

FREE SAMPLE CHAPTER

THE BACKEND OF LUCK

Engineering the Online Gambling Platform

IN THIS SAMPLE

Geofencing and Location Verification

From Volume 4: Compliance, Player Safety, Data Residency, and Governance

GUSTAVO LIMA

THEBACKENDOFLUCK.COM

Chapter 24e: Geofencing and Location Verification

Location verification in online gambling isn't a nice-to-have feature; it's a legal requirement that determines whether your platform can operate at all. In the US, state-by-state licensing means a player 500 meters across the New Jersey border into Pennsylvania needs to be verified against the correct jurisdiction's rules. In Europe, it determines which regulatory framework applies and what responsible gaming controls you enforce. Get it wrong and you're offering unlicensed gambling, which is a criminal offence in most jurisdictions.

This chapter covers the multi-signal location verification system used in production iGaming platforms: IP geolocation with MaxMind, GPS validation for mobile, VPN/proxy detection, Cloudflare edge geo cross-referencing, and the jurisdiction matrix that ties it all together.

Multi-Signal Verification Architecture

A single signal isn't enough. IP geolocation is accurate to the city level but can be spoofed. GPS is accurate to meters but only available on mobile. Cloudflare edge headers are hard to spoof but only give country-level precision. You need all of them, cross-referenced against each other.

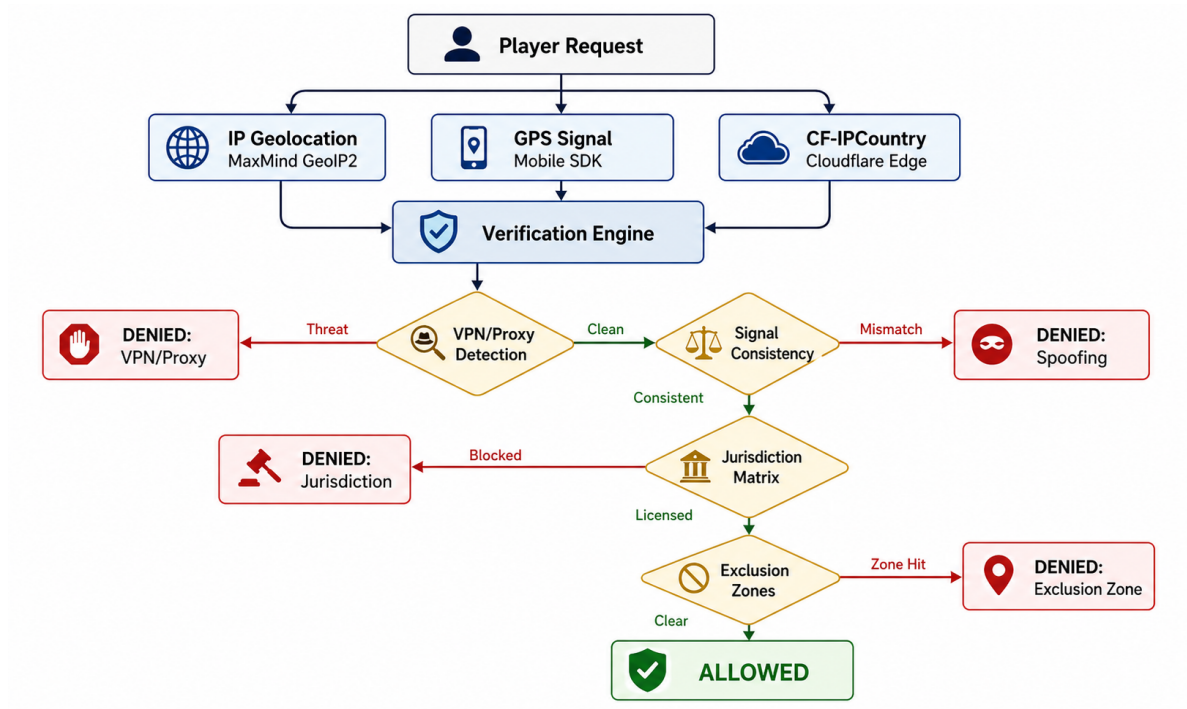


Figure 1: Multi-Signal Verification Architecture.

