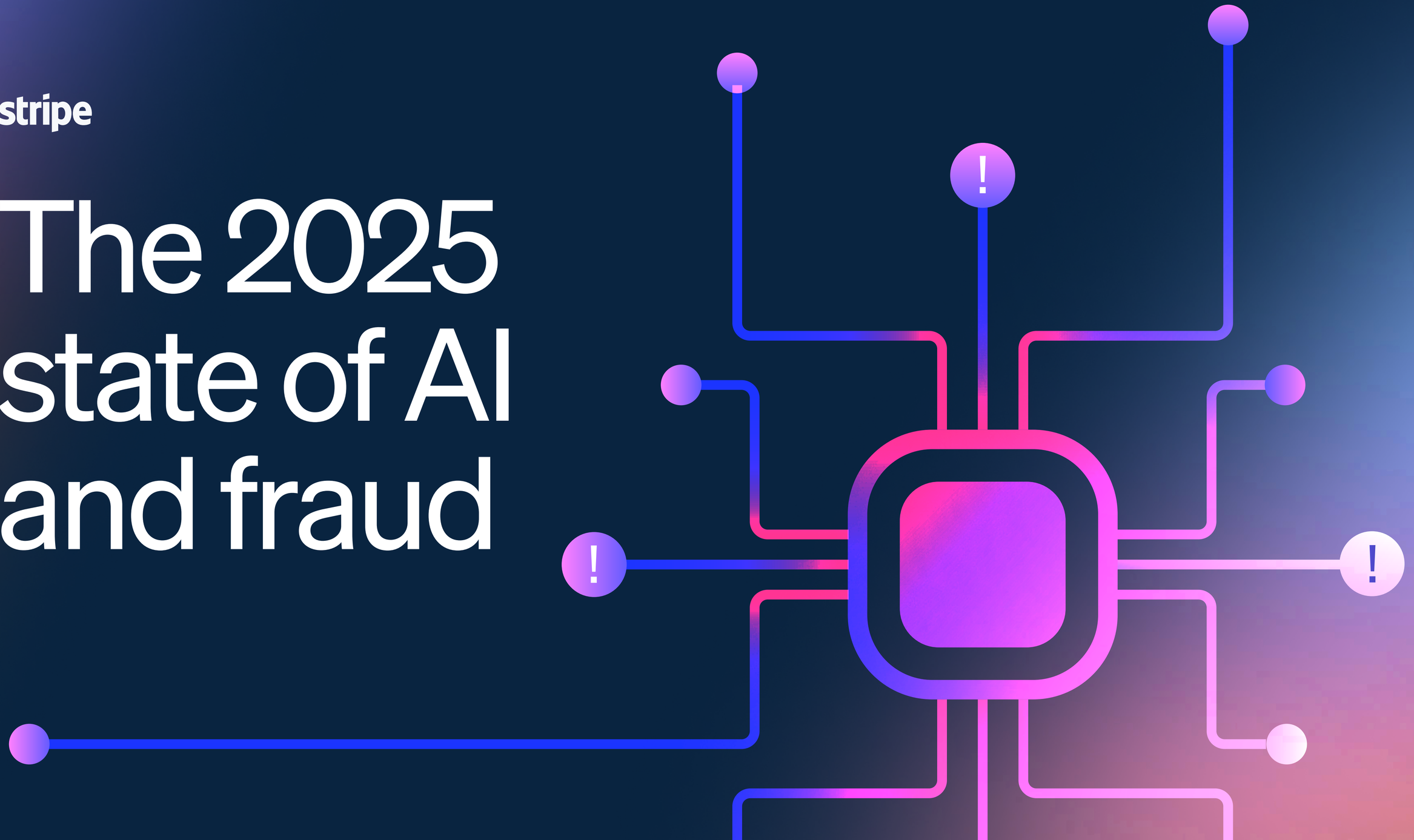
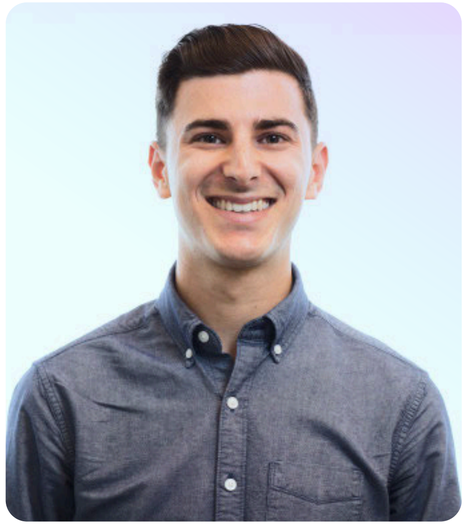
stripe

