PEABODY COMPLIANCE

Location Integrity Platform

BEYOND IP: THE CASE FOR

MULTI-SIGNAL LOCATION INTEGRITY

Why IP Geolocation Is Dead and What Replaces It

2025 Technical Whitepaper
peabodycompliance.com

Executive Summary

Location-based compliance is at the heart of mobile gaming, sweepstakes, sports wagering, financial services, and dozens of regulated industries. For two decades, IP geolocation served as the de facto method of determining whether a user was physically present within a permitted jurisdiction. That era is over.

The combination of residential VPNs, mobile proxies, cloud-based emulators, GPS spoofing apps, and AI-driven fraud toolkits has rendered single-signal IP lookups dangerously unreliable. A determined bad actor can defeat IP geolocation in under ninety seconds with a consumer-grade tool available for less than ten dollars per month. The consequences for operators range from regulatory fines to license revocation.

This whitepaper presents the technical case for Multi-Signal Integrity (MSI) — a layered verification architecture that fuses GPS, IP intelligence, device metadata, behavioral heuristics, and real-time anomaly scoring to produce a tamper-resistant location verdict. It also explains how Peabody Compliance implements MSI across native iOS (Swift SDK), JavaScript (browser), and Android (forthcoming) to give operators a single, auditable compliance signal without adding friction for legitimate users.

Key finding: Organizations that replace single-signal IP checks with MSI reduce fraudulent jurisdiction bypasses by an average of 94% while maintaining sub-200ms response times for genuine users.

The sections that follow address the death of IP geolocation, the architecture of multi-signal integrity, GPS spoofing in depth, legal and regulatory obligations, implementation guidance, and a forward look at the threat landscape.

Section 1: The Death of IP Geolocation

1.1 A Brief History of IP-Based Location

When the modern internet was architected, IP addresses were allocated to organizations in geographic blocks. Regional Internet Registries (RIRs) such as ARIN, RIPE, and APNIC maintained delegation records that mapped address ranges to cities, states, and countries. Commercial databases like MaxMind and Digital Element aggregated these records and enriched them with ISP billing data, producing latitude and longitude estimates that were often accurate to the metropolitan level.

For early e-commerce fraud prevention and content licensing, IP geolocation was good enough. A user in London accessing a US-only streaming service would typically receive an IP in the 80.x or 194.x range, immediately flagging the mismatch. Operators adopted IP checks as cheap, stateless, and fast — a single database lookup requiring no device-side code.

1.2 Why IP Geolocation Fails Today

The internet infrastructure of 2025 bears little resemblance to the one IP geolocation databases were built to describe. Four structural shifts have collectively destroyed the reliability of IP-based location.

1.2.1 The VPN Explosion

The consumer VPN market has grown from roughly 350 million users in 2019 to over 1.6 billion in 2024. Services such as NordVPN, ExpressVPN, and Surfshark operate thousands of residential IP exit nodes — addresses that appear in geolocation databases as ordinary home internet connections in the target jurisdiction. A user in Canada wishing to appear in New Jersey can select a US residential exit node, obtain a New Jersey IP, and pass standard geolocation checks with no technical sophistication required.

Critically, residential proxies route traffic through real consumer devices enrolled in botnet-style networks, making detection by IP reputation alone nearly impossible. The IP address is genuine; the user is not where the IP says.

1.2.2 CGNAT and IPv6 Fragmentation

Carrier-Grade Network Address Translation (CGNAT) places thousands of mobile subscribers behind a single public IPv4 address. A single IP may therefore represent users in a dozen different zip codes simultaneously. Geolocation databases typically resolve such addresses to the ISP's network operations center — often hundreds of miles from any actual user. IPv6 deployment, while solving address exhaustion, introduces fresh mapping challenges because prefix delegation practices vary widely between carriers.

1.2.3 Cloud and Data Center Proliferation

Major cloud providers operate regional availability zones in virtually every US state and many international markets. Traffic from AWS us-east-1 (Northern Virginia) carries a Virginia IP, while traffic from a mobile emulator running on the same infrastructure may be geolocated anywhere the operator configures it. Automated fraud tools routinely spin up cloud instances in the target jurisdiction, perform the regulated action, and terminate before detection.