Script Reference: `scripts/chapter-24/location-verification/geofence.py`: full multi-signal location verification service.

The verification flow runs in this order for a reason:

1. **VPN/proxy detection first.** If the IP is a known VPN exit node, datacenter IP, or anonymous proxy, stop immediately. No amount of GPS data can override this; the player is actively trying to circumvent geofencing.
2. **Signal consistency second.** Cross-reference IP country against GPS country against Cloudflare edge country. If they disagree significantly, the spoofing score rises.
3. **Jurisdiction matching third.** Only after we're confident the location data is genuine do we check whether the player is in a licensed jurisdiction.
4. **Exclusion zones last.** Fine-grained checks like physical casino proximity restrictions only matter if the player is already in the right jurisdiction.

The Jurisdiction Matrix

Every licensed jurisdiction has specific requirements. This isn't a simple "allowed/blocked" list: each jurisdiction carries age limits, currency, game type restrictions, GPS requirements, and re-verification intervals.

Jurisdiction	Min Age	Currency	GPS Required	Re-verify	Game Types
US-NJ	21	USD	Yes	30 min	Slots, Table, Live, Sports
US-PA	21	USD	Yes	30 min	Slots, Table, Live, Sports
US-MI	21	USD	Yes	30 min	Slots, Table, Live, Sports

Jurisdiction	Min Age	Currency	GPS Required	Re-verify	Game Types
GB	18	GBP	No	60 min	Slots, Table, Live, Sports
MT	18	EUR	No	120 min	Slots, Table, Live, Sports
SE	18	SEK	No	60 min	Slots, Table, Live Casino
DK	18	DKK	No	60 min	Slots, Table, Live, Sports
BR	18	BRL	No	30 min	Slots, Table, Live, Sports

Sanctioned and unlicensed countries are blocked at the country level:

Blocked	Reason
KP (North Korea)	International sanctions
IR (Iran)	International sanctions
SY (Syria)	International sanctions
CU (Cuba)	US sanctions
AF, IQ, LY, SD, YE	Conflict zones / no licensing framework
US (country-level)	Blocked; individual licensed states whitelisted

The US is an interesting case: blocked at the country level because you cannot offer online gambling to “the US” generically. You can only offer it to specific states where you hold a license. A player whose IP resolves to “US” without a state-level region code is denied.

US State-Level Precision

US state verification is the hardest geofencing problem in iGaming. Boundary accuracy, permitted tolerance, and approved verification methods are jurisdiction-specific. Treat any numeric threshold, including the 500-metre design target used in this chapter, as configuration rather than a universal GLL-19 requirement. A player in Atlantic City may be eligible under a New Jersey licence, while a player across the state boundary may not be.

In the US deployments modelled here, mobile location uses device-derived location plus independent network and anti-spoofing signals. IP geolocation alone is not sufficient for a high-confidence boundary decision because:

1. Mobile carriers often route through out-of-state gateways
2. IP-to-location accuracy drops to city level at best on cellular networks
3. Applicable regulations and approved controls may require the operator to establish the physical location of the device and prevent location fraud