The 2025 state of AI and fraud





Josh Ackerman

Head of Product, Radar

Foreword

Fraudulent actors now use AI to create fake identities, steal customer card data, and run large-scale card testing operations. At the same time, AI gives businesses a stronger defense against these threats.

To understand how companies navigate this shift, we analyzed billions of attempted payments across millions of businesses on Stripe and interviewed DoorDash, FreshBooks, and other Stripe users. We also worked with Milltown Partners to survey more than 4,000 payments leaders from around the world.

This report reveals the outsized impact that AI has on fraud and explores how AI agents could shape the future of fraud. We also highlight how AI-powered prevention and detection tactics can combat this new wave of fraud, helping keep businesses safe.

Contents

Key takeaways

More sophisticated card testing attacks

Fraudulent actors use AI to gather vast datasets of stolen card credentials, then make thousands of card testing transactions per business, per day, to validate those cards.

Proliferation of false identities

Fraudulent actors pair fake identities with AI-generated websites to create a more believable presence for their fraudulent business and expand their fraud schemes. As a result, 30% of businesses say that AI is making merchant fraud worse.

Accelerated adoption of AI-powered fraud tools

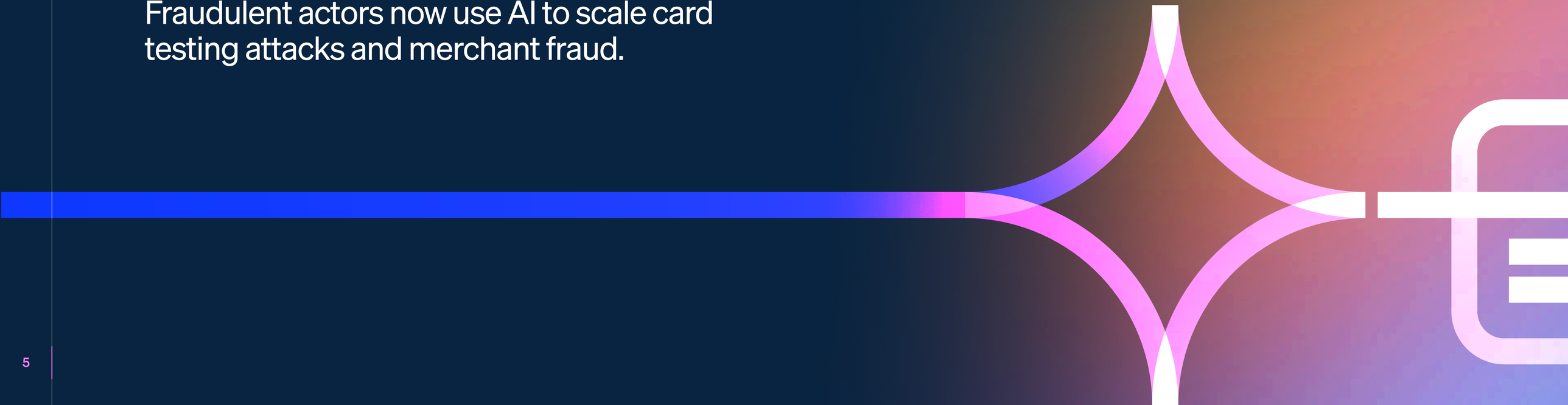
47% of businesses use AI to detect and prevent fraud, making it the most popular usage of AI in payments. Insurance companies and SaaS platforms lead in AI adoption for fraud prevention due to their complex workflows and high-value transactions.