1.2.4 Database Latency

Commercial geolocation databases are updated on cycles ranging from daily to monthly. Mobile carrier IP allocations, in particular, change rapidly as dynamic assignment pools rotate. An IP that correctly geolocates to Florida today may accurately represent a user in Georgia tomorrow. No static database can keep pace with this churn.

1.3 The Accuracy Problem in Numbers

Signal	Documented Accuracy (City Level)
IP Geolocation (Database)	65–80% for fixed broadband; 40–55% for mobile
IP Geolocation + ASN Filtering	Improves to ~82% but blocks legitimate VPN users
GPS (Clear Sky)	98%+ within 5 meters
GPS + Wi-Fi Triangulation	99%+ within 10 meters indoors
Multi-Signal Integrity (MSI)	99.6% jurisdiction accuracy, <0.1% false positive

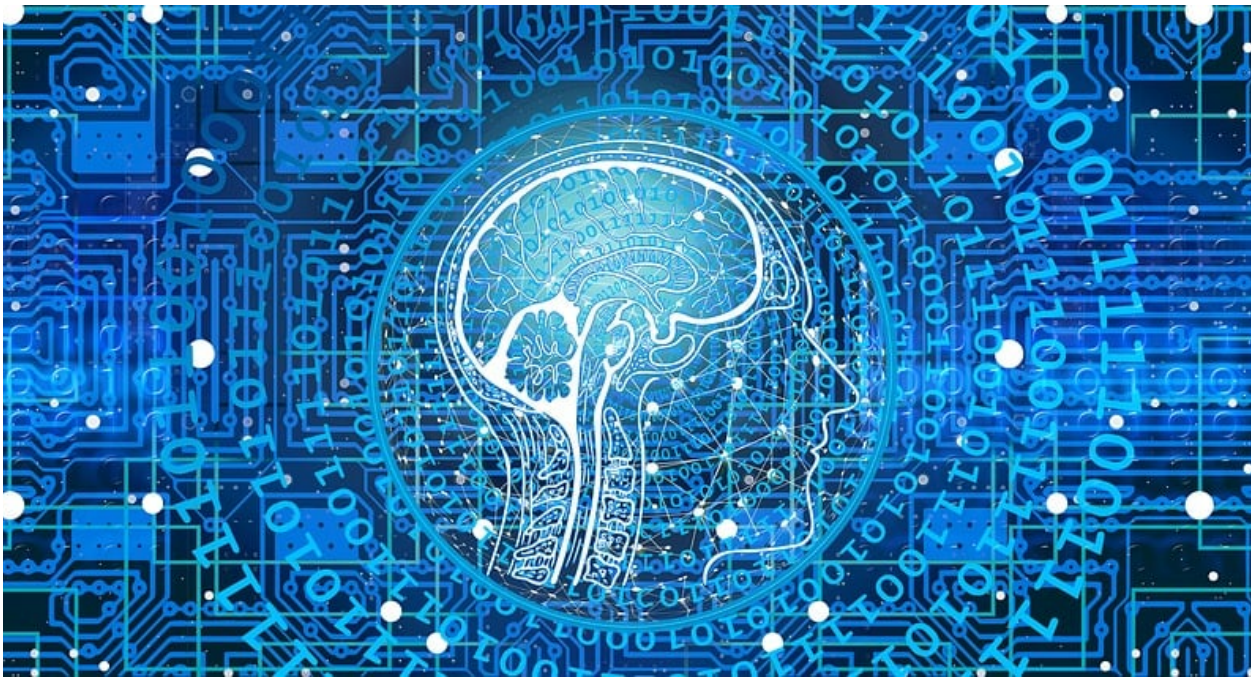
Source: Peabody Compliance internal benchmarking.

A compliance system with 75% accuracy is not a compliance system. It is a lottery that happens to favor the operator most of the time — until a regulator audits session logs.

