Ravelin

AI VS AI: FRAUDSTERS VS FRAUD FIGHTERS AND THE FUTURE OF FRAUD

2025 REPORT

ravelin.com

VS

TYPES OF AI TOOLS USED BY **FRAUDSTERS**

LLM-based GenAI - for spear phishing attacks vs consumers and employees

Synthetic IDs - to scale up fake account creation

Generative AI – to create scripts for attacks

Vocal cloning – for spear phishing on the phone, against consumers and employees

TYPES OF AI TOOLS USED BY **FRAUD FIGHTERS**

Machine learning - to stop fraud and learn from past behavior

Big data analysis - to detect anomalies

Natural language processing - to better understand context and text inputs

Adversarial AI - to simulate attacks

Generative AI - to assist with day-to-day fraud ops, reporting, and more

CONTENTS

A MATTER OF SCALE:
MARTIN SWEENEY ON AI IN FRAUD

We've read a lot about the "AI revolution" in every sector of professional, personal and public life. At the end of the day, how does the rumored onslaught of AI fraud manifest itself, if at all? And how helpless are we against it?

AI in fraud is a matter of scale.

Ravelin was one of the first AI-native fraud prevention companies, building the entire fraud detection solution around engineering principles and deploying multiple machine learning models to continuously improve performance.

This automation, stemming from the adoption of ML and AI, is what allowed our customers to scale up and grow without disproportionately increasing their headcount.

Of course fraudsters will use AI. It's inevitable that they will be able to. Like the fraud prevention community has industrialized our artisanal process, fraudsters will also use AI to industrialize theirs, and they will have more of a production line of attacks and people perpetrating them. And they have more efficient tools to do it, whether that means AI and LLMs or anything else.

Our survey results showed that 64% of merchants have already been targeted by AI fraud – but, as tech experts, we also might want to take that with a pinch of salt.

What's the real story? Even if fraud teams have irrefutable proof that AI tools are used against their fraud department, this can be a simple, obvious application. For example, a criminal might use ChatGPT to write a refund abuse claim or a phishing email. But is that groundbreaking or impossible to prevent? I don't think so.

I think the real story is that AI is part of a package of tools that help people become more efficient in perpetrating the crimes they already wanted to perpetrate. There is no magic "help me be a really good fraudster" button. But there is a series of improvements fraudsters can make to their process to make it harder to detect. Just as there have always been.

On our end, as fraud prevention experts, we want to do the same: Continuous improvements to our processes, strategies, and tooling, to make ourselves more efficient and to be able to use at scale – which ought to include machine learning tools, NLP, LLMs and any AI that might be useful in stopping fraud.

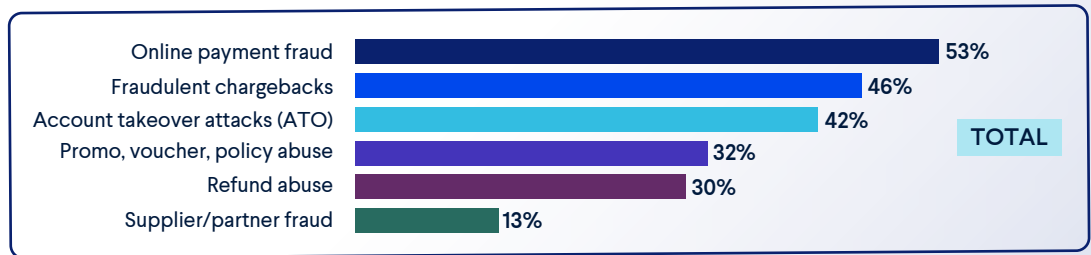Automation, efficiency and working smart is what Ravelin has always been about.