New detection and prevention strategies

Companies such as DoorDash and FreshBooks are using Stripe's AI models to incorporate the learnings from the scale of the Stripe network into their fraud calculations, reducing chargebacks and blocking fraudulent merchants from onboarding.

The AI threat in online payments

Fraudulent actors now use AI to scale card testing attacks and merchant fraud.

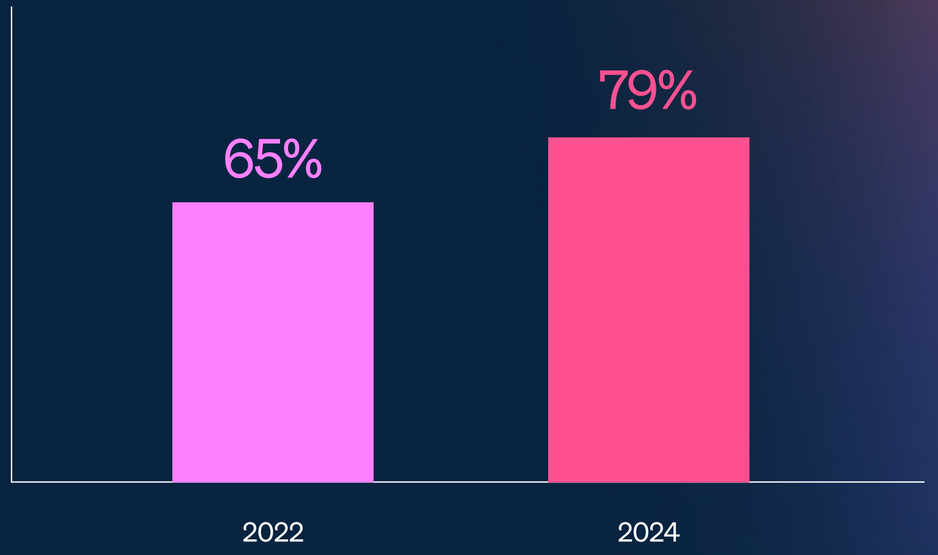


More sophisticated phishing scams and card testing attacks

Card testing is one of the most challenging types of fraud to detect and block: attacks blend in easily with legitimate traffic, and fraudulent actors are constantly changing their tactics.

Now we're seeing fraudulent actors use AI to enhance both ends of their operation. First, they use generative AI to create convincing phishing scams and fake websites that replicate ones where customers are making purchases, efficiently gathering vast datasets of stolen card credentials. Then, they use automated tools to validate these cards through large-scale testing attacks. This not only puts customers' personal information at risk, but it also increases disputes for businesses.

The rise of payment fraud attempts and attacks has coincided with the increase in adoption of generative AI



2025 AFP® Payments Fraud and Control Survey

Large-scale attempted card testing attacks

Among card testing attacks blocked by Stripe

1 in 4

involve bad actors attempting more than 1 million transactions against a single business

Stripe data, global, 2025

Fraudulent actors are bypassing KYC checks with fake accounts

Nearly one in three business leaders surveyed say AI is worsening fake account creation and merchant fraud. In particular, fraudulent actors are using generative AI tools to create fake identities and falsified documents that are so convincing they can bypass platforms' and marketplaces' Know Your Customer (KYC) verification systems.

The problem compounds when fraudulent actors pair these fake identities with AI-generated business websites, allowing them to create a more believable presence for their fraudulent business and expand their fraud schemes. For example, a fraudulent actor can set up a fake account on a marketplace and sell fraudulent goods and services, or they can create a fake account to obtain product licenses that they then resell.

30%

of business leaders say that AI is making fake account creation and merchant fraud worse in either sophistication or volume

2025 "State of fraud" survey

500,000

number of global fake account creation attempts blocked by Radar for Platforms from January to May 2025

Stripe data, global, 2025

How FreshBooks combats an increase in merchant fraud

FreshBooks

Andrew Gunner

Head of Product

"We're seeing absolute advances in fraudsters applying very advanced technology to try to defraud us. For example, we've seen an uptick in fraudulent actors using generative AI to target our platform. As a result, we're focused on trusting and validating a user at the point of onboarding, and monitoring that behavior throughout their journey with us.