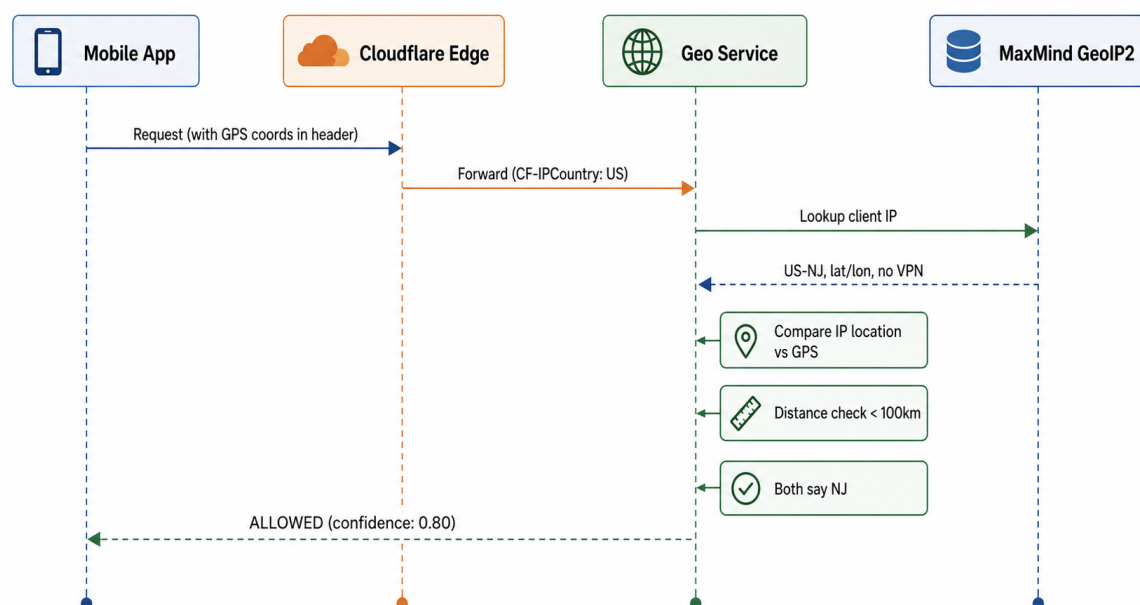


Figure 2: GPS Requirement on Mobile.

In this reference policy, a US-jurisdiction request without an approved device-location signal is denied even when IP points to the state. Confirm the exact signal mix, accuracy threshold, and fallback path with the regulator and approved geolocation provider.

IP vs GPS Cross-Reference

When both IP and GPS signals are available, we compute the haversine distance between them. If they're more than 100km apart, something is wrong; either the GPS is spoofed, or the player is using a VPN that we didn't catch.

VPN and Proxy Detection

VPN detection is the first line of defence. We use MaxMind's GeoIP2 Insights database, which flags:

Threat Type	Detection Method	Response
VPN	Known VPN provider IP ranges	Immediate deny
Anonymous Proxy	Proxy database matching	Immediate deny
Datacenter/Hosting	ASN classification	Immediate deny
Tor Exit Node	Exit node list matching	Immediate deny

In this reference policy, a detected VPN, anonymous proxy, hosting network, or Tor exit is a deny or manual-review condition even when GPS appears valid. The binding response is jurisdiction-specific: document the applicable licence or control requirement rather than treating the UKGC and all US states as one technical rule.

Cloudflare Edge vs Server-Side Comparison

If you're using Cloudflare (and you should be for DDoS protection: see Chapter 14), you get a free geolocation signal via the CF-IPCountry header. This is determined at the edge, closest to the player, before any proxying.

We use this as a corroborating signal:

- If CF says GB and IP says GB: confidence increases
- If CF says IR and IP says GB: spoofing score increases significantly
- CF doesn't give state-level precision, so it can't replace IP+GPS for US states

The spoofing score combines multiple signals:

Mismatch	Score Impact
IP vs CF country mismatch	+0.4
IP vs GPS country mismatch	+0.5
Sub-meter GPS accuracy (likely spoofed)	+0.3
Tor exit node detected	+0.8

A combined score above 0.7 results in denial. The threshold is conservative; we'd rather block a legitimate player who can re-verify than allow a spoofed location.