"
Like the fraud prevention community has industrialized our artisanal process, fraudsters will also use AI to industrialize theirs"
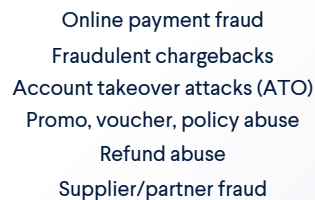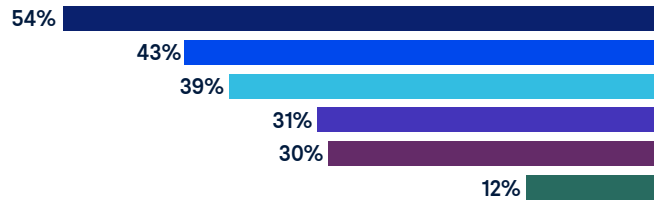
WILL AI MAKE FRAUD MORE DIFFICULT TO PREVENT?

"Do you believe any of these types of fraud will become more frequent and/or difficult to prevent in the next 12 months due to AI?"

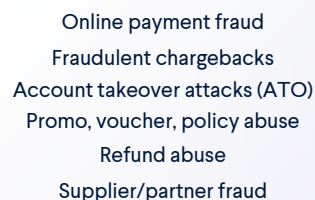Most merchants expect AI-enabled fraud to affect **payment fraud the most** – and **partner fraud the least.**

TOTAL

Online payment fraud	53%
Fraudulent chargebacks	46%
Account takeover attacks (ATO)	42%
Promo, voucher, policy abuse	32%
Refund abuse	30%
Supplier/partner fraud	13%

RETAIL

54%	Online payment fraud
43%	Fraudulent chargebacks
39%	Account takeover attacks (ATO)
31%	Promo, voucher, policy abuse
30%	Refund abuse
12%	Supplier/partner fraud

TRAVEL

Online payment fraud	49%
Fraudulent chargebacks	49%
Account takeover attacks (ATO)	44%
Promo, voucher, policy abuse	36%
Refund abuse	29%
Supplier/partner fraud	13%

DIGITAL GOODS

52%	Online payment fraud
55%	Fraudulent chargebacks
45%	Account takeover attacks (ATO)
35%	Promo, voucher, policy abuse
29%	Refund abuse
12%	Supplier/partner fraud

MARKETPLACES

Online payment fraud	55%
Fraudulent chargebacks	35%
Account takeover attacks (ATO)	42%
Promo, voucher, policy abuse	27%
Refund abuse	31%
Supplier/partner fraud	15%

HOW CAN AI STOP FRAUD?

"Which of the following tools do you find most effective for fighting fraud?"

