway, which argues for funding a program with a defined scope rather than a single tool to evaluate.

03

Base the decision on measured results. Among companies that made the switch to AI-powered defenses, 77% report better results than manual methods, and 59% stop nine in 10 attempts before any money leaves the business, against 32% of those running no AI tools.

04

Test the belief that manual review suffices. Most companies without AI believe their manual checks already work, and they are 89% likelier than AI adopters to say so. The conviction runs deepest among goods companies at 54%, the group that is least protected and most targeted.

05

Assume your competitors are already moving. Nearly six in 10 companies without AI are installing the technology now or will do so within 12 months, and only 2% rule it out. Appetite spans the market: 59% of all companies are likely to buy new payment-security tools, rising to 75% among those already equipped.

September 2026 Report

PREVENTION **FIRST**

Building a Smarter Defense Against Payments Fraud

PYMNTS INTELLIGENCE | Bottomline

METHODOLOGY

This edition of The Payments Fraud Defense series is based on a PYMNTS Intelligence survey of 150 U.S. treasury and finance executives, fielded in July 2026. Respondents work at firms with at least $100 million in annual revenue and are responsible for or knowledgeable about how their organization defends the payments it sends out to vendors and suppliers. The report examines payables fraud only, meaning fraud tied to outbound payments, and does not cover receivables. Firm size and sector comparisons split the sample into revenue bands and industry groups covering tech, services and goods sectors. The AI-user comparison splits the sample by whether a firm uses AI or machine learning for fraud detection, with 65 firms classified as users and 85 as non-users.

THE PYMNTS INTELLIGENCE TEAM THAT PRODUCED THIS REPORT:

Kim Cardenas, Ph.D.
Senior Research Analyst

Carson Olshansky
Senior Writer

Lynnley Browning
Managing Editor

Franco Coraggio
Research Analyst

ABOUT

PYMNTS INTELLIGENCE

PYMNTS Intelligence is a leading global data and analytics platform that uses proprietary data and methods to provide actionable insights on what's now and what's next in payments, commerce and the digital economy. Its team of data scientists includes leading economists, econometricians, survey experts, financial analysts and marketing scientists with deep experience in the application of data to the issues defining the future of the digital transformation of the global economy. This multilingual team has conducted original data collection and analysis in more than three dozen global markets for some of the world's leading publicly traded and privately held firms.

Bottomline

Bottomline helps businesses transform the way they pay and get paid. A global leader in business payments and cash management, Bottomline's secure, comprehensive solutions modernize payments for businesses and financial institutions globally. With over 35 years of experience, moving more than $16 trillion in payments annually, Bottomline is committed to driving impactful results for customers by reimagining business payments and delivering solutions that add to the bottom line. Bottomline is a portfolio company of Thoma Bravo, one of the largest software private equity firms in the world, with more than $170 billion in assets under management. For more information, visit www.bottomline.com.

We are interested in your feedback on this report. If you have questions, comments or would like to subscribe, please email us at feedback@pymnts.com.

DISCLAIMER

Prevention First: Building a Smarter Defense Against Payments Fraud may be updated periodically. While reasonable efforts are made to keep the content accurate and up to date, PYMNTS MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED "AS IS" AND ON AN "AS AVAILABLE" BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.