Confidence Scoring

The final confidence score determines whether we allow or deny:

Signal	Contribution	Notes
IP matches jurisdiction (state-level)	+0.4	For US states
IP matches jurisdiction (country-level)	+0.5	For EU/other
GPS matches jurisdiction	+0.3 to +0.4	+0.4 for state-level
CF edge matches country	+0.2	Corroborating only

Minimum confidence to allow: 0.5. This means:

- UK player with IP match only: 0.5 (just passes)
- NJ player with IP + GPS: 0.8 (high confidence)
- NJ player with IP only on mobile: denied (GPS required)
- NJ player with IP + GPS + CF: 0.8+ (maximum confidence)

Session Re-Verification

Location verification isn't a one-time check. Players move. Sessions last hours. Jurisdictions require periodic re-verification:

Jurisdiction	Re-verify Interval	Basis
US-NJ	30 minutes	NJAC 13:69O
US-PA	30 minutes	PGCB Technical Standards
US-MI	30 minutes	MGCB Regulations

Jurisdiction	Re-verify Interval	Basis
GB	60 minutes	UKGC LCCP
MT	120 minutes	MGA guidelines
SE, DK, BR	60 minutes	Respective regulators

If a session exceeds its re-verification interval without a fresh check, the next API call triggers re-verification before processing the request.

Three-Environment Deployment

Component	Development	Staging	Production
IP Provider	Override map (test IPs)	MaxMind GeoLite2	MaxMind GeoIP2 Insights
GPS	Simulated coordinates	Device simulator	Real device GPS
CF Edge	Hardcoded header	Cloudflare dev proxy	Cloudflare production
Redis Cache	Local Redis	ElastiCache (single)	ElastiCache (cluster)
Audit Log	In-memory list	PostgreSQL	PostgreSQL + S3 archive

Test Coverage

Script Reference: `scripts/chapter-24/location-verification/tests/test_geofence.py`: 33 tests covering all verification scenarios.

Test Category	Count	What It Validates
Haversine distance	3	Zero distance, known distance, short distance
VPN/proxy/datacenter	3	Each threat type denied
Jurisdiction resolution	5	NJ, UK, MT, BR allowed; blocked country denied
US state precision	2	GPS override, mobile GPS requirement
CF edge comparison	2	Confidence boost, mismatch detection
IP-GPS discrepancy	2	Large mismatch denied, small mismatch allowed
Spoofing detection	1	Sub-meter GPS flagged
Blocked countries	5	Parameterized sanctions check
Jurisdiction matrix	4	Required fields, GPS flag, age gates
Re-verification	3	After interval, recently checked, unknown jurisdiction
Audit trail	2	Verification logged, denial logged

Release Gates

Script Reference: `scripts/chapter-24/release-gates/jurisdiction_matrix_test.py`: 55 checks validating every jurisdiction config.

The jurisdiction matrix release gate validates: - All sanctioned countries are blocked (10 checks) - No licensed jurisdictions accidentally blocked (5 checks) - Age gates correct per jurisdiction (8 checks) - Currencies correct (8 checks) - Game types match regulatory approval (8 checks) - GPS requirements for US states (8 checks) - Re-verification intervals configured (8 checks)

This gate runs on every deployment that touches geofencing configuration. A single misconfigured jurisdiction means offering unlicensed gambling in that territory.

References and Primary Sources

- **New Jersey Division of Gaming Enforcement, Chapter 690 Internet and Mobile Gaming regulations:** <https://state.nj.us/lps/ge/docs/Regulations/CHAPTER690.pdf>
- **AWS WAF geographic match rule statement:** <https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-geo-match.html>
- **Cloudflare IP geolocation reference:** <https://developers.cloudflare.com/network/ip-geolocation/>
- **Android location permissions:** <https://developer.android.com/develop/sensors-and-location/location/permissions>
- **Apple Core Location documentation:** <https://developer.apple.com/documentation/corelocation>
- **OWASP MASVS, resilience and anti-tampering controls:** <https://mas.owasp.org/MASVS/>

Cloud and device documentation supports the signal-collection design, but neither an IP-country header nor a device GPS fix alone proves regulatory compliance. The binding regulator's rules determine which signals, rechecks, spoofing controls, and denial behavior are mandatory in each market.

What's Inside the Full Series

You just read one chapter. The full work is a six-volume series, also sold as a single Complete Edition, that takes an online gambling platform from a blank page to a running, regulated, audited business. It is written from production experience, and it ships with runnable code, tests, and live companion sites, not just diagrams.

