incode

2025

incode

The Hidden Flaws in Fraud Prevention: Why Proprietary AI models are the Future.

Introduction: Why Legacy Fraud Prevention is Failing

As fraud becomes increasingly sophisticated, businesses are realizing that traditional identity verification (IDV) systems are **too slow, too rigid, and too dependent on third-party technology** to keep up. Cybercriminals are leveraging AI at an unprecedented scale, using deepfakes, synthetic identities, and automated fraud techniques to bypass outdated verification measures.

The problem? **Most IDV vendors don't control their own fraud detection technology.** Instead, they rely on licensed third-party models that take **months to adapt** to new fraud patterns. Meanwhile, fraudsters iterate in **days or even hours.**

To effectively combat modern fraud threats, businesses need a **fully proprietary AI-driven fraud prevention system—**one that adapts to fraud in **real-time,** eliminates reliance on external vendors, and offers industry-leading accuracy.

In this guide, we'll expose the hidden flaws in traditional fraud prevention and explain why **proprietary AI is the only way forward.**

The Broken State of Third-Party ID Verification

1 Slow Adaptation to Fraud

- Third-party IDV providers **license their AI models from external vendors,** meaning they have no direct control over fraud detection updates.
- It takes **months** for these vendors to roll out updates for emerging fraud techniques, leaving businesses exposed to attacks.
- In contrast, **fraudsters constantly refine their attacks—**new deepfake and synthetic identity threats emerge weekly, if not daily.

3 Limited Customization & Industry Adaptability

- Third-party AI models **aren't designed for specific industries or regional fraud patterns.**
- A company operating in **Latin America** may face different fraud tactics than one in **Europe,** yet legacy vendors offer **one-size-fits-all fraud detection.**
- Without proprietary AI, businesses **can't fine-tune fraud detection models to their exact needs.**

2 High False Positive & False Negative Rates

- **Traditional IDV tools often use blunt-force fraud detection techniques,** which leads to false positives (blocking legitimate users) and false negatives (letting fraudsters slip through).
- **Example:** A fintech company using a third-party IDV provider **saw a 15% increase in legitimate users being wrongly flagged as fraud** because their vendor's fraud detection algorithm was too outdated.

4 Lack of Compliance Agility

- **Regulatory landscapes shift constantly** (GDPR, AI Act, CCPA, KYC/AML updates). Businesses relying on third-party AI models struggle to adapt quickly.
- **Delayed compliance** updates can result in regulatory fines and reputational damage.

Key Takeaway:

Legacy fraud prevention systems lack the agility, accuracy, and adaptability needed to combat modern fraud. The only way forward is a fully proprietary AI system.

The Power of Proprietary AI in Fraud Prevention

Why Proprietary AI is the Future

A proprietary AI-driven fraud prevention system is built from the ground up. This allows for:

Real-time fraud model updates

Adapting to new attack vectors within days, not months.

Industry-specific fraud detection

Customizing models for fintech, e-commerce, crypto, travel, and gig economy fraud patterns.

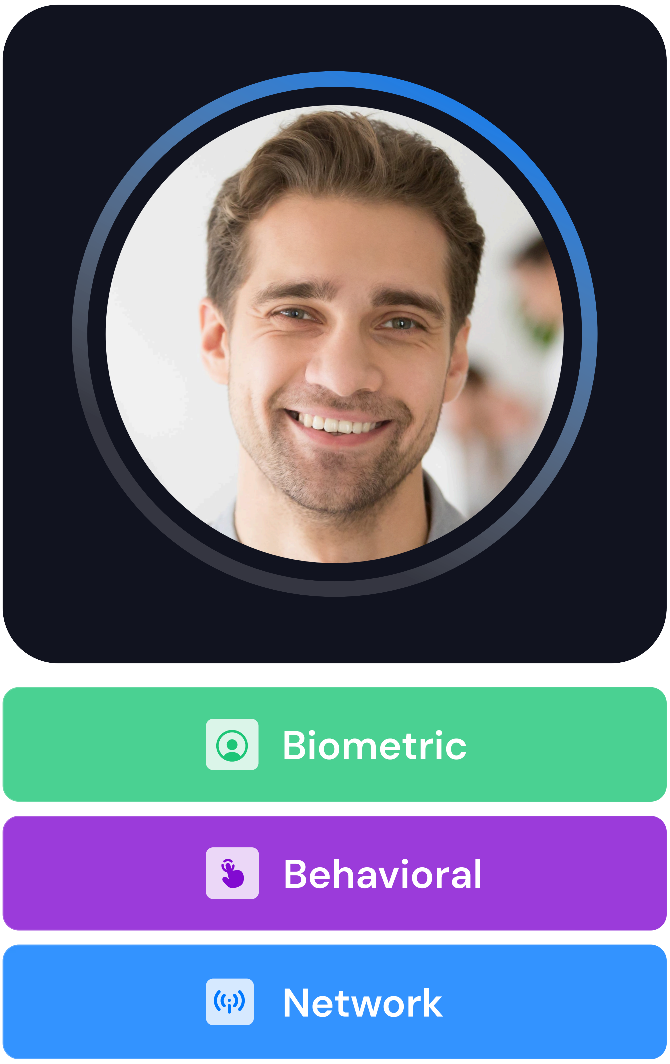
Seamless user experience

Reducing false positives and eliminating unnecessary friction.

