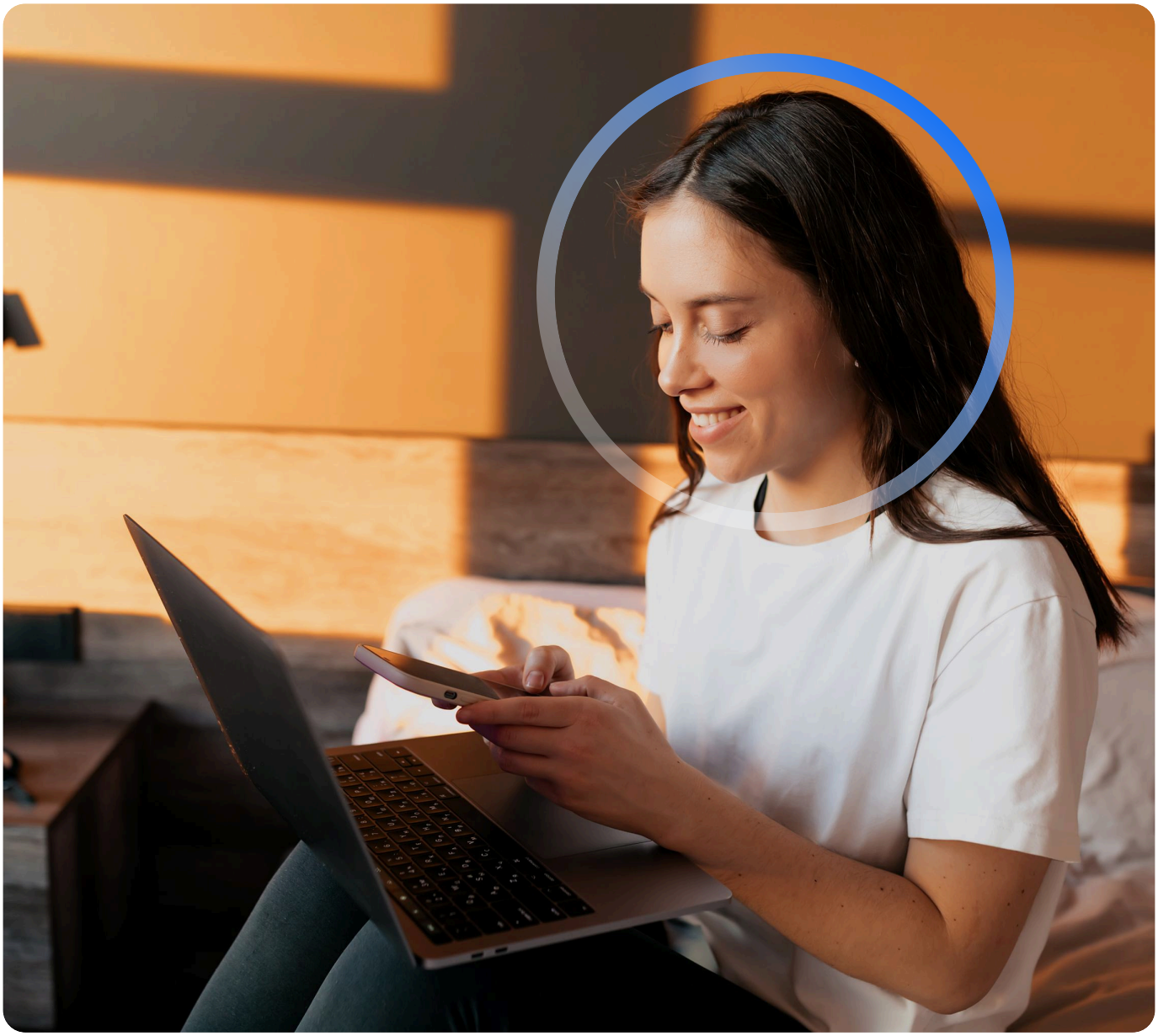
incode

2025

Incode Technologies. contact@incode.com +1 (415) 688-9562 www.incode.com

incode

AI vs. AI: How Businesses Can Beat AI-Powered Fraud with AI-Powered Defenses.



Incode Technologies. contact@incode.com +1 (415) 688-9562 www.incode.com

Introduction: The AI Arms Race in Fraud Prevention

Fraud prevention is no longer about static rules or human oversight – it's an AI arms race. **Fraudsters are using AI to launch more sophisticated, scalable attacks,** and businesses that rely on outdated fraud detection methods will be outpaced.

Cybercriminals leverage **deepfake technology, synthetic identities, and AI-driven automation** to bypass traditional security measures. The only way to stop AI-powered fraud is with AI-powered defenses that **adapt in real time through proprietary machine learning models** specifically trained to detect emerging threats. **Incode is that kind of vendor –** we developed every layer of our technology stack in-house, allowing us to adapt faster than any third-party-dependent IDV vendor.