105 chapters. About 3,504 pages. Six volumes. One Complete Edition. Below are the points that matter most, then what each volume covers, who it is for, and a few of the moments that readers remember.

The most important points

- Your gambling licence is the single most valuable asset the business holds, and one Caribbean permit opens access to a 62.3 billion dollar market.
- RNG is certified with the math, because it is the one system you cannot get wrong: every card, every reel, every dice roll.
- Two players hit the same 2.3 million euro jackpot within 2 milliseconds, and the book shows the architecture that decides who was first.
- A bot network drained 4.2 million euros in six days before batch detection caught it, and the anti-fraud build that closes that gap.
- Blue-green entire Kubernetes clusters, so you upgrade the operating system under a live casino with no maintenance window.
- Post-quantum key exchange migrated on your schedule, before a regulator forces the rotation.
- KYC evidence and self-exclusion taken from API call to a defensible audit trail, with data residency across many jurisdictions at once.
- Datacenter blueprints across five continents, on-premises and cloud, with Terraform at scale.
- Scaling from 150,000 to 2.3 million concurrent users for a single match, and the 336 gigabyte log file that took down a control plane.
- Run 100 casino brands from one dashboard, and stand up a new white-label brand at the press of a button, with the provisioning scripts included.
- Every claim is backed by runnable code, real tests, live dashboards, and a working demo you can open today.

Volume 1: Markets, Regulation, Launch, and Business Foundations

About 410 pages.

Defines the commercial, legal, regulatory, and launch basis of an iGaming operator: the ecosystem, global markets, licensing, planning, team structure, contracts, and the complete Brazilian betting platform build.

Who it is for: founders, executives, legal and compliance teams, and consultants.

Chapters in this volume:

- The Online Casino Ecosystem
- Regulation and Compliance Landscape
- Global Market Analysis
- Market Analysis and Industry Players
- Differences Between Betting Sites and Online Casinos
- Licensing Guide
- Casino Implementation Planning and Timeline
- Team Structure and Operations
- Legal Framework and Contracts
- Building a Brazilian Betting Platform: Architecture, Compliance, and Implementation
- Appendix: How to Launch an Online Casino or Betting Operation: A Practical Guide by Jurisdiction
- Appendix: Data Sources Verification

Why this volume earns its place:

- Why your gambling licence is the single most valuable asset the business holds, and how a single Caribbean permit grows into access to a 62.3 billion dollar market.
- A full Brazilian betting platform build, from the SIGAP rules to the first real money bet.

Volume 2: Platform, Game, and Product Architecture

About 619 pages.

Covers the product core: platform architecture, supplier integration, wallets, games, RNG, distributed systems, edge runtime, the Brazilian platform, and sportsbook architecture.

Who it is for: CTOs, architects, principal engineers, and technical product leads.

Chapters in this volume:

- Complete Platform Architecture
- Supplier Integration Control Plane
- Online Poker Platform Architecture
- Real-Time Cash Flow Management for Online Casinos
- Live Casino Streaming Infrastructure
- Mobile-First Architecture for iGaming
- Casino Mathematics and Game Economy
- Game Exploits, Fake Hacks, and the Engineering of Trust
- Cryptocurrency and DeFi Integration
- Random Number Generation (RNG)
- Real-Time Clock Module Implementation
- Distributed Systems Deep Dive

- Architecture Patterns Deep Dive
- Deploying iGaming Platforms on Cloudflare Workers
- Cloudflare Hybrid Runtime: Edge/Core Split, Degraded Mode, and Consistency Guarantees
- Building a Brazilian Betting Platform: Architecture, Compliance, and Implementation
- Sports Betting Architecture: From Odds Feed to Settlement

Why this volume earns its place:

- RNG is the one system you cannot get wrong. This volume certifies it with the math, not hand waving.
- Two players hit the same 2.3 million euro jackpot within 2 milliseconds. Here is the architecture that decides who was first.
- What genuinely belongs at the edge and what stays at the origin, and how the split survives a degraded origin on Cloudflare Workers.

Volume 3: Security Engineering and Runtime Defense

About 768 pages.