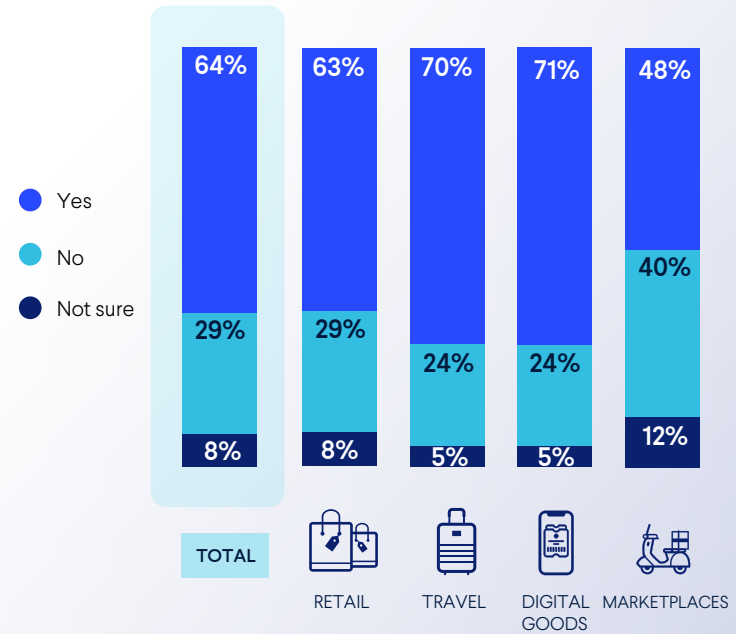| Tool	Percentage
Two-factor authentication (2FA)	54%
Machine learning	47%
IP analysis	39%
Device ID analysis/device fingerprinting	38%
Rules engine	25%
Graph networks	25%
Behavioral analysis	19%
Consortium data	17%
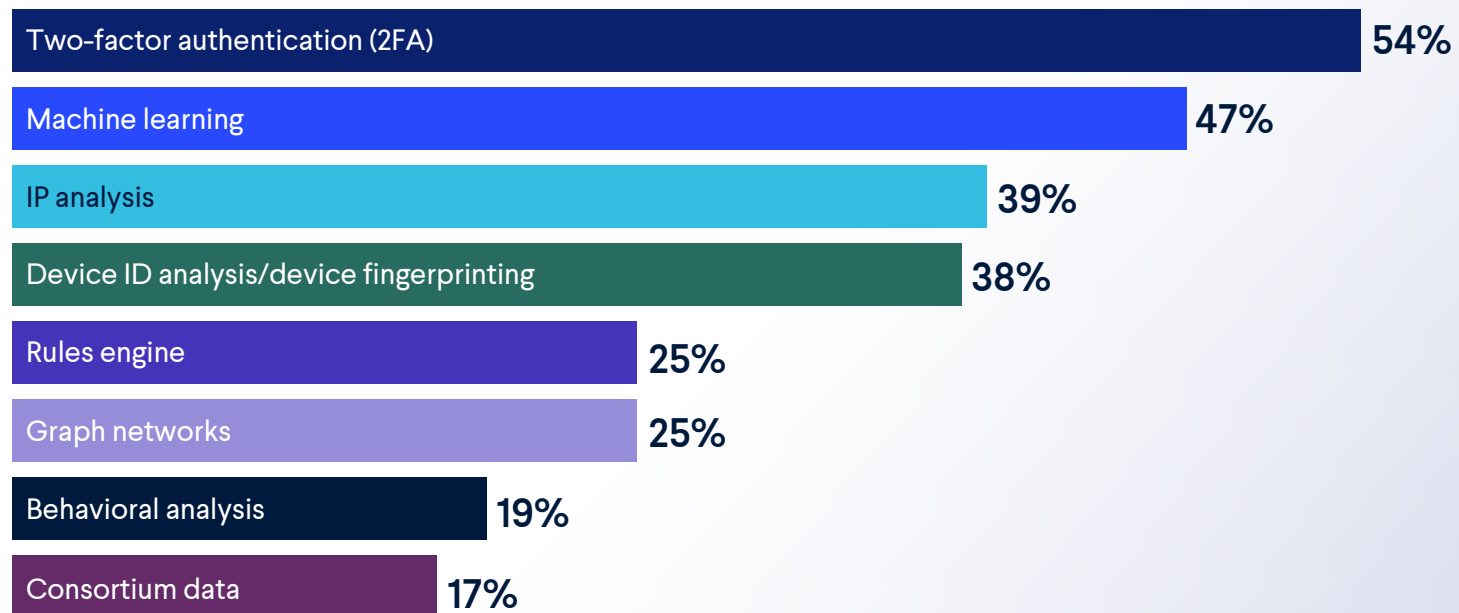
AI-POWERED FRAUD:
PERCEPTION VS REALITY

Digital Goods report the most AI fraud, while **Marketplaces are reporting the fewest attacks.**