In particular, our partnership with Stripe has unlocked capabilities for us to complete the link between merchant risk and transaction monitoring. Merchant underwriting has historically been a periodic and distinct process from transaction monitoring for payments. This made it more difficult and manual to understand whether a merchant's actual payment activity deviates from their expected behavior, leading to more alerts and higher false positives. With Stripe, we can now use a dynamic and risk-based decisioning that, in conjunction with our underwriting data, provides a real-time view of our portfolio health on a day-to-day basis.

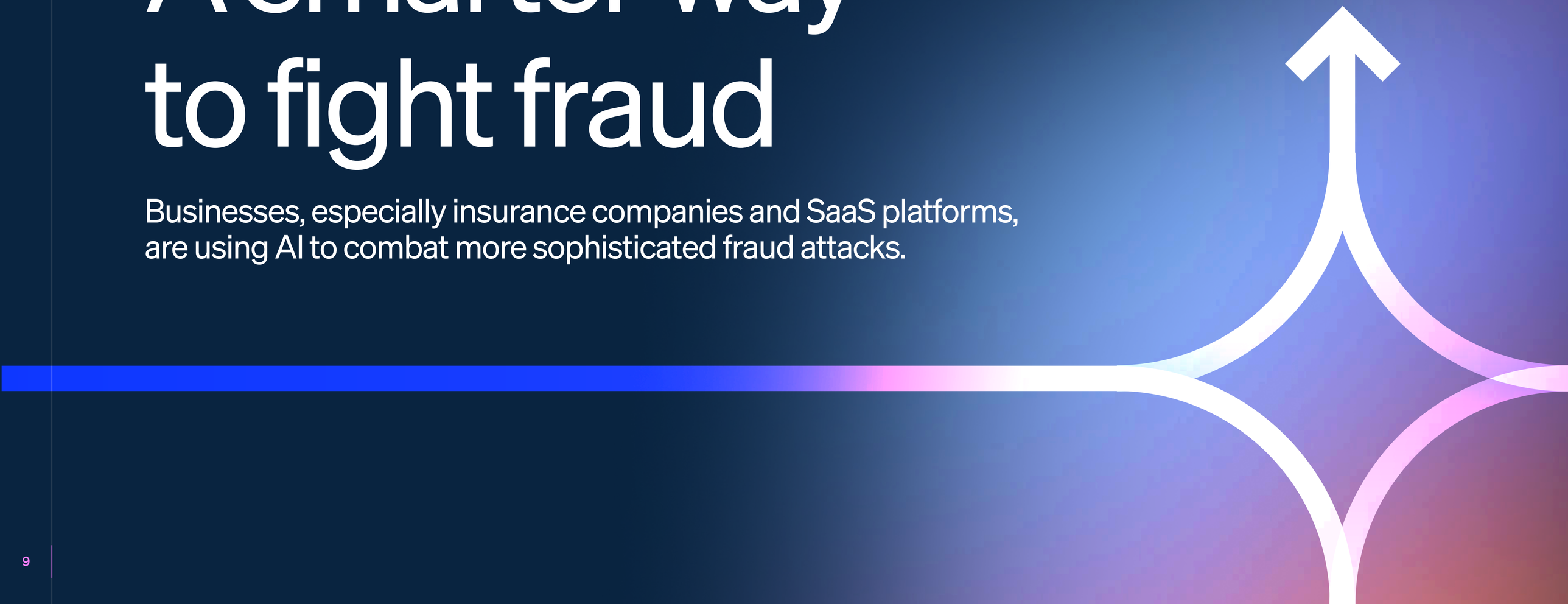
This tooling has significantly increased the efficiency of our risk team to focus efforts where manual intervention is truly needed, and has allowed us to block more than 300 fraudulent accounts from onboarding onto our platform in just 3 months."