Hands-on security engineering: anti-fraud, HSM infrastructure, OpenBao, DevSecOps pipelines, secrets hygiene, SIEM, IDS/IPS, mTLS, post-quantum cryptography, operator access, and bot traffic.

Who it is for: security engineers, AppSec, SecOps, platform security, and technical auditors.

Chapters in this volume:

- Anti-Fraud System Deep Dive
- Hardware Security Module Infrastructure
- OpenBao Operations: Secret Engines, Dynamic Credentials and Disaster Recovery
- DevSecOps for iGaming
- DevSecOps Pipeline Implementation: From GitHub Actions to Self-Hosted GitLab CI
- Secrets Management and Git Hygiene for iGaming Engineering
- Wazuh SIEM for iGaming Compliance
- AWS SIEM Implementation for iGaming Compliance
- Network IDS/IPS: Suricata and AWS Network Firewall for iGaming
- Post-Quantum Cryptography for iGaming Platforms
- Mutual TLS Between Kubernetes Services for iGaming Platforms
- Blue-Green Cluster Switching for iGaming Kubernetes Environments
- IP Reputation and Blocklist Integration for iGaming Platforms
- Mobile Operator Access: Cloudflare Access, OpenBao SSH CA, and the Case Against Teleport
- Email Authentication and Anti-Spoofing for iGaming Brand Domains
- Security Workflow Automation with n8n on Kubernetes
- Synthetic Traffic and the Bot Lifecycle

Why this volume earns its place:

- A bot network pulled 4.2 million euros in six days before batch detection caught it. The anti-fraud build that closes that gap.

- Blue-green entire Kubernetes clusters, so you upgrade the operating system under a live casino with no maintenance window.
- A regulator will eventually require post-quantum key exchange. Migrate now, on your schedule, not during a forced rotation.

Volume 4: Compliance, Player Safety, Data Residency, and Governance

About 552 pages.

The governance-led view: the broad security and compliance foundation, KYC, geofencing, player protection, self-exclusion, regulatory reporting, data residency, and AI governance.

Who it is for: compliance engineering, regulatory teams, privacy leads, responsible-gaming teams, and data governance owners.

Chapters in this volume:

- Security and Compliance
- KYC Evidence Lifecycle
- Geofencing and Location Verification
- GLI-GSF Compliance Framework: Online Gaming Information Security
- Regulatory Reporting and Evidence Export
- Responsible Gaming and Player Protection Systems
- Self-Exclusion Registries: From API to Audit Trail
- Data Residency and Backup/Recovery
- The Jurisdiction Transfer Gateway and Cookie Consent
- Migrating a Single-Jurisdiction Casino Platform to Hub and Spoke
- PostgreSQL Aegis: Testing Layered Encryption End-to-End
- Data Governance for iGaming Platforms
- AI Governance for iGaming Platforms under the EU AI Act
- Appendix: postgres-aegis Bugs and Fixes

Why this volume earns its place:

- The KYC evidence lifecycle and self-exclusion registries taken from API call all the way to a defensible audit trail.
- Geofencing, data residency, and the jurisdiction transfer gateway that lets one platform obey many regulators at once.
- AI governance for iGaming under the EU AI Act, written for the systems you actually run.

Volume 5: Infrastructure, Datacenter, and Deployment

About 424 pages.

Infrastructure in one place: caching, the internal registry, developer inner loops, infrastructure patterns, datacenter regions across five continents, AWS, Terraform, and decommissioning.

Who it is for: infrastructure teams, SREs, datacenter engineers, and platform engineers.

