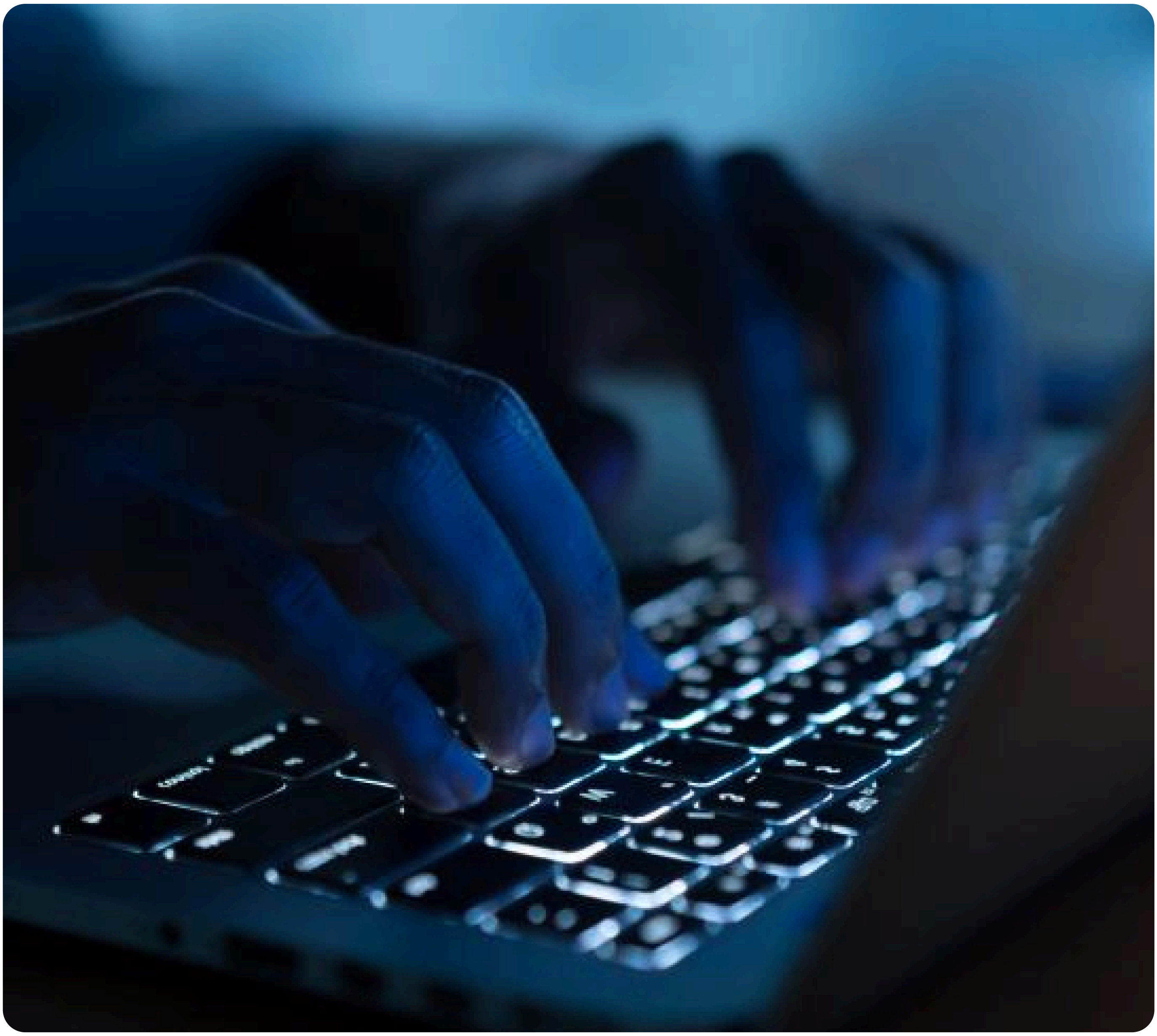
incode

2025

incode

The Fraud Industry: How Cybercriminals Run Scalable, AI-Powered Enterprises.