Regulatory adaptability

Quickly implementing compliance updates across multiple markets.

Incode's Proprietary AI in Action



Unlike third-party-dependent IDV vendors, Incode owns 100% of its AI stack.

This means:

- We analyze fraud patterns in **real-time,** training our models specifically on the fraud challenges our customers face.
- **We don't wait for external vendors to push updates —** we adapt fraud detection strategies immediately.
- **Our proprietary liveness detection** ensures that businesses verify real people, not AI-generated deepfakes.

Incode's Fraud Prevention Metrics

99.65%
accuracy in detecting synthetic identity fraud.

50%
lower false positive rate than third-party IDV vendors.

11x
faster onboarding times due to AI-driven automation.

98.53%
True Positive Rate (TPR) for selfie-to-ID verification.

Ranked #1
in NIST FRVT testing for accuracy and speed among IDV providers.

The Role of Digital Personhood in Fraud Prevention

The Evolution of Identity Verification

In the past, verifying identity meant checking a government-issued ID against a database. **But modern fraud techniques have outpaced this approach.**

Digital Personhood: Beyond Basic ID Checks

Identity is more than a set of credentials on an ID card. Digital personhood includes:

- **Biometric & behavioral patterns** (e.g., facial expressions, motion analysis).
- **Social & contextual interactions** (e.g., previous relationships, transaction history).
- **Liveness detection—**verifying that a real person is present, not an AI-generated deepfake.

The Risks of Ignoring Digital Personhood

Without advanced personhood verification, businesses risk:

- **Falling victim to deepfake fraud,** where AI-generated faces and voices impersonate real users
  .
- **Losing legitimate customers** due to overly aggressive fraud filters.
- **Data breaches and identity theft**, as centralized ID databases remain a key target for hackers.

How Incode Enhances Digital Personhood Verification

- **Multimodal Liveness Detection:** We integrate physical, digital, and behavioral liveness checks to detect deepfakes, synthetic identities, and bot-driven fraud.
- **AI-Driven Behavioral Analysis:** Our system evaluates user interactions in real time, identifying suspicious activity before fraud occurs.
- **Passive & Active Verification:** We offer seamless, real-time verification without requiring unnecessary user actions, reducing friction in onboarding.

Industry Use Cases: How Proprietary AI is Transforming Security

Fintech & Payments

- Prevents synthetic identity fraud in loan applications.
- Reduces false positives in transaction monitoring.

E-Commerce & Marketplaces

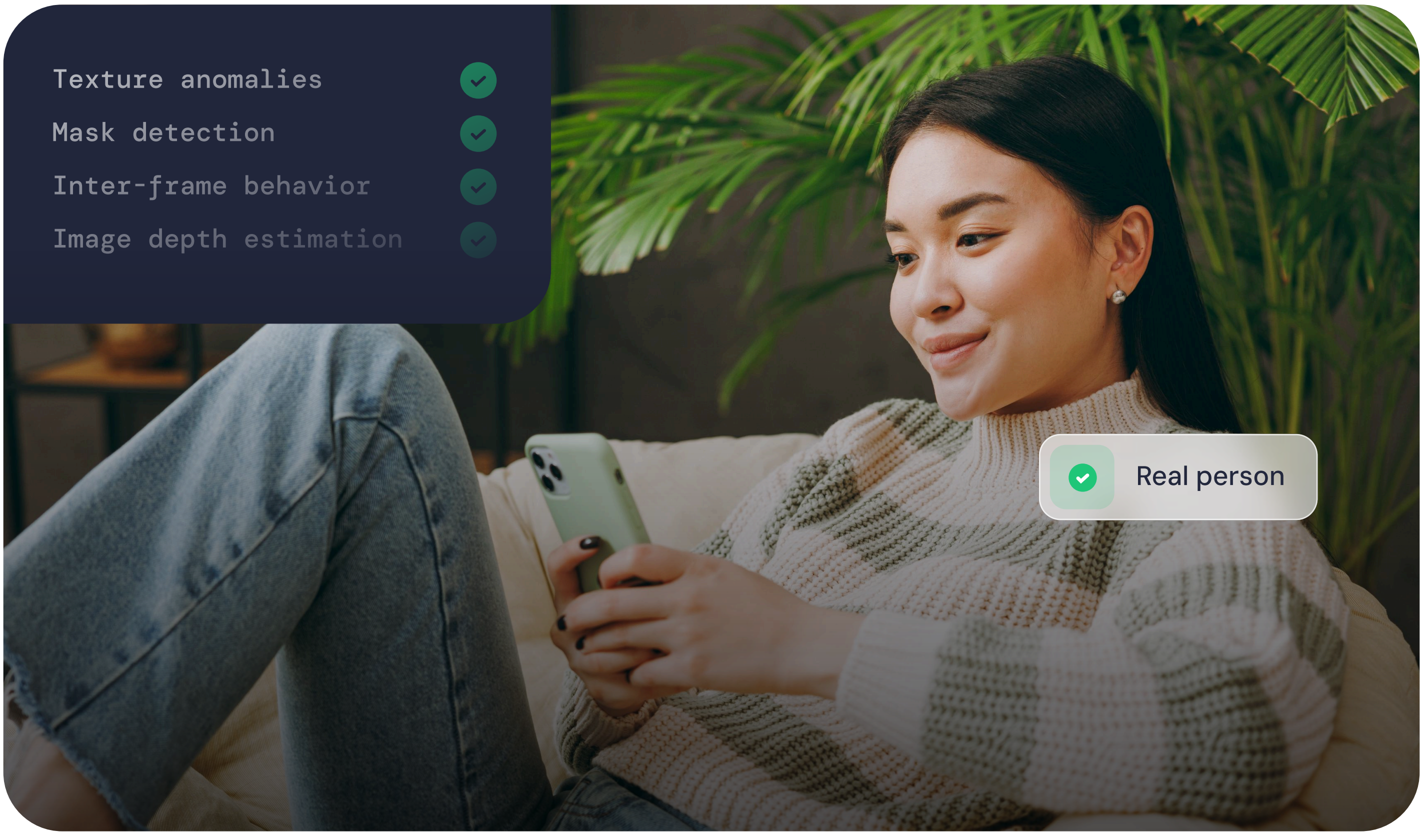
- Blocks automated bot-driven fake accounts.
- Prevents chargeback fraud using behavioral biometrics.