Chapters in this volume:

- Caching Strategies and Benefits
- Internal Docker Registry: Why You Need Your Own and How to Build It
- Developer Inner-Loop Experience in Containerized iGaming Platforms
- Infrastructure Patterns Deep Dive
- Elastic Compute and Cluster Autoscaling on EKS
- On-Premises Infrastructure for US-Regulated iGaming
- Datacenter Infrastructure for Regulated Gaming
- European Datacenter Infrastructure for Regulated Gaming
- Datacenter Infrastructure for Regulated Gaming: Asia-Pacific and Middle East
- Datacenter Infrastructure for Africa and Offshore Jurisdictions
- Latin America Datacenter Infrastructure for Regulated Gaming
- AWS Platform Deployment for iGaming
- Terraform at Scale for iGaming Infrastructure
- Secure Infrastructure Decommissioning

Why this volume earns its place:

- Datacenter blueprints across five continents, on-premises and cloud, for markets that demand local infrastructure.
- Terraform at scale and elastic autoscaling on EKS, plus the 100 millisecond line between a responsive casino and one that bleeds players.

Volume 6: Operations, Finance, Growth, and Case Studies

About 731 pages.

The operating system of the business: FinOps, QA, operational playbooks, analytics, incident management, financial operations, CRM, migration and launch case studies, war stories, and platform onboarding.

Who it is for: operations leaders, PMO, financial operations, CRM and marketing teams, and executive operators.

Chapters in this volume:

- FinOps Deep Dive
- Performance Benchmarks and Metrics
- Cache, DNS, and Traffic Surge Engineering
- Testing and QA in Gambling
- AI-Driven Game QA: Finding Real Bugs With Simulated Players
- AI-QA Multi-Agent Architecture: The Harness as an Adversary
- Operational Playbooks
- Workflow Engine and Case Management
- Notifications and Transactional Communications
- Disputes, Chargebacks, and Player Support
- Docker Disk Lifecycle, Truncation, and the Anatomy of a Disk-Full Incident
- Data and Analytics
- Incident Management

- Cash-Flow Integrity Incident Response
- Financial Operations
- The Financial Truth Layer: Ledger, Treasury, and Reconciliation
- Marketing Technology and CRM Systems
- Case Study: On-Premises to Cloud Migration
- Case Study: Security Incident Response
- Case Study: Launching in a New Regulated Market
- Case Study: Scaling for the World Cup
- Case Study: The Grey-Market Doorway and the Regulated Alternative
- War Stories: When Everything Goes Wrong
- Future Technology and Innovation in iGaming
- Prediction Markets: Where Trading Meets Betting
- Platform Onboarding: From Contract to First Real-Money Bet
- Configuration and Rules Distribution: Feature Flags, Jurisdiction Rules, and the Propagation Model
- Operating 100 Casinos From One Dashboard
- Casino as a Service: White-Label Provisioning at the Press of a Button
- Appendix: Academic Bibliography
- Appendix: Education, Certifications, and Industry Resources

Why this volume earns its place:

- Scaling from 150,000 to 2.3 million concurrent users for one match. Capacity planning gets no second chance.
- 336 gigabytes in one log file took down the control plane. The war stories, and the playbooks that prevent the next one.
- Run 100 casino brands from one dashboard, and stand up a new white-label brand at the press of a button with the provisioning scripts included.

Why readers buy the whole thing

- It is complete. Markets and regulation, platform and game, security, compliance, infrastructure, and operations all connect into one system you can actually build.
- It is real. Every claim is backed by code you can run and tests you can read, with live dashboards and a working demo you can open today.
- It is current. Post-quantum crypto, the EU AI Act, Cloudflare edge runtimes, prediction markets, and Casino as a Service are here because operators face them now.
- It pays for itself. One prevented fraud incident, one avoided outage, or one faster launch is worth many times the price of the series.

Get the Complete Edition and all six volumes at thebackendofluck.com. Portuguese edition at portrasdasorte.com.br.

YOU JUST READ ONE CHAPTER

There are 104 more, across six volumes and one Complete Edition. The full platform, end to end: markets and regulation, wallet and game session, RNG certification, anti-fraud and HSM, KYC and data residency, datacenter blueprints, FinOps, and the case studies behind them.

GET THE FULL SERIES

Complete Edition and all six volumes:

thebackendofluck.com

Portuguese edition: portrasdasorte.com.br

Corrections and feedback: thebackendofluck.com/errata.html

Write to the author: gustavo@thebackendofluck.com