"Are you concerned about fraudsters using AI technology (LLMs, machine learning, synthetic IDs, etc) to attack you or your customers?"
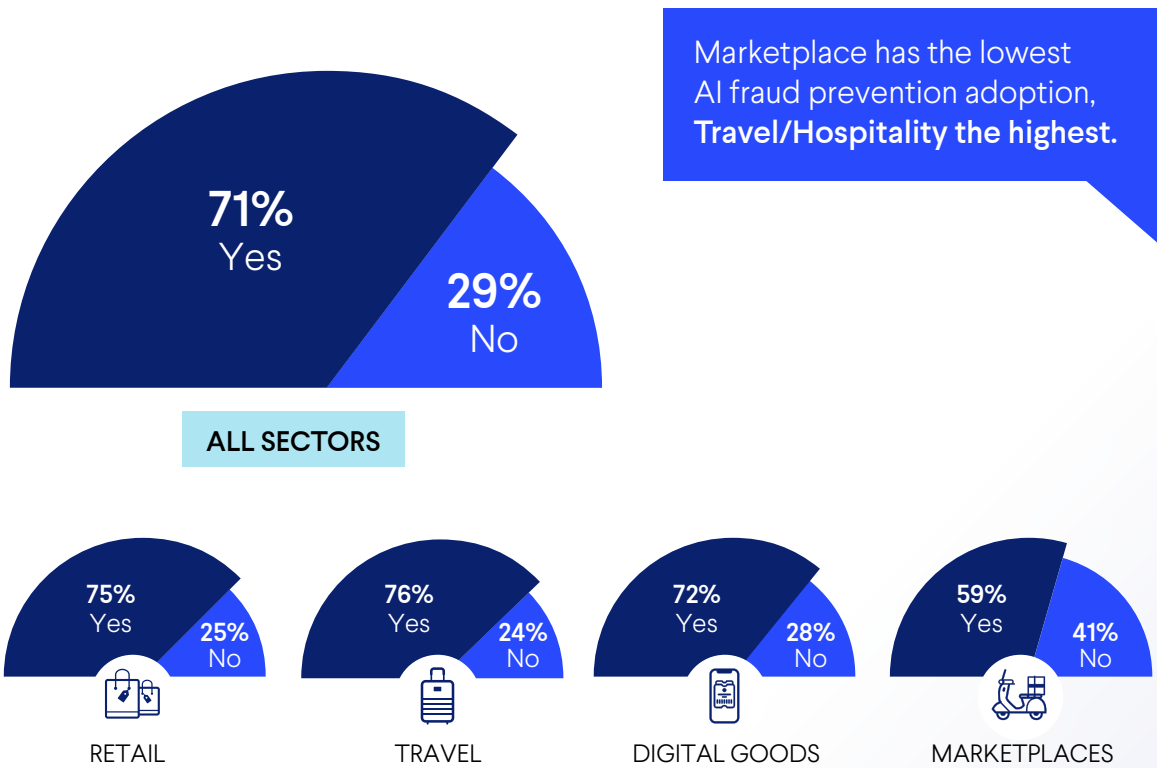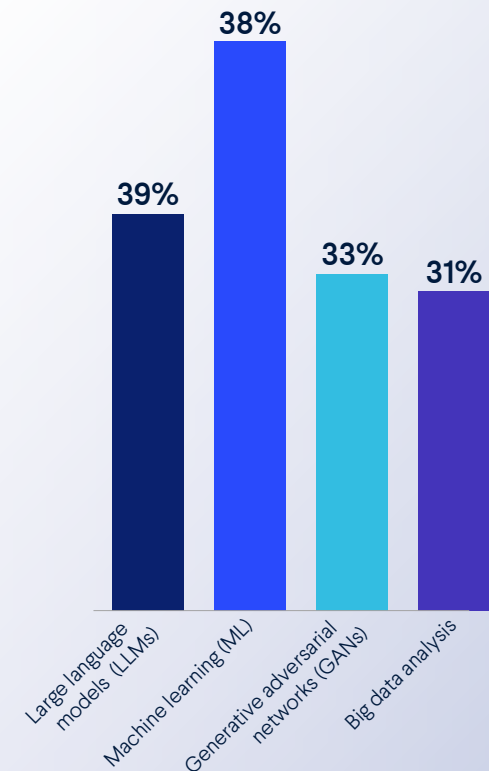
"Are you aware of any fraudster activity involving any type of AI technology (LLMs, machine learning, synthetic IDs, etc) attempted against your company in the past 12 months?"learning, synthetic IDs, etc) to attack you or your customers?"