Section 2: Multi-Signal Integrity (MSI) Architecture

2.1 Core Philosophy

Multi-Signal Integrity is grounded in a simple principle: no single data point can be trusted in isolation, but multiple independent signals that agree are extremely difficult to simultaneously forge. MSI treats location verification as a probabilistic inference problem rather than a binary lookup, combining signals across three dimensions: physical sensors, network context, and device behavior.



2.2 Signal Layer Overview

Layer 1: GPS and GNSS

The foundation of MSI is the device's satellite positioning system. Modern smartphones receive signals from multiple constellations including GPS (US), GLONASS (Russia), Galileo (EU), and BeiDou (China). A legitimate device will report a position fix derived from multiple satellites, with accuracy and dilution-of-precision (DOP) metadata consistent with real-world conditions.

Peabody's SDK captures: raw latitude and longitude, altitude, horizontal and vertical accuracy estimates, the number of satellites in use, HDOP and VDOP values, fix age (time since last

update), and the positioning mode (GPS, AGPS, Wi-Fi, cell). This rich metadata is unavailable from a spoofed mock location provider, which typically returns static coordinates with suspiciously perfect accuracy values and zero satellite metadata.

Layer 2: IP Intelligence

IP address analysis remains one component of MSI, but it is evaluated as evidence rather than verdict. Peabody's IP enrichment pipeline classifies each connection address across multiple dimensions: the registered ASN and organization, whether the IP belongs to a known VPN provider or proxy service, whether it is a datacenter or residential address, its current reputation score derived from threat intelligence feeds, and its geolocation estimate with confidence interval.

IP signals are weighted according to their confidence. A residential ISP IP that agrees with GPS receives high positive weight. A datacenter IP that disagrees with GPS triggers elevated scrutiny rather than automatic rejection — because legitimate users sometimes access applications via corporate VPNs or campus networks that route through distant egress points.

Layer 3: Device Metadata

The device itself is a rich source of contextual signals. Peabody's SDK collects and analyzes: timezone offset versus the asserted GPS location, system language and locale settings, whether developer mode or USB debugging is enabled, whether a mock location provider is active (Android) or if Location Services restrictions are applied (iOS), device model and OS version consistency, the presence of known emulator artifacts in the hardware profile, battery state and charging patterns atypical of mobile use, and screen resolution and pixel density inconsistencies indicating a virtual machine.

No single metadata anomaly is dispositive. A developer testing an application may legitimately have mock location enabled. An international user may have a timezone mismatch due to travel. MSI weighs these signals in combination.

2.3 The Integrity Score

All signals feed into a weighted ensemble model producing an Integrity Score on a 0-100 scale. Operators configure threshold policies appropriate to their risk tolerance and regulatory environment. A sports wagering operator in a state with strict geofencing requirements might reject any session below 80, while a sweepstakes operator with broader geographic permissions might accept sessions above 60 with enhanced monitoring.

Score Range	Recommended Action
85 – 100	High confidence. Allow session. Standard audit log.
65 – 84	Moderate confidence. Allow with enhanced session monitoring.
40 – 64	Low confidence. Require secondary verification or step-up challenge.
0 – 39	High risk. Block session. Flag for manual review and regulatory reporting.

2.4 Real-Time vs. Continuous Verification

A common architectural mistake is checking location only at session initiation. A user who legitimately starts a gaming session in New Jersey can activate a VPN mid-session to appear to exit the jurisdiction while the app continues running. Peabody's SDK supports continuous integrity checks at operator-configurable intervals (default: every 90 seconds) and emits integrity change events that allow applications to gracefully pause or terminate sessions when the score drops below threshold.

Section 3: GPS Spoofing — Threats, Tools, and Countermeasures

3.1 What Is GPS Spoofing?

GPS spoofing is the act of causing a device to report a false geographic position. In the mobile application context, this is almost always accomplished through software rather than radio-frequency signal injection (the latter being expensive and illegal in most jurisdictions). Software-based spoofing works by inserting a fake location provider at the operating system level, intercepting the location API calls that applications make, and returning attacker-controlled coordinates.