Gig Economy & Rideshare Platforms

- Detects fraudulent driver profiles created with stolen identities.
- Uses liveness detection to prevent fake account farming.

Crypto & Web3

- Prevents deepfake-based KYC fraud.
- Ensures regulatory compliance with AI-driven identity verification.



Leading businesses don't let security and compliance roadblocks stall their growth. They invest in **scalable, proprietary technology** that eliminates fraud risks while optimizing customer experience.

The Future of Fraud Prevention: What Businesses Must Do

Ditch Third-Party AI Vendors

Audit your current fraud detection stack—**does it rely on external AI models?**

Implement Real-Time Fraud Detection

Adopt an AI-native fraud prevention solution that updates models within days, not months.

Use Multi-Layered Identity Verification

Combine liveness detection, document forensics, and behavioral analytics to stop fraud before it happens.

Prioritize Compliance & User Experience

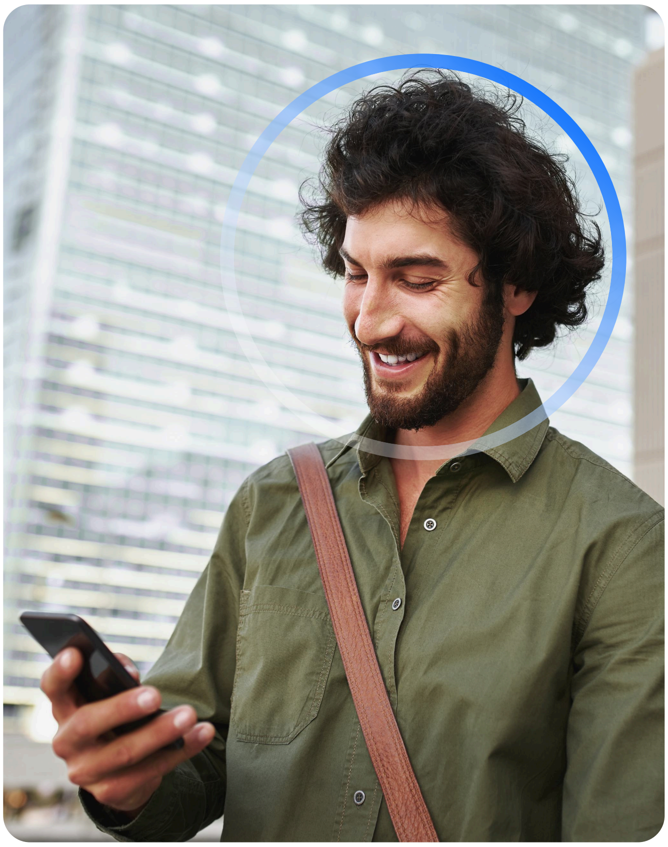
Ensure fraud prevention doesn't create friction for legitimate users.

Conclusion: Why Incode is the Future of AI-Driven Fraud Prevention

At Incode, we own and control 100% of our AI stack, allowing us to:

- Adapt to fraud within days, not months.
- Deliver frictionless, AI-driven identity verification.
- Keep businesses ahead of evolving fraud threats without third-party limitations.

The future of fraud prevention belongs to businesses that invest in proprietary, real-time AI solutions.



Want to learn more?

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

Request a demo today