Left chart legend:
- Very concerned
- Somewhat concerned
- A little concerned
- Not concerned

	TOTAL	RETAIL	TRAVEL	DIGITAL GOODS	MARKETPLACES
Very concerned	46%	51%	51%	43%	40%
Somewhat concerned	45%	40%	43%	50%	47%
A little concerned	8%	6%	7%	7%	11%
Not concerned	1%	1%			2%

Right chart legend:
- Yes
- No
- Not sure

	TOTAL	RETAIL	TRAVEL	DIGITAL GOODS	MARKETPLACES
Yes	64%	63%	70%	71%	48%
No	29%	29%	24%	24%	40%
Not sure	8%	8%	5%	5%	12%

The Travel/Hospitality sector is most concerned, with **Marketplaces the least concerned.**

ADOPTION OF ANTI-FRAUD AI

71% Yes

29% No

ALL SECTORS

Marketplace has the lowest AI fraud prevention adoption, **Travel/Hospitality the highest.**

75% Yes   **25%** No
RETAIL

76% Yes   **24%** No
TRAVEL

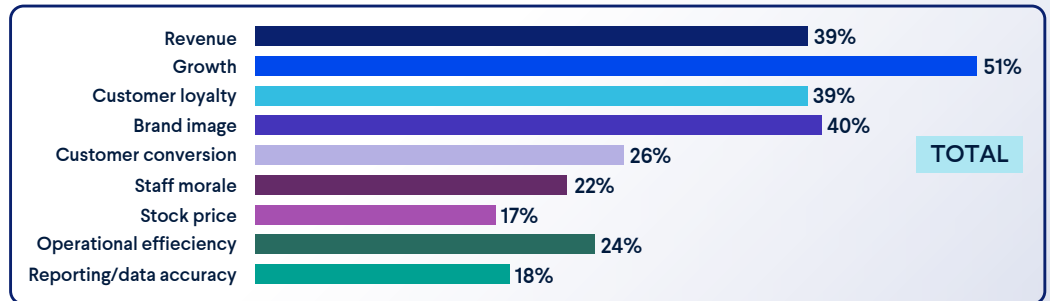**72%** Yes   **28%** No
DIGITAL GOODS

59% Yes   **41%** No
MARKETPLACES

"Are you currently using machine learning (ML), large language models (LLMs) or any other AI technology to detect and/or prevent fraud?"

"Which of the following types of artificial intelligence do you believe are or could be useful in the fight against fraud?"

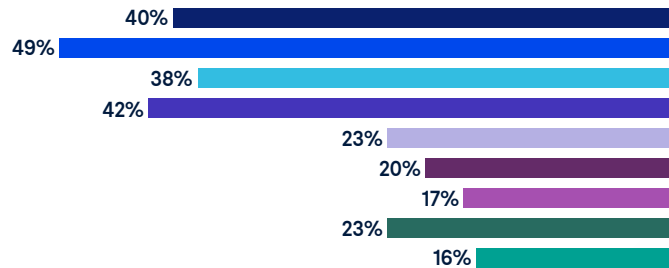| Type	Percentage
Large language models (LLMs)	39%
Machine learning (ML)	38%
Generative adversarial networks (GANs)	33%
Big data analysis	31%

