How to turn risk data into profit protection, operational automation, and smarter growth decisions

YOUR ANTI-FRAUD KNOWS MORE THAN YOU USE

frog

A 7-MINUTE GUIDE FOR IGAMING OPERATORS

TABLE OF CONTENTS

Why are you only using 30% of your risk tech? 03

Device Fingerprinting: genuine growth vs fake growth 05

Scoring Engine: why doesn't every risk require a block? 07

Real-Time Monitoring: why morning reports are too late? 09

How to scale without drowning in manual review 11

The hidden profit engine inside your anti-fraud 13

The 5 benchmarks of a scalable anti-fraud infrastructure 16

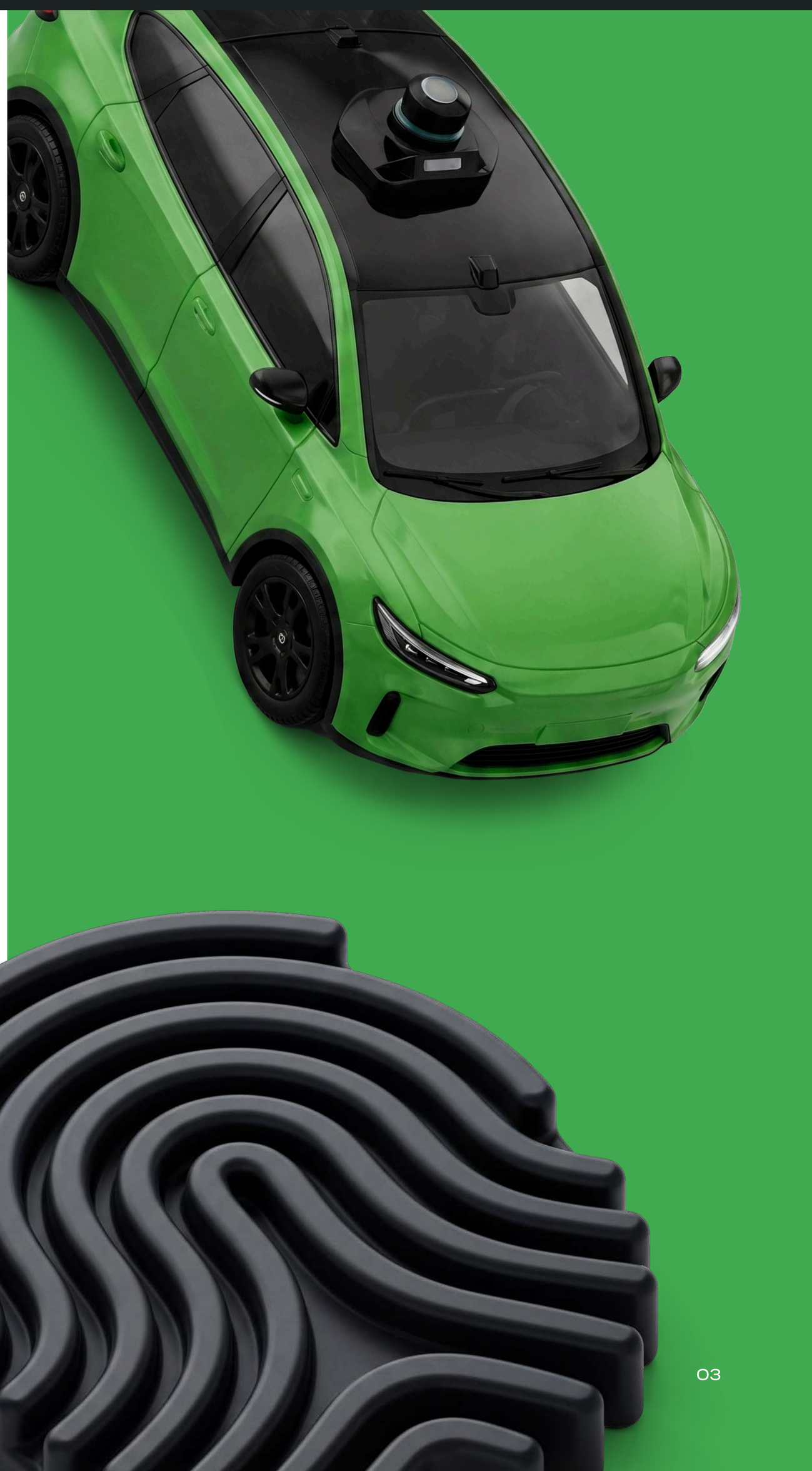
frogo

WHY ARE YOU ONLY USING 30% OF YOUR RISK TECH?