300

fraudulent accounts blocked in 3 months with Stripe

A smarter way to fight fraud

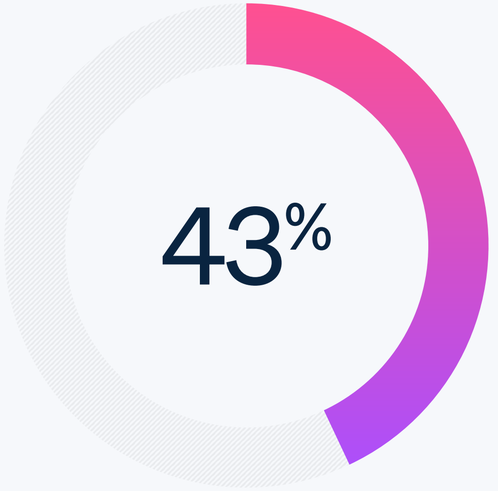
Businesses, especially insurance companies and SaaS platforms, are using AI to combat more sophisticated fraud attacks.



Businesses prioritize AI for fraud detection and prevention

Payments are a data-rich domain requiring hundreds of microdecisions in real time, making it ripe for AI-powered optimizations. Companies around the world are rapidly embracing this opportunity, using AI to automate all aspects of payments, such as payments compliance, payments performance monitoring, and customer communication about their payments.

However, one use case stands out: fraud detection and prevention. Using AI to detect and prevent fraud is the most popular usage of AI in payments, allowing businesses to detect subtle patterns and anomalies across hundreds of signals that indicate fraudulent activity.



of business leaders who already use AI to manage payments

2025 "State of payments" survey

Top ways companies use AI in payments

2025 "State of payments" survey

Insurance, SaaS, and travel companies are leading the way

While businesses across all industries are adopting AI to combat fraud, those in insurance, SaaS, and travel are more likely to do so compared to companies in other industries. This may be due to their complex workflows and high-value transactions, creating a greater need for AI-powered fraud tools that can scale with their risk.

How different industries use AI to combat fraud

Insurance

To reduce claims payout fraud, insurance companies use AI-powered identity verification tools to confirm that the recipient is who they claim to be.