This guide explores the evolution of AI-driven fraud, its impact across industries, and how businesses can stay ahead with **cutting-edge, proprietary AI technology.**

The Rise of AI-Driven Fraud: How Cybercriminals Leverage AI

1 Deepfake & Synthetic Identity Fraud

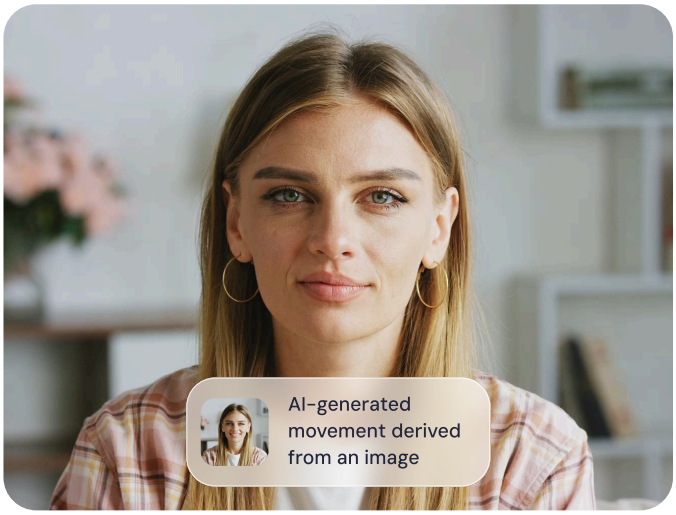
- AI-generated faces and voice-cloning **bypass traditional ID verification.**
- **$25 million stolen** in deepfake CFO scam (2024 case study).
- Synthetic IDs account for **60% of fraud losses** in fintech lending.

2 AI-Driven Document Forgery

- Generative AI tools create **highly realistic fake IDs, passports, and bank statements.**
- **80% of traditional IDV solutions** fail to detect AI-forged documents.
- **Fraud-as-a-Service (FaaS)** platforms offer automated deepfake ID creation.

3 Automated Social Engineering & Account Takeovers

- AI-generated emails & chatbots **mimic real customer interactions.**
- **Credential stuffing & phishing attacks increased 120%** in 2024 due to AI automation.
- Machine-learning-powered fraud bots **bypass CAPTCHAs and MFA.**



Why Traditional Fraud Prevention is Failing

Fraud evolves faster than legacy fraud detection models can adapt. Traditional ID verification, rule-based fraud detection, and manual reviews are too slow to keep up with AI-powered threats.

The Key Weaknesses of Legacy Fraud Prevention:

Static AI Models

Many fraud prevention solutions rely on AI models that update only **every 6-12 months.**

Third-Party Dependencies

Vendors relying on external databases take **weeks or months** to update fraud detection capabilities.

Manual Review Bottlenecks

AI-powered fraudsters operate in real time, while manual fraud reviews introduce **delays and inefficiencies.**

One-Size-Fits-All Approaches

Fraud solutions that treat all users the same **increase friction** for legitimate customers while missing sophisticated fraud patterns.

The Case for Proprietary AI in Fraud Prevention

To combat AI-powered fraud, businesses need **proprietary, real-time AI solutions** that adapt as fast as cybercriminals innovate. **Incode is the only vendor that fully owns and controls its machine learning stack,** allowing us to train our models on specific fraud trends within days.

Real-Time Model Training & Deployment

Incode updates fraud detection models within **days, not months,** ensuring faster adaptation to new fraud patterns.

Full In-House Technology

Unlike third-party-dependent vendors, Incode does not rely on external data providers, which **delays updates** and limits precision.

Multi-Layered Fraud Detection

We combine **liveness detection, behavioral biometrics, and document forensics** to offer unmatched fraud prevention accuracy.

Minimal User Friction

AI-driven decisioning enables **frictionless user verification,** improving conversion rates while blocking fraud.

Incode's Metrics Proving the Power of Proprietary AI:

40+
proprietary AI models running simultaneous fraud checks.

99.65%
accuracy in detecting synthetic ID fraud.

11x
faster onboarding with AI-driven automation.

50%
reduction in false positives, minimizing unnecessary user friction.

Industry Applications: How Different Sectors Are Adapting

AI-powered fraud isn't limited to fintech—it's impacting **e-commerce, gaming, marketplaces, travel, and gig economy platforms.**

Fintech & Financial Services

- AI-powered fraud accounts for **$40 billion in projected losses by 2027.**
- Real-time AI fraud detection **increases loan approval accuracy by 30%.**
- **Behavioral biometrics** reduce account takeovers by 70%.