If you treat anti-fraud like an airbag, it only deploys after the crash. By then, the damage is done: a fraud ring has cleared payouts, a bonus campaign is drained, or a rigid rule has blocked a high-value VIP.

When risk tech is purely reactive, it's just an expensive tax on your growth. **Modern anti-fraud should be your business autopilot.**

The exact same data and tools you use to catch bad actors can be integrated directly into your daily operations to protect your margins, clean up your traffic, and automate your scale.





30%

WHAT MOST TEAMS ALREADY USE:

alerts · fixed limits · basic rules · manual reviews · post-incident blocks

BUSINESS ROLE:
detect and stop visible fraud

LIMITATION:
reactive, manual, hard to scale

70%

WHAT OFTEN STAYS UNDERUSED:

behavioral analysis · device intelligence · graph networks · dynamic risk scoring · real-time monitoring · automation · cross-team insights

BUSINESS ROLE:
protect margin, automate decisions, fuel growth

LIMITATION:
lower ops load, higher-quality traffic, faster payouts, smarter scaling

Where is your business bleeding cash right now?

Over the next few pages, we'll look at this underused 70% and show you how to turn raw risk data into automated operations.

DEVICE FINGERPRINTING:

THE DIFFERENCE BETWEEN GENUINE GROWTH AND FAKE GROWTH

When a marketing campaign spikes, your CRM reports a wave of "New Players."

But in iGaming, abusers rarely use a device just once. Basic tracking, like cookies or IPs, won't catch them – sophisticated fraud rings easily bypass these using proxies, virtual machines, and anti-detect browsers.

If your team only spots a multi-accounter after they've drained a bonus or cleared a payout, your defense is simply lagging.

Device Fingerprinting looks beyond the surface. By analyzing deep hardware configurations and browser attributes, it identifies the actual device behind the click, connecting the dots before a fraudster can do any damage.

BEFORE

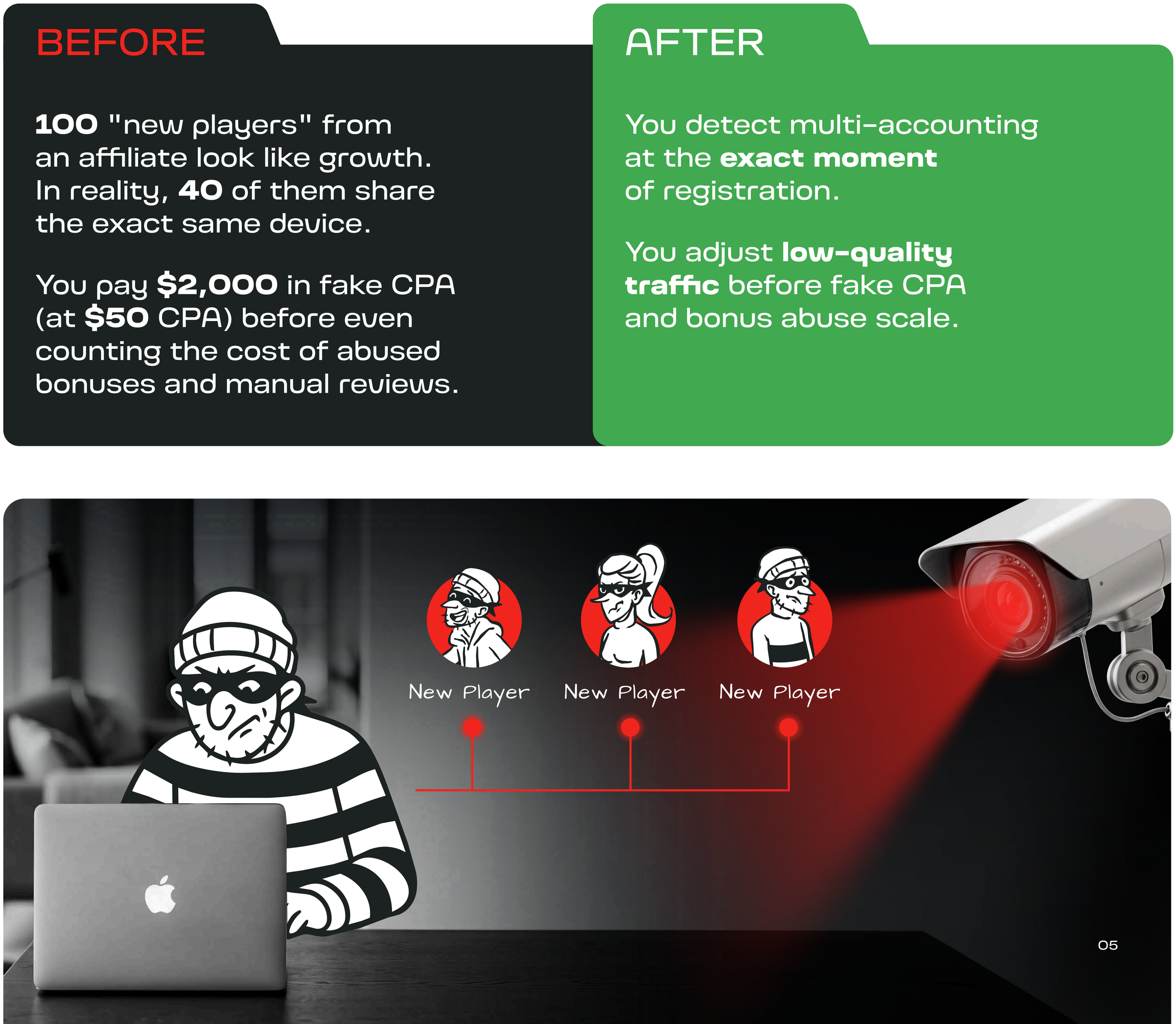
100 "new players" from an affiliate look like growth. In reality, **40** of them share the exact same device.