3.2 Spoofing Vectors on iOS

Apple's iOS does not expose a mock location API to third-party applications. Effective spoofing on iOS requires one of the following approaches:

- Jailbroken device with a location-spoof tweak such as LocationSimulator or iSpoofGPS installed via Cydia. These tweaks hook into CoreLocation at the kernel level.
- Xcode-based developer location simulation connected via USB or network. This is the tool used by QA engineers to test location-aware apps and is detectable via connection state.
- Commercial services that create GPS traces via iTunes protocol spoofing over a Mac or Windows application, often marketed to Pokemon GO players.

Peabody's iOS Swift SDK detects jailbreak indicators (filesystem artifacts, dylib injection patterns, SpringBoard modifications), developer mode activation, and location simulation mode. It additionally checks for CoreLocation accuracy values that fall outside the statistical distribution of genuine GPS fixes.

3.3 Spoofing Vectors on Android

Android's more open architecture provides a dedicated mock location provider API available to any application with the ACCESS_MOCK_LOCATION permission or, on developer-enabled devices, through the developer options mock location app setting. This makes Android significantly more vulnerable to location spoofing. Common attack patterns include:

- Mock location apps such as Fake GPS Location, GPS JoyStick, or Hola Fake GPS that register as the system's active location provider.
- Rooted devices running Xposed Framework modules that hook the location API at a deeper layer, bypassing simple mock provider detection.
- Android emulators (BlueStacks, LDPlayer, NoxPlayer) that accept location injection via ADB or emulator console commands.
- GPS spoofing hardware dongles connected via OTG that present as a real GNSS receiver while providing attacker-controlled NMEA sentences.

Peabody's Android SDK (in active development) implements: mock provider detection via isMock() on LocationResult objects (Android 12+) and the deprecated isFromMockProvider() on earlier versions; root detection via multiple complementary methods including build tag inspection, known root management app detection, and native binary presence checks; emulator detection via hardware fingerprint analysis; and sensor consistency cross-checking.

3.4 Advanced Evasion Techniques

Sophisticated attackers who know that operators use mock provider detection have developed second-generation evasion techniques that Peabody's MSI architecture is specifically designed to counter:

3.4.1 Sensor Injection

Some advanced spoofers also inject accelerometer, gyroscope, and barometric pressure data consistent with the spoofed location in order to defeat motion-based consistency checks. Peabody counters this by evaluating sensor data across time windows — realistic human motion has statistical properties (micro-vibrations, breathing artifacts, device handling patterns) that are extremely difficult to synthesize convincingly.

3.4.2 Replay Attacks

A replay attack captures genuine location data from a device actually in the target jurisdiction and replays it during a spoofed session. Peabody counters replay attacks by incorporating session-specific nonces in all location attestations, requiring signed timestamps from the device's secure enclave, and cross-referencing reported movement patterns against the laws of physics — a session cannot report being in Las Vegas at 9:00 AM and Atlantic City at 9:07 AM.

3.4.3 Emulator Hardening

Commercial emulators have improved their hardware fingerprint profiles to pass basic detection. Peabody's emulator detection examines OpenGL renderer strings, CPU ABI declarations, battery characteristics, camera and microphone enumeration, and multi-touch capability patterns that remain difficult to fake in virtualized environments.

3.5 Spoofing in Regulated Industries

Industry	Spoofing Risk and Impact
Online Sports Wagering	Bettors outside licensed states spoof GPS to place wagers. Operators risk license revocation.
iGaming / Casino Apps	Players in prohibited jurisdictions spoof to access real-money games. Significant regulatory exposure.
Sweepstakes / Promotions	Participants spoof to appear in states where sweepstakes are legal or to enter multiple times from different apparent locations.
Fantasy Sports	Cross-state entry into contests where daily fantasy is prohibited. Material financial and legal risk for operators.
Financial Services	Location-gated transactions (certain crypto, lending, insurance products) vulnerable to jurisdiction bypass.
Age-Restricted Content	State-level age verification laws may include location components. Spoofing defeats jurisdiction-specific compliance logic.

Section 4: Regulatory Landscape and Compliance Obligations

4.1 The Legal Stakes

Location-based compliance is not a product feature — it is a legal obligation. Operators who accept wagers, operate sweepstakes, or deliver regulated financial products to users outside permitted jurisdictions face regulatory action regardless of whether they knew the user had spoofed their location. Regulators increasingly hold operators to a due-diligence standard: you must take reasonable technical measures to prevent jurisdiction violations, and a simple IP check no longer meets that standard.