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

Introduction: Fraud as a Business

Fraud is no longer a game of lone hackers or opportunistic scammers. It has evolved into a full-fledged industry - complete with structured operations, technological advancements, and global market dynamics. Cybercriminals now operate like startups, leveraging **Fraud-as-a-Service (FaaS)** platforms to scale their attacks, automate operations, and optimize for higher "conversion rates."

As businesses adopt AI to improve efficiency, fraudsters do the same. Generative AI, deepfake technologies, and automation tools have supercharged fraud, making it more efficient, scalable, and harder to detect.

In this eBook, we explore how cybercriminals operate like legitimate tech enterprises, how fraud adapts faster than traditional security measures, and what businesses across industries must do to stay ahead.

How AI Supercharged Cybercrime

The Evolution from Small-Scale Hacks to Industrialized Fraud

Fraud has shifted from isolated cyberattacks to mass-scale, automated crime networks. With AI-driven tools, criminals can:

- Generate **synthetic identities** at scale.
- Bypass ID verification with **deepfake technology.**
- Automate phishing attacks and scam campaigns with **minimal human involvement.**
- **Distribute fraud tools globally** via underground marketplaces.

The Metrics Behind AI-Powered Fraud:

54.55%

of professionals report concerns about deepfake and synthetic identity fraud - even if they haven't faced an attack directly.

40%

believe AI-driven fraud is underreported, suggesting that businesses are unaware of the full extent of their vulnerabilities.

70%

express significant concerns about privacy risks when sharing ID documents with human agents - driving the demand for automated fraud detection.

30x

increase in deepfake fraud from 2022 to 2023, making most current solutions obsolete.

Fraud-as-a-Service: The Business Model Behind Cybercrime

How FaaS Works:

Much like software companies offer Software-as-a-Service (SaaS), cybercriminals now provide Fraud-as-a-Service (FaaS) - allowing even non-technical actors to launch sophisticated attacks.

Subscription-Based Fraud

Criminals sell monthly subscriptions to fraud toolkits, just like SaaS businesses.

Customer Support for Criminals

Some platforms offer 24/7 chat support for troubleshooting hacking tools.

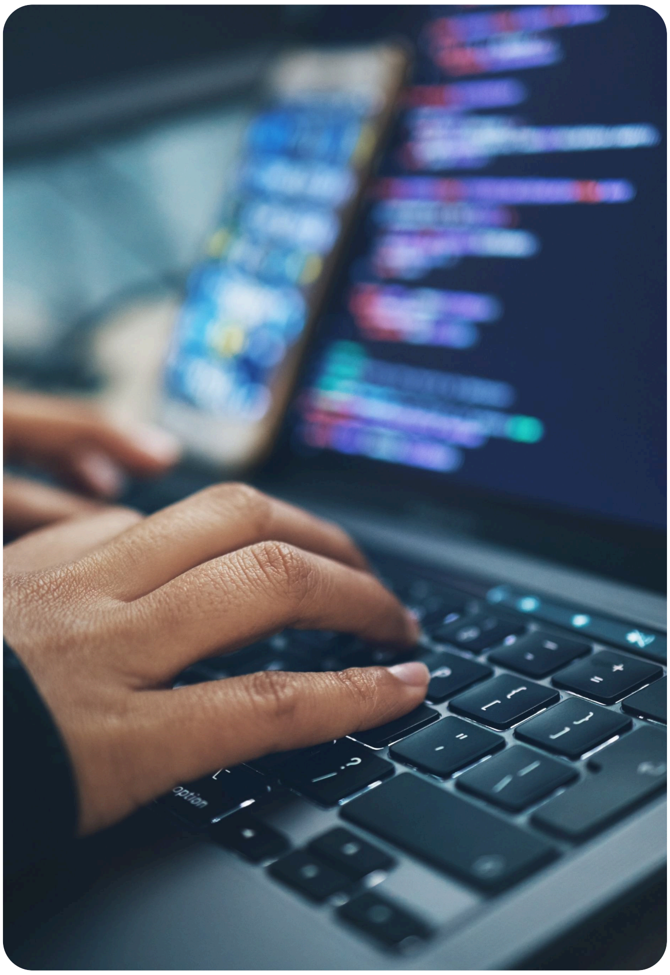
On-Demand Attacks:

Buyers can order phishing campaigns, deepfake ID creation, or account takeover attacks on demand.