You pay **$2,000** in fake CPA (at **$50** CPA) before even counting the cost of abused bonuses and manual reviews.

AFTER

You detect multi-accounting at the **exact moment** of registration.

You adjust **low-quality traffic** before fake CPA and bonus abuse scale.



QUICK AUDIT

DO YOU KNOW YOUR REAL MULTI-ACCOUNTING RATE?

- ○ YES
- ○ NO

If the answer is “no”, your “new player” growth may include connected accounts, recycled users, and bonus hunters you are still paying for.

SCORING ENGINE:

NOT EVERY RISK NEEDS A BLOCK

€10,000

Many operators rely on basic rules:

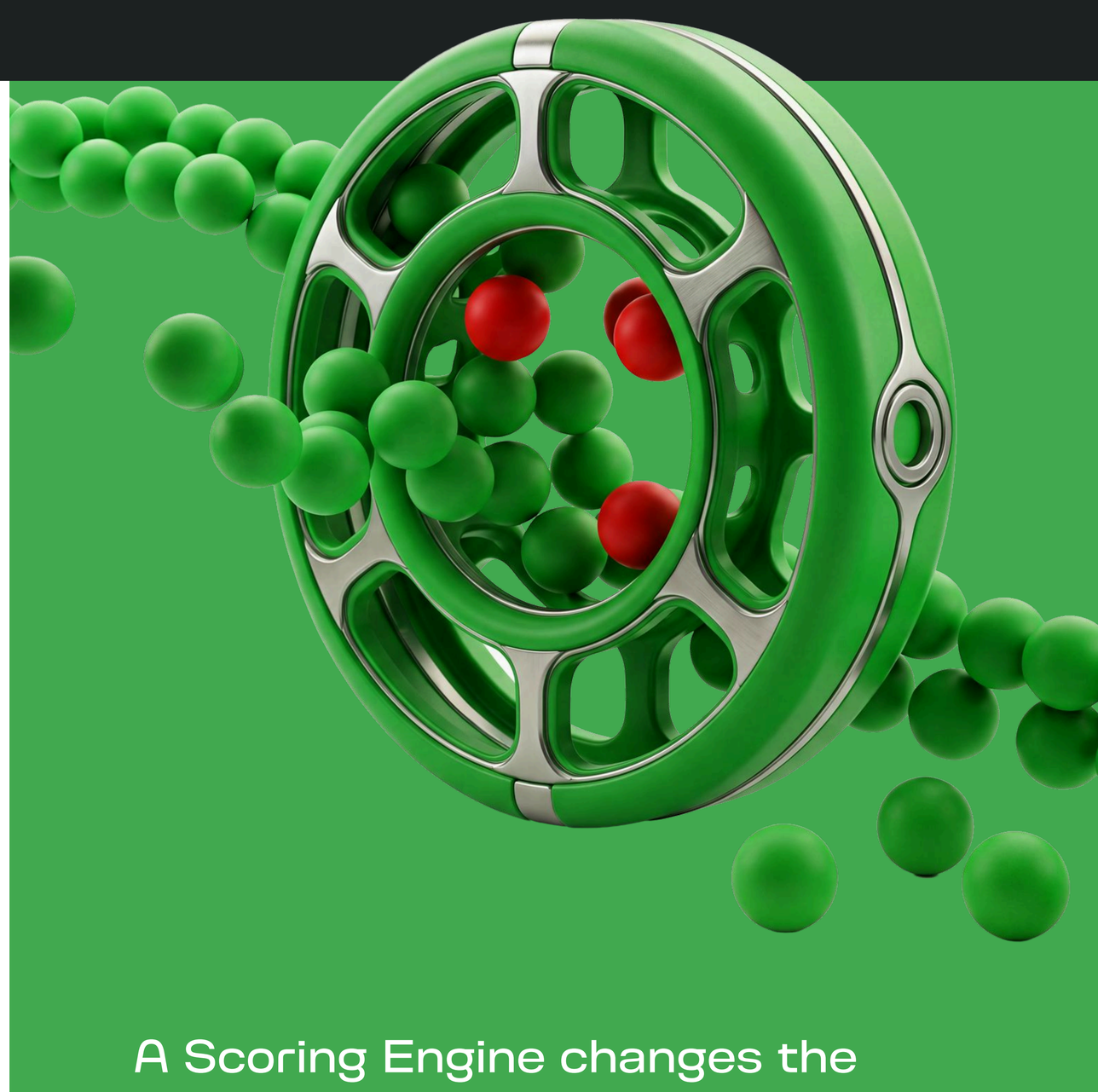
for example, every withdrawal above €10,000 goes to manual review. It feels safe, but it quickly creates noise.

~99%

But ~99% of large withdrawals are not fraud.

Often, it is simply a legitimate player who has won, plays at higher stakes, or cashes out more frequently. And if the same player triggers that rule several times a day, the team keeps reviewing the same low-risk case again and again.

The result: operational time is wasted, good players face additional friction, and retention quietly takes the hit.



A Scoring Engine changes the logic. Instead of treating every unusual action the same way, it functions like a precision filter that combines risk factors to separate real risk from normal player behavior.

THE SHIFT

BEFORE

100% MANUAL REVIEWS

Your team spends **1,5+ hours** every day filtering noisy alerts and manually reviewing safe, borderline payouts.

As traffic grows, the review queue explodes. Good players wait longer, and high-risk attacks get buried in the noise.