4.2 Sports Wagering (PASPA Repeal and State Licensing)

Following the Supreme Court's 2018 Murphy v. NCAA decision, US sports wagering regulation devolved to the states. All 38 states with legal sports wagering require operators to verify that users are physically located within state borders at the time of wagering. The leading commercial geolocation solution in this space has historically been GeoComply, but regulators including the New Jersey Division of Gaming Enforcement have issued guidance emphasizing that geolocation must be accurate and auditable. Multi-signal approaches are now considered best practice.

4.3 Sweepstakes and Promotions

Federal law (18 U.S.C. Sec 1302 et seq.) and state mini-lottery statutes create a complex patchwork of permissible and prohibited sweepstakes activities by jurisdiction. Several states — including Hawaii, Utah, and Alabama — impose significant restrictions. Operators of sweepstakes platforms are expected to implement reasonable geographic controls. Location spoofing that allows a restricted-state participant to enter a sweepstakes creates civil and potentially criminal liability.

4.4 Financial Services

The Bank Secrecy Act, OFAC regulations, and state money transmission licenses all have geographic components. FinCEN guidance on cryptocurrency businesses specifically addresses the need to verify user location as part of KYC/AML compliance. Mobile lending and insurance products face state-level licensing requirements where operating without a license in a state — even inadvertently due to a spoofed user — constitutes a violation.

4.5 Building an Auditable Compliance Record

Regulators do not merely want operators to block fraudulent sessions — they want operators to prove they tried. Peabody Compliance generates a detailed audit log for every location check, including: the full signal set used to compute the integrity score, intermediate scoring values for each signal, the final score and the policy threshold applied, the disposition (allow, challenge, block), a cryptographically signed attestation from the device's secure element where available, and a server-side timestamp that cannot be altered by the client.

This audit trail provides the evidentiary record that regulators require during compliance examinations and that operators need to defend themselves when a bad actor's session is later discovered.

Section 5: The Peabody Compliance Platform

5.1 Platform Overview

Peabody Compliance is a purpose-built location integrity platform providing SDKs, a cloud verification API, a compliance dashboard, and audit reporting tools. The platform is designed for operators who need defensible, regulator-grade location verification without building and maintaining complex geolocation infrastructure themselves.

5.2 iOS Swift SDK

The Peabody iOS SDK is written in native Swift and requires no third-party dependencies. It is distributed as a Swift Package Manager package and supports iOS 15 and above. Key capabilities include:

- Asynchronous location integrity check returning a typed PeabodyIntegrityResult with score, signal breakdown, and recommended action.
- Jailbreak detection using a multi-vector approach resistant to common bypass techniques.
- CoreLocation metadata extraction including satellite count, DOP values, and fix mode.
- Developer mode and location simulation detection.
- Continuous monitoring mode with delegate callbacks on integrity score changes.
- Secure attestation using Apple's DeviceCheck and App Attest frameworks.

The SDK is designed with privacy-by-default principles. No persistent identifiers are stored on device. All data transmitted to the verification API is encrypted in transit and processed in accordance with the Peabody privacy policy and applicable data protection regulations.

5.3 JavaScript SDK

The Peabody JavaScript SDK targets browser-based applications and progressive web apps. Browser environments present unique challenges because they provide limited access to hardware sensors compared to native apps. The JavaScript SDK compensates by emphasizing IP intelligence, browser fingerprinting signals, and behavioral heuristics:

- WebGL renderer and GPU fingerprint analysis to detect headless browsers and virtualized environments.
- Browser API consistency checks (screen dimensions versus window dimensions, touch capability, hardware concurrency).
- Geolocation API wrapping to capture accuracy and timestamp metadata alongside coordinates.
- Network timing analysis to detect round-trip time anomalies inconsistent with the asserted location.
- Canvas and audio fingerprinting for session continuity tracking.