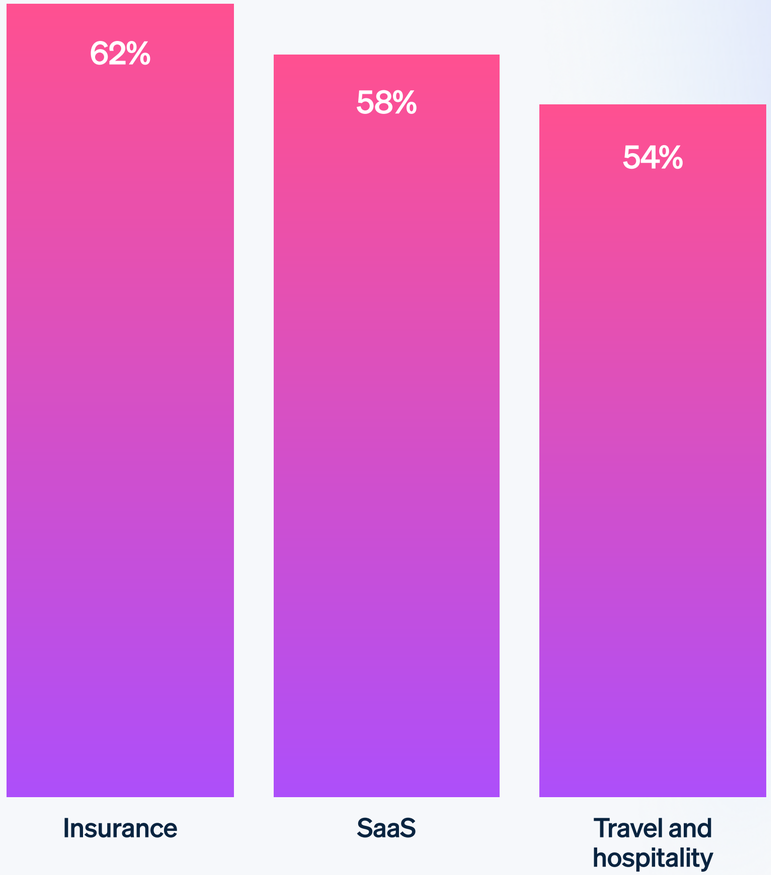
SaaS

To keep up with their rapid user growth, SaaS companies use AI to detect fraudulent sign-ups, prevent account takeovers, and identify subscription abuse patterns across their expanding user base.

Travel and hospitality

To combat fraud on high-value bookings like international flights and hotel packages, travel companies use AI to identify and block risky transactions before they are processed.

Top industries using AI for fraud detection and prevention



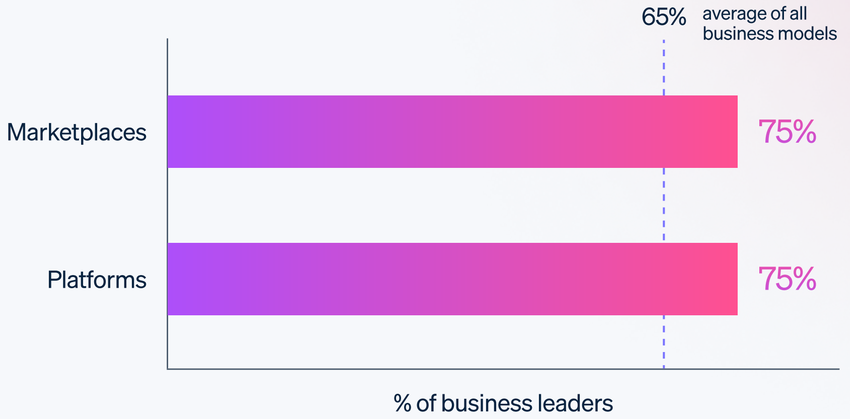
2025 "State of payments" survey

Platforms and marketplaces have higher AI adoption rates

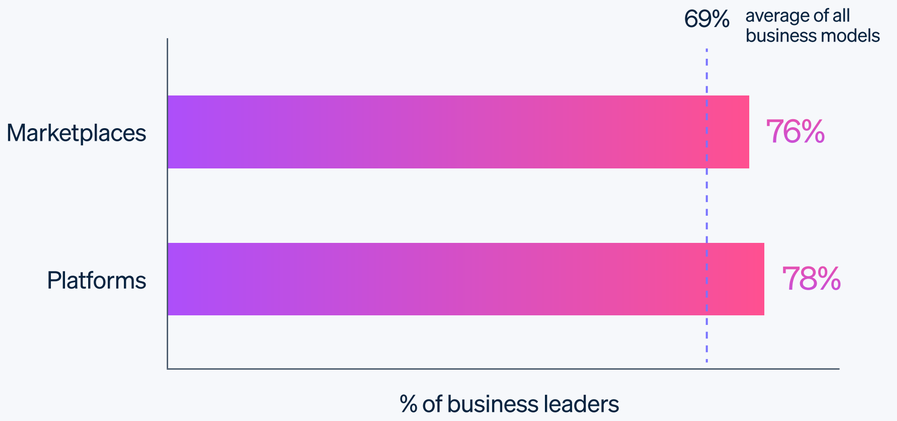
Fraud is especially challenging for platforms and marketplaces that enable payments: three in four leaders surveyed say fraud is evolving too fast for their business to keep up. Platforms and marketplaces face both transaction fraud and merchant fraud, and often rely on a patchwork of in-house tools, basic payment processor checks, and third-party services to manage risk. As they grow, processing higher payment volumes and onboarding more users inherently adds complexity.

Platforms and marketplaces recognize that traditional, manual approaches to fraud detection can't scale to address these multidimensional risks. As a result, our survey shows they're adopting AI-powered fraud prevention tools at a significantly faster-than-average rate.