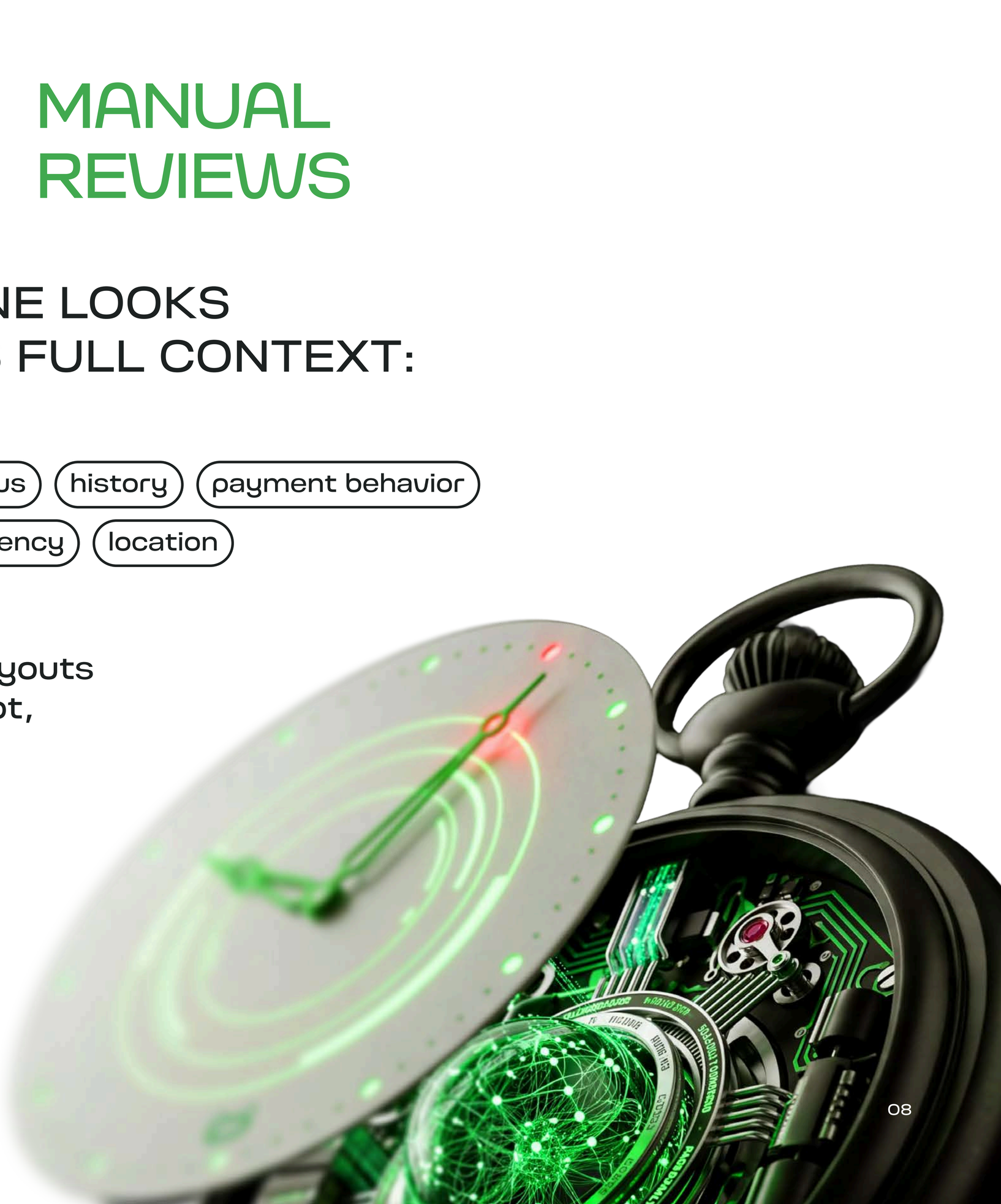
AFTER

1,5% MANUAL REVIEWS

A SCORING ENGINE LOOKS AT THE PLAYER'S FULL CONTEXT:

game activity · account status · history · payment behavior · device signals · payout frequency · location

Up to **98%** of low-risk payouts are processed on autopilot, while analysts focus only on critical cases.



frogo

QUICK AUDIT

DOES YOUR RISK LOGIC ADAPT TO EACH PLAYER'S BEHAVIOR?

- ○ YES
- ○ NO

If not, you may be applying the same rigid rules to VIPs, casual players, new users, and real fraudsters. That means slower payouts for good players, weaker retention, and lower LTV.

REAL-TIME MONITORING:

WHY MORNING REPORTS ARE TOO LATE?

By the time your team sees the pattern in a report, the damage may already be done:

the payout has cleared, the bonus budget is gone, the traffic source has been paid, or the same fraud cluster has already moved to the next account.

Real-time monitoring changes that. It tracks critical actions as they happen: registrations, deposits, withdrawals, bonus activations, and other high-risk events.

To prevent leaks, your risk engine must track critical actions in real time.

Instead of making analysts dig through backend logs, a modern setup pushes instant alerts directly to where your team actually works.

Suspicious patterns can surface while there is still time to act.

SIGNAL	EARLY ACTION	LOSS PREVENTED
50 accounts from the same IP or device	Detect registration spikes instantly	Avoid rising verification costs
A single device is attempting multiple cards	Catch the card-testing pattern	Reduce chargeback risk
Unusual withdrawal behavior (GEO/method mismatch)	Flag before payout	Stop money from leaving the platform
Connected accounts reusing promo codes	Detect bonus abuse early	Protect bonus budget

REAL-TIME MONITORING



SEE THE PATTERN EARLIER



REACT FASTER



PREVENT RISK FROM TURNING INTO LOSS

QUICK AUDIT

In your last fraud case, how much time passed between the first signal and the team’s reaction?