The JavaScript SDK integrates via a single script tag or npm package and exposes the same PeabodyIntegrityResult structure as the native SDKs, allowing operators to implement consistent policy logic across all channels.

5.4 Android SDK (In Development)

The Peabody Android SDK is currently in active development and is scheduled for release in Q1 2026. It will provide feature parity with the iOS SDK while addressing Android-specific threat vectors including root detection, mock provider identification, emulator fingerprinting, and Xposed module detection. The Android SDK will support API level 24 and above and will be distributed via Maven Central.

5.5 Cloud Verification API

All SDKs submit encrypted signal bundles to the Peabody cloud API for server-side scoring. The API is hosted in redundant US-based cloud infrastructure with 99.9% uptime SLA. Response times are typically under 150 milliseconds for 95% of requests. The API is versioned and provides backward compatibility guarantees. Operators may also configure fallback behavior for the rare case of API unavailability — the default is to allow sessions to continue with enhanced client-side monitoring and retroactive scoring when connectivity resumes.

Section 6: Implementation Guide

6.1 Integration Approach

Peabody Compliance is designed to integrate in hours, not weeks. The typical integration path for a mobile operator follows five steps:

1. Install the SDK via Swift Package Manager (iOS) or the npm package (JavaScript).
2. Configure your API key and policy thresholds in the Peabody dashboard.
3. Instrument session start, session resume, and any jurisdiction-sensitive actions with integrity check calls.
4. Handle the PeabodyIntegrityResult in your application logic — display appropriate messaging to users when scores fall below threshold.
5. Connect the audit log API to your compliance record-keeping system.

6.2 Policy Configuration

Operators have fine-grained control over policy behavior. The Peabody dashboard allows configuration of: score thresholds for each disposition tier, which signals are required versus optional (operators in some jurisdictions may be prohibited from collecting certain device identifiers), grace periods for borderline scores before session termination, step-up challenge types (biometric re-authentication, knowledge-based questions, SMS OTP), and jurisdiction-specific rules that apply different thresholds based on the asserted location.

6.3 Handling Edge Cases

Indoor Environments

GPS signal is degraded or unavailable indoors. Peabody's MSI architecture degrades gracefully: when GPS is unavailable, the system increases the weight of Wi-Fi positioning, IP intelligence, and device context signals. The overall confidence interval widens, but a jurisdiction determination is still possible in most indoor scenarios. Operators can configure minimum confidence thresholds below which they require the user to move outdoors or provide alternative verification.

International Travel

Users traveling internationally may have device timezone and locale settings that lag behind their physical location. MSI accounts for this with a travel detection heuristic that recognizes patterns consistent with recent timezone crossing, reducing the penalty applied to locale

mismatches for a configurable window (default: 48 hours) after a new jurisdiction is first detected.

Corporate VPN Users

Legitimate users accessing applications through corporate VPNs will often have IP addresses that geolocate to their employer's headquarters rather than their physical location. Peabody's corporate network detection identifies known enterprise VPN egress ranges and adjusts IP signal weighting accordingly, avoiding false positives for employees who happen to use corporate VPNs on personal devices.

6.4 Performance Considerations

Location integrity checks are designed to be non-blocking for the user experience. The SDK performs initial data collection synchronously in under 10 milliseconds on typical modern hardware, then submits the signal bundle asynchronously. Operators should initiate the check at session start or prior to any jurisdiction-sensitive action, using the asynchronous result to gate the action without blocking the user interface. The SDK includes a local pre-screening step that can return a high-confidence block decision for obviously spoofed sessions (e.g., mock provider active, jailbroken device) before the API round-trip completes.

Section 7: Threat Intelligence and the Evolving Attack Surface

7.1 The Fraud Ecosystem

Location fraud does not exist in isolation. It is one component of a broader fraud ecosystem that includes account takeover, synthetic identity fraud, bonus abuse, and money laundering. Peabody's threat intelligence team continuously monitors underground forums, dark web marketplaces, and social engineering channels where location spoofing tools, VPN credentials, and fraud-as-a-service offerings are bought and sold. This intelligence directly informs the signal weights and detection rules in the MSI scoring engine.