E-Commerce & Marketplaces

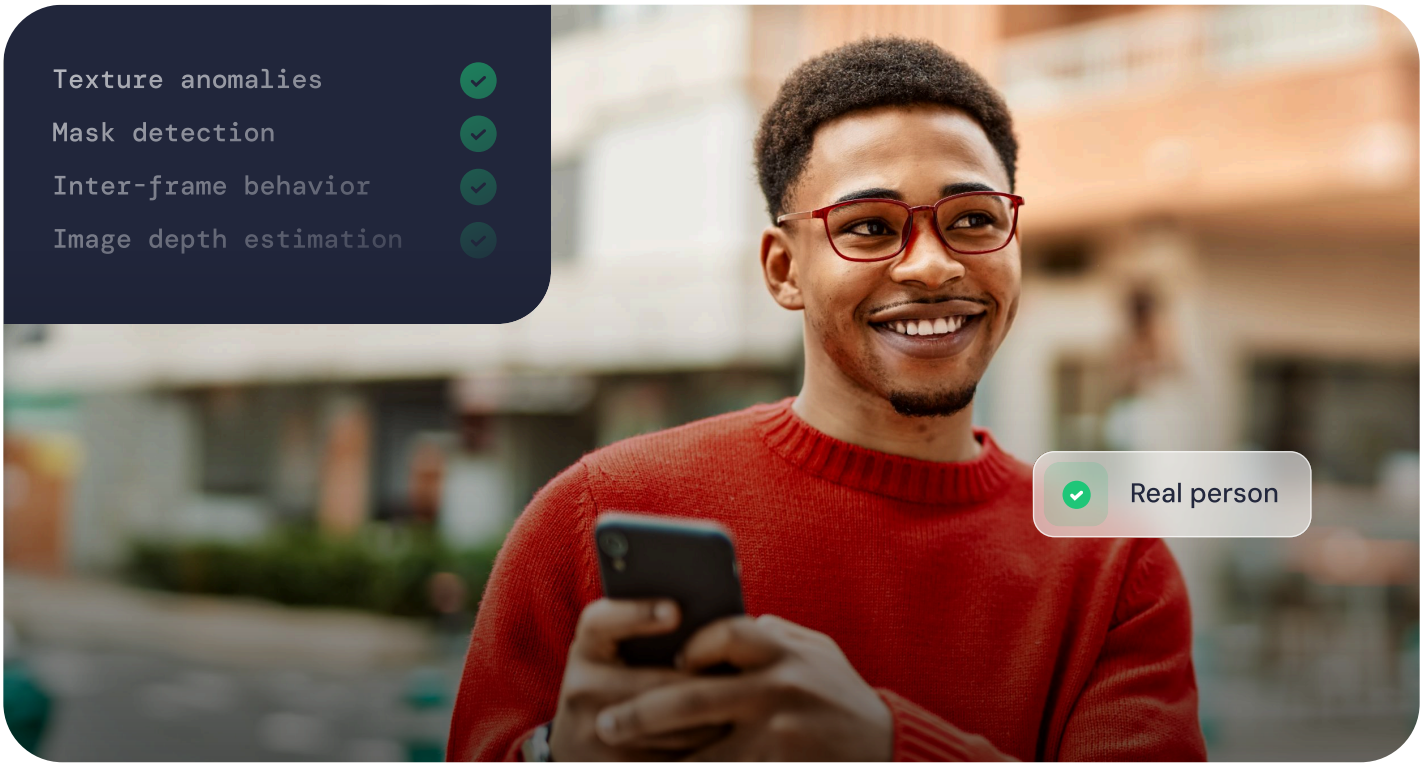
- Fraud bots attack marketplaces every **17 seconds.**
- **Synthetic review fraud** increased by 80% in 2024.
- AI-driven risk scoring reduces **fraud chargebacks by 35%.**

Gig Economy & Rideshare Platforms

- **Fraudulent driver accounts** increased 120% in 2024 due to synthetic identities.
- **AI-powered IDV reduces** fake account creation by 60%.
- Automated fraud detection ensures **faster worker onboarding** without sacrificing security.

Travel & Hospitality

- Deepfake-driven hotel & airline **scams surged 90% year-over-year.**
- **AI verification reduces** booking fraud by 50%.
- Biometric check-in solutions enhance security **without impacting customer experience.**



The Fraud Prevention Playbook: What Businesses Need to Do Now

Businesses that want to stay ahead of AI-powered fraud must **invest in real-time, proprietary AI solutions** that provide faster fraud detection, lower user friction, and seamless compliance.

Immediate Actions:

- Audit your current fraud detection system for **third-party dependencies.**
- **Implement behavioral biometrics and passive liveness detection.**
- **Upgrade to real-time fraud detection models** that adapt faster.

Mid-Term Strategy:

- Automate fraud detection and compliance tracking for **scalability.**
- Deploy **real-time biometric authentication** to reduce synthetic identity fraud.
- Improve onboarding workflows to **boost conversions while reducing fraud risks.**

Long-Term Vision:

- **Continuously work with a KYC vendor** to train proprietary AI models to stay ahead of fraud evolution.
- Ensure **global adaptability,** supporting fraud prevention across multiple regions and regulatory environments.
- Use an **AI-driven fraud intelligence network** to anticipate emerging threats before they reach scale.

Conclusion: The Future of AI-Powered Fraud Prevention

The battle against fraud is now AI vs. AI - and **only businesses with proprietary, real-time AI defenses will thrive.**

Companies must adopt multi-layered fraud detection, real-time AI adaptation, and frictionless user verification to ensure secure, seamless business growth.

Incode's proprietary AI models give businesses the ability to adapt to fraud trends within days, unlike vendors who rely on third-party updates that take months.

Want to learn more?

For more insights on future-proofing business growth, visit Incode.com.

Request a demo today