- ◯ Less than 5 minutes
- ◯ Within the same day
- ◯ Within an hour
- ◯ We only saw the damage in a report

If it takes longer than 5 minutes, your monitoring is closer to reporting than real-time prevention.

HOW TO SCALE

WITHOUT DROWNING IN MANUAL REVIEW

If x10 your traffic means you need to x2 your risk team just to process payouts, your business model isn't scalable.

To grow safely over the next 3 to 5 years, you must disconnect transaction volume from your operational headcount.

A high-end anti-fraud system acts as a silent filter – processing legitimate traffic in milliseconds so you can scale traffic without expanding your risk department.



OPERATIONAL HEADCOUNT

QUICK AUDIT

Can your risk setup scale without adding more manual work?

- [ ] Can your system safely auto-approve more than 95% of payouts in milliseconds without human intervention?
- [ ] Do your rules adapt to normal traffic patterns instead of flooding the team with false positives when marketing scales?
- [ ] Can your blacklists and whitelists update automatically via API instead of forcing analysts to copy-paste IPs, cards, affiliates, or emails by hand?

If the answer is “no” to any of these, your anti-fraud setup may not be ready for volume growth.

The point of advanced anti-fraud tech is to automate your operations so you can double your volume while keeping your overhead completely flat.

frogo

THE HIDDEN PROFIT ENGINE

INSIDE YOUR ANTI-FRAUD

Most executives treat anti-fraud as a mandatory expense, just a wall to keep the bad guys out.

But look at it from a risk specialist's perspective. A solid anti-fraud system is a massive stream of real-time user data.
It continuously captures exact behavioral logs, device fingerprints, and transaction flows.
And the best part? You've already paid for this data.

When you share these specific data points across your company, your anti-fraud tech stops being a cost center and starts directly driving revenue.

HERE IS HOW DIFFERENT TEAMS CAN USE YOUR ANTI-FRAUD LOGS DAILY:

VIP-Support	Detect potential VIPs early, solve login or payment issues before complaints, and recognize already known players across brands, products, or GEOs
Payments	Monitor payment health, spot conversion anomalies, and route trusted or risky traffic through the right payment paths
Affiliate Managers	Detect CPA fraud, audit traffic quality before payouts, and use graphs to reveal multi-accounting clusters or proxy traffic
Product team	Catch anomalies in key business metrics, detect abused flows, and protect against SMS fraud or automated registrations
Internal Security	Monitor suspicious employee behavior, risky manual approvals, employee play, and internal account misuse

QUICK AUDIT

How many teams use your anti-fraud data today?

- ○ Risk only
- ○ Risk + Payments
- ○ Risk + 2–3 business teams
- ○ Risk, Payments, VIP, Affiliate, Product, Security, Retention, Marketing

Anti-fraud shouldn’t be an isolated Risk tool. A scalable setup connects teams around the same risk signals, so the whole business can make faster decisions, reduce costs, protect revenue, and find new growth opportunities.

frog

5 BENCHMARKS

OF A SCALABLE ANTI-FRAUD INFRASTRUCTURE

When your risk technology is used to its full potential, your operational metrics shift from cost-heavy to profit-driven.



98%

auto-payout rate



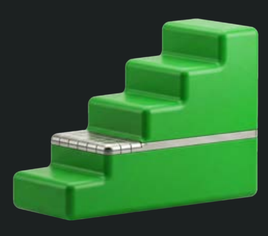
1:50K

1 analyst per 50,000+ MAU



0.5 sec

onboarding scoring



LTV>0

Fraud-user LTV above zero



<5 min

Manual fraud-incident review under 5 minutes

THIS IS WHY WE BUILT FROGO

Frogo is the anti-fraud platform that combines all of these capabilities into a single system.

We act as a proactive technology and risk partner, helping your team integrate the API, configure risk logic, optimize scoring for your traffic patterns, and turn raw risk signals into useful insights.

frogo

SEE IT IN ACTION

WE'LL SHOW YOU EXACTLY HOW FROGO CAN PUT YOUR PLATFORM'S RISK MANAGEMENT ON AUTOPILOT

BOOK A DEMO



frogo