Most platform and marketplace business leaders agree fraud is evolving too rapidly for their company to keep up



Most platform and marketplace business leaders have adopted AI or automation tools to fight fraud



2025 "State of fraud" survey

How DoorDash uses AI to fight fraud

DOORDASH

Rishabh Pandey

Software Engineer,
Payments Fraud team

"DoorDash has been investing heavily in our AI and ML infrastructure when it comes to fighting fraud. Because of the rise of fraud, we have to take advantage of AI to fight against it. For example, we have configurable rule engines, which helps us use AI in real time when we're trying to make a decision for any incoming transaction.

Apart from that, we also have our own in-house fraud models for each different payment workflow. For example, order checkout has its own model, gift cards have their own model, and so on. Each of these models uses different signals—behavioral or transactional signals depending on the payment—and historical context about the user, like their activity on our platform and their previous transaction history.

One of the signals DoorDash uses is the risk score that Radar provides after evaluating our transaction. This helps us incorporate the benefits of the scale of the Stripe network into our fraud calculations. Since incorporating Radar risk scores, we've seen a 10% decrease in chargeback costs at DoorDash."

10%

decrease in chargeback costs since incorporating Radar risk scores

What does the future of AI and fraud look like?

We interviewed subject matter experts at Stripe from our payments performance and fraud teams, and analyzed user interviews and feedback, to explore what the future of AI and fraud could look like.

While there are many uncertainties, one thing is clear: fraud detection will be shaped by AI agents acting as both new fraud vectors and sophisticated defenses. This evolution will also drive changes in identity verification, as traditional methods become less reliable against AI-generated fake documents.

Agentic commerce could add a new dimension to fraud detection

We expect new fraud challenges as agentic commerce becomes mainstream. For example, to support agentic commerce, businesses may need to use “universal wallets,” which may create additional avenues for account takeovers.

AI agents could help make risk analysis more efficient

Agents can both detect and interpret fraud patterns that teams might miss as well as help eliminate the need to conduct manual reviews during fraud investigations.

Identity verification tools could focus on harder-to-fake factors

As fraudulent actors increasingly use generative AI to create convincing fake-identity documents, we expect identity verification and authentication will evolve to include more secure inputs, such as biometrics and passkeys.

How Stripe can help

Stripe is a fully integrated suite of financial and payments products that powers payments for online and in-person retailers, subscription businesses, software platforms and marketplaces, and everything in between. From reducing fraud to verifying identities, you can use Stripe to:

- **Detect and block fraud** using AI that trains on data across millions of global companies with **Stripe Radar**. We've been able to reduce dispute rates for Radar users by 17% last year, even as industry-wide ecommerce fraud increased 15%.
- **Reduce card testing attacks.** Thanks to our **Payments Foundation Model**, an industry-first AI model trained on tens of billions of transactions, our detection rate for attacks on large users significantly increased from 59% to 97%.
- **Detect fraudulent connected accounts**, set custom account-level rules, and intervene on suspicious transactions with **Radar for Platforms**.
- **Protect against fraudulent actors** creating fake accounts on your platform with **Stripe Identity**, which helps you verify the identities of individuals and identify false credentials.

To learn more about how Stripe can help your business fight fraud, **contact us** or **sign up for an account.**

Methodology

Stripe analyzed billions of attempted payments from millions of businesses from 2024 to 2025. Across those transactions and businesses, we looked at card testing activity—both the size of the attacks and their frequency—and the number of fake accounts being created on Stripe.

In early 2025, Stripe also worked with Milltown Partners (in partnership with their data provider, Focaldata) to run two surveys: “State of payments” and “State of fraud.” For “State of payments,” we surveyed 2,052 business leaders from Australia, Brazil, France, Germany, Japan, the Netherlands, Singapore, the United Kingdom, and the United States. For “State of fraud,” we surveyed 2,052 business leaders from Australia, Canada, France, Germany, Japan, the Netherlands, Singapore, the UK, and the US.

We also interviewed Stripe subject matter experts from our payments performance and fraud teams.