Scalability & Automation:

AI-powered bots handle thousands of fraud attempts simultaneously.

Real-World FaaS Cases:



$25 million CFO deepfake scam:

A global engineering firm lost millions after an employee followed fraudulent video call instructions from an AI-generated CFO impersonation.

Deepfake-driven political robocalls:

AI-generated voices of politicians urged voters to click malicious links during elections.

Marketplace account hijacking:

Fraudsters used synthetic identities to take over accounts in ride-sharing and freelance gig platforms, stealing earnings from legitimate workers.

Industries at Risk: Beyond Finance

While fintech is a major target, fraud is expanding into every digital industry. Businesses in marketplaces, hospitality, travel, igaming, and the gig economy are increasingly in cybercriminals' crosshairs.

E-Commerce & Marketplaces: Automated Fake Accounts

- **Bots generating fake user accounts** to exploit promo discounts.
- **Stolen credit cards** used in Buy-Now-Pay-Later (BNPL) scams.

Travel & Hospitality: Fake Bookings & Identity Fraud

- **Synthetic IDs** used for hotel check-ins, bypassing security measures.
- **Stolen payment details** used for luxury travel fraud.

Gig Economy: Freelancer & Rideshare Fraud

- **Fake Driver & Delivery Accounts:** Fraudsters create synthetic gig worker identities, undermining platform trust.
- **Payment Fraud:** Exploiting payout systems to steal wages from real workers.

Crypto & DeFi: Synthetic Identity Scams

- **Fake KYC documents** used to launder illicit funds.
- **Deepfake influencers** promoting fake investment schemes.

Why Businesses Struggle to Keep Up

Fraudsters iterate faster than security teams, adapting to new detection methods in weeks.

The key challenges for businesses are:

- **Slow Response Times:** Many ID verification vendors take months to update fraud detection models, leaving businesses vulnerable.
- **Reliance on Third-Party Solutions:** Many security vendors depend on third-party data sources, making their fraud detection capabilities outdated.
- **High Friction, Low Security:** 70% of users abandon onboarding when verification processes are too complex - yet weak security leads to costly fraud losses.

The Future of Fraud: What's Next?

With AI-driven fraud evolving rapidly, businesses must adopt real-time, AI-powered fraud prevention solutions to stay ahead.

Looking toward 2030:

- **Fraud models will evolve in days –** organizations relying on solutions that can't adapt quickly will face mounting losses.
- **Deepfake attacks will become mainstream –** businesses must integrate liveness detection and behavioral biometrics.
- **FaaS will continue expanding –** fraud tools will become more accessible and more sophisticated.
- **Regulatory pressure will increase –** governments worldwide will tighten ID verification and fraud prevention regulations.

How Businesses Can Prepare

Fraud is now a fully industrialized sector – businesses must treat fraud prevention as an essential investment, not just a compliance measure.

Key Recommendations:

- Adopt AI-powered fraud detection to counter AI-driven attacks.
- Minimize third-party reliance – proprietary technology ensures faster fraud adaptation.
- Implement multi-layered verification – combine liveness checks, document forensics, and behavioral biometrics.
- Stay agile – fraud adapts in days, your defenses should too.

Fraud isn't slowing down. Businesses that fail to evolve will find themselves outpaced by cybercriminals who treat fraud as a scalable, AI-driven enterprise.

Want to learn more?

Let's discuss how Incode can help Despegar scale effortlessly across LATAM.

Request a demo today