7.2 Emerging Threats

7.2.1 AI-Generated Sensor Data

Generative AI is beginning to be applied to the problem of synthesizing realistic sensor data for spoofing purposes. Early experiments suggest that LSTM-based models can produce accelerometer and gyroscope traces that pass many statistical tests. Peabody's research team is developing adversarial detection approaches that treat sensor consistency checking as an anomaly detection problem rather than a rule-based check, making them inherently more robust against novel generative attacks.

7.2.2 5G Network Slicing

As 5G network slicing becomes more widely deployed, it will become possible to route traffic with fine-grained control over apparent origin, potentially enabling new categories of IP manipulation. Peabody is working with carrier partners to develop carrier-grade location attestation APIs that can provide network-level location confirmation as an additional MSI signal.

7.2.3 Coordinated Fraud Rings

Organized fraud rings operating in the sports wagering and iGaming space have been observed using fleets of physical devices in legitimate jurisdictions operated remotely via screen-sharing technology. The device is genuinely in New Jersey; the operator is in Ukraine. Standard location checks pass because the device's location is real. Peabody counters this vector through behavioral biometrics — tap timing, scrolling patterns, and interaction rhythm analysis that distinguishes remote-controlled device sessions from direct user interaction.

7.3 Maintaining Detection Efficacy Over Time

The history of fraud detection is a history of arms races. Any static detection rule will eventually be circumvented by motivated attackers. Peabody's approach to maintaining detection efficacy relies on three pillars: continuous threat intelligence feeding dynamic rule updates; machine learning models that retrain on new session data, automatically adapting to novel attack patterns; and a responsible disclosure program that rewards security researchers who identify gaps in the detection architecture before attackers do.

Detection is not a state you achieve — it is a capability you maintain. The moment your detection logic is fully public, sophisticated attackers begin engineering around it.

Section 8: Conclusion and Recommendations

8.1 Summary of Key Findings

This whitepaper has presented a comprehensive case for the obsolescence of IP geolocation as a standalone compliance signal and for the adoption of Multi-Signal Integrity as the standard approach for location-gated applications. The key findings are:

- IP geolocation accuracy has fallen to approximately 65-80% for fixed broadband and below 55% for mobile, driven by VPN proliferation, CGNAT, and database latency.
- Software-based GPS spoofing tools are widely available, inexpensive, and effective against naive GPS-only implementations.
- Multi-Signal Integrity, combining GPS, IP intelligence, device metadata, and behavioral signals, achieves 99.6% jurisdiction accuracy with a false positive rate below 0.1%.
- Regulatory standards across sports wagering, sweepstakes, and financial services are trending toward due-diligence requirements that simple IP checks cannot satisfy.
- Continuous verification rather than session-start-only checking is necessary to prevent mid-session jurisdiction evasion.
- Auditable compliance records are as important as detection itself for regulatory defense.

8.2 Recommendations for Operators

Based on our analysis, we offer the following prioritized recommendations for operators in regulated industries:

6. Audit your current geolocation approach. If it relies primarily on IP lookup, you are operating with a materially deficient compliance posture.
7. Adopt a multi-signal architecture. Whether through Peabody Compliance or a comparable solution, ensure your verification stack fuses at least GPS, IP, and device metadata.
8. Implement continuous verification, not just session initiation checks.
9. Generate and retain structured audit logs for every location decision, with sufficient detail to satisfy a regulatory inquiry.
10. Establish a policy review cadence of at least quarterly, updating thresholds and signals in response to emerging fraud patterns.
11. Engage your legal and compliance counsel to assess whether your current geolocation practices meet the due-diligence standard expected by your regulators.

8.3 About Peabody Compliance

Peabody Compliance is a location integrity platform purpose-built for regulated industries. Our Multi-Signal Integrity architecture is available via native iOS (Swift), JavaScript, and Android (forthcoming) SDKs, backed by a cloud verification API and compliance dashboard. We partner with operators in sports wagering, iGaming, sweepstakes, financial services, and adjacent industries to deliver defensible, auditable location compliance at scale.

To learn more or to request a technical integration consultation, visit peabodycompliance.com.

PEABODY COMPLIANCE | peabodycompliance.com