| AI VS AI IN FRAUD REPORT

THE CONSEQUENCES OF AI-FUELLED FRAUD

"Are you concerned about the impact of AI-enabled fraud on any of the following metrics and results at your company? Please select all that apply."
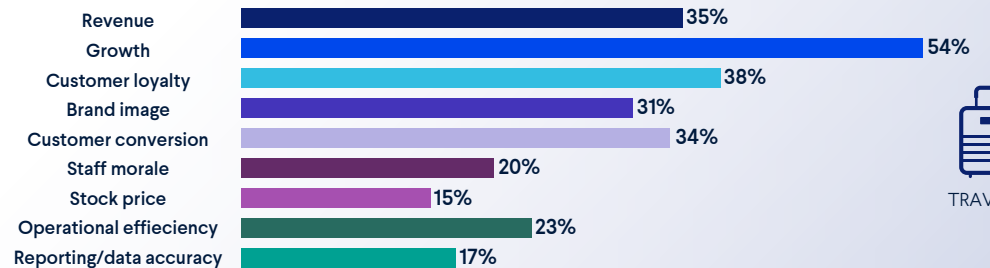
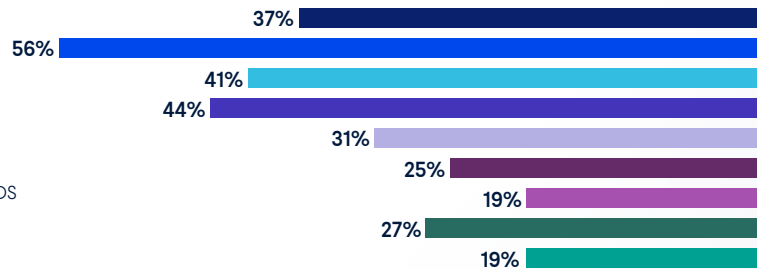Merchants believe AI-powered fraud will **impact growth, brand image** and **customer loyalty** the most.
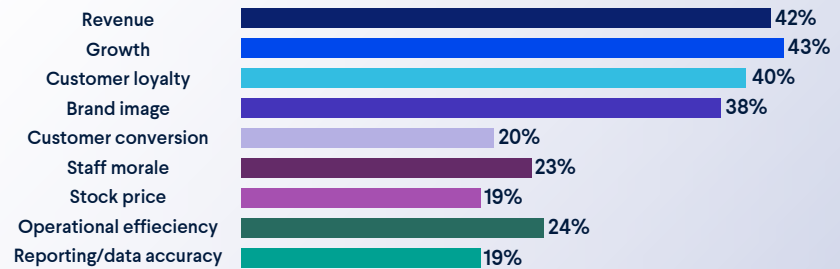
TOTAL

Metric	Total
Revenue	39%
Growth	51%
Customer loyalty	39%
Brand image	40%
Customer conversion	26%
Staff morale	22%
Stock price	17%
Operational efficiency	24%
Reporting/data accuracy	18%

RETAIL

RETAIL	Metric	TRAVEL
40%	Revenue	35%
49%	Growth	54%
38%	Customer loyalty	38%
42%	Brand image	31%
23%	Customer conversion	34%
20%	Staff morale	20%
17%	Stock price	15%
23%	Operational efficiency	23%
16%	Reporting/data accuracy	17%

TRAVEL

DIGITAL GOODS

DIGITAL GOODS	Metric	MARKETPLACES
37%	Revenue	42%
56%	Growth	43%
41%	Customer loyalty	40%
44%	Brand image	38%
31%	Customer conversion	20%
25%	Staff morale	23%
19%	Stock price	19%
27%	Operational efficiency	24%
19%	Reporting/data accuracy	19%

MARKETPLACES

Ravelin is AI-native, using a ML-first multi-model approach to enabling automation that allows merchants to accept more payments and serve customers with confidence.

1

Ravelin's solutions make use of **ML models trained on clients' own data and risk landscape** – and they grow alongside our clients, constantly learning and improving.

2

Using **LLM tech**, Ravelin's AI fraud rule generator understands requests in any language to generate complex fraud rules that match your policies.

3

We've deployed **natural language processing (NLP)** in our ML models to better understand non-numerical signals such as text within context, for greater precision.

All data gathered as part of Ravelin's Global Fraud Survey.
For more details and more data please download the Global Fraud Survey Report.

Thank you for reading our AI vs AI in Fraud Report

Ravelin builds AI-native solutions to help companies accept payments with confidence, learning from your historical data to inform a payments strategy that works for your specific needs and goals – and no-one else's.

Get in touch today to find out more about solutions addressing online payment fraud, refund abuse, account security, 3D Secure, transaction optimization, promo abuse, or supplier fraud.

Book a call at ravelin.com/contact-us.

Questions? Comments?
Please write to marketing@ravelin.com.

We frequently release new findings in fraud and payments.
Make sure you follow us on **LinkedIn** or by signing up at **ravelin.com.**