paladin vendor report | **fraud prevention**

paladinfraud

Thank you for downloading the Paladin Vendor Report.

The Merchant Risk Council's (MRC) mission is to provide members with useful tools and sometimes scarce information to help lower fraud and improve your customer's purchasing experience. At the MRC, we understand how difficult it is to navigate a complex ecommerce environment and find the right solution for specific fraud and risk needs. As a benefit of your MRC membership, we are offering members a discounted copy of the Paladin Vendor Report (PVR).

The PVR, gathered by the industry experts at Paladin, provides detailed information on over 40 vendors who offer a wide variety of different fraud prevention tools, platforms, and services. This report is designed to give you a comprehensive overview of the different products offered by each company and present analysis to help you focus on who may ultimately best align with your individual fraud prevention goals.

We hope you find this report to be a helpful resource that will provide you and your business with valuable insights. We are also interested in hearing your feedback on the report and encourage you to send any comments directly to programs@merchantriskcouncil.org.

Sincerely,

Markus Bergthaler
Director of Programs, MRC

The 2021 Paladin Vendor Report

Offering an unprecedented view into today's fraud prevention platforms and solutions.

Every day at Paladin Group, we're in the thick of the fast-paced world of fraud solutions. This is especially important as the global pandemic has accelerated the use of digital environments at a level never experienced before. As malicious individuals take advantage of COVID19 and related scams, it's become even more important to remain focused on streamlining and maximizing the capabilities of an organizational fraud management operation.

As experts on today's solution providers, services, and tools, it's our job to maintain a high-level view of the fraud prevention landscape as well as a detailed, on-the-ground understanding of every solution and every challenge. As the number of providers and services grow and technology evolves, merchants' options become increasingly complex and varied.

Since it's our mission to serve as an authority on these products and their strengths, areas of opportunity, and enhancements, we published the first-ever Paladin Vendor Report (PVR) in 2017. It offered an unprecedented exploration of how merchants could mitigate the risks that come with accepting payments in an omni-channel, card-not-present world. Because of the constant evolution of many popular fraud mitigation solutions, we decided to provide the Paladin Vendor Report on an annual basis. And now, we're pleased to publish the latest: the 2021 Paladin Vendor Report. We've offered previous participants the chance to update their sections and incorporated additional participating vendors.

We focus on several key areas during the discovery process. (Not all are applicable to every vendor, but for consistency, we examined each of the following wherever relevant.)

PRODUCT - The vendor's current functionality.
SERVICES - Available offerings to help merchants during integration and throughout their client lifecycle, including reporting.
BUSINESS DEVELOPMENT - Current partnerships and channels for direct and indirect customers.
MARKETING - The verticals vendors are focusing on and messaging
SALES - A breakdown of market segments.
TECHNOLOGY - How the product works from a technical perspective.

Introduction

What this report offers: the PVR helps merchants navigate the ever-expanding number of solution providers and services available to them. We spoke with vendors who offer risk-mitigation products to merchants in the Card Not Present (CNP) and omni-channel environments—then gathered, examined, and compiled the information for each participating vendor.

Vendors had the option to participate in the report, and Paladin was compensated for the research performed. Our team spent hours in discussion with each of these vendors. We test-drove their products and gathered overviews of their services, marketing, sales, technologies, and future plans. For vendors who chose not to participate in the report, we drew upon our extensive interaction, client input, and research to share a summary of their services.

This report is a groundbreaking effort to gain as much first-hand knowledge as possible from fraud prevention vendors, compiling our findings in a way that's helpful and revolutionary for our industry and the merchants who depend on us. This report is purely informational, and it is not designed to rate the products and services of the vendors, review them, give opinions on them, or give a thumbs-up (or down) about the vendors. The report's intent is to provide clarity regarding what products and services fraud mitigation vendors offer.

The vendors are segmented into six different categories based on their core offerings. Some of the vendors offer other products that complement their core offering or have additional functionality or products. Some vendors provide services in overlapping segments, and this report offers a separate overview for each of the following categories:

- **User Behavior & Behavioral Biometrics**
- **3DS & Consumer Authentication**
- **Device Identification, Reputation, & Reputation**
- **Fraud Platforms & Decision Engines**
- **Identity & Data Verification**
- **Chargeback Management & Platform**

Core functionality icon key

3rd Party API Capabilities	Payment Gateway Capabilities	Operational Support
Machine Learning	Guaranteed Chargeback Liability	ATO Detection Capabilities
Account/Client Management	Device Fingerprint Capabilities	Historical Sandbox Testing
Professional Guidance/Services	User Behavior Capabilities	Pre-Authorization Functionality
Fraud Engine/ Platform Functionality	Non-Production Real Time Rules Testing	

3rd Party API Capabilities – The ability to call out via API to third-party vendors for data, device fingerprinting, etc.

Payment Gateway Capabilities – The ability to process payments directly through their own platform or solution.

Operational Support – Provides outsourced operational support, at a cost, for reviewing high-risk transactions and/or managing chargebacks.

Machine Learning – Matching algorithms to detect anomalies in the behavior of transactions or users.

Guaranteed Chargeback Liability – Guarantees merchants do not take fraud losses for vendor-approved transactions.

ATO Detection Capabilities – Using device characteristics to detect account takeover/ account penetration.

Account/Client Management – Personnel dedicated to working directly with clients.

Device Fingerprint Capabilities – Built directly into the platform (not a third-party API call).

Historical Sandbox Testing – Ability to test rules against historical transactions in a non-production environment.

Professional Guidance/Services – Provides outsourced support for data analysis, rules-building, and recommended best practices, etc.

User Behavior Capabilities – Built-in (not via third-party) capabilities to capture cursor movements, mouse clicks, and time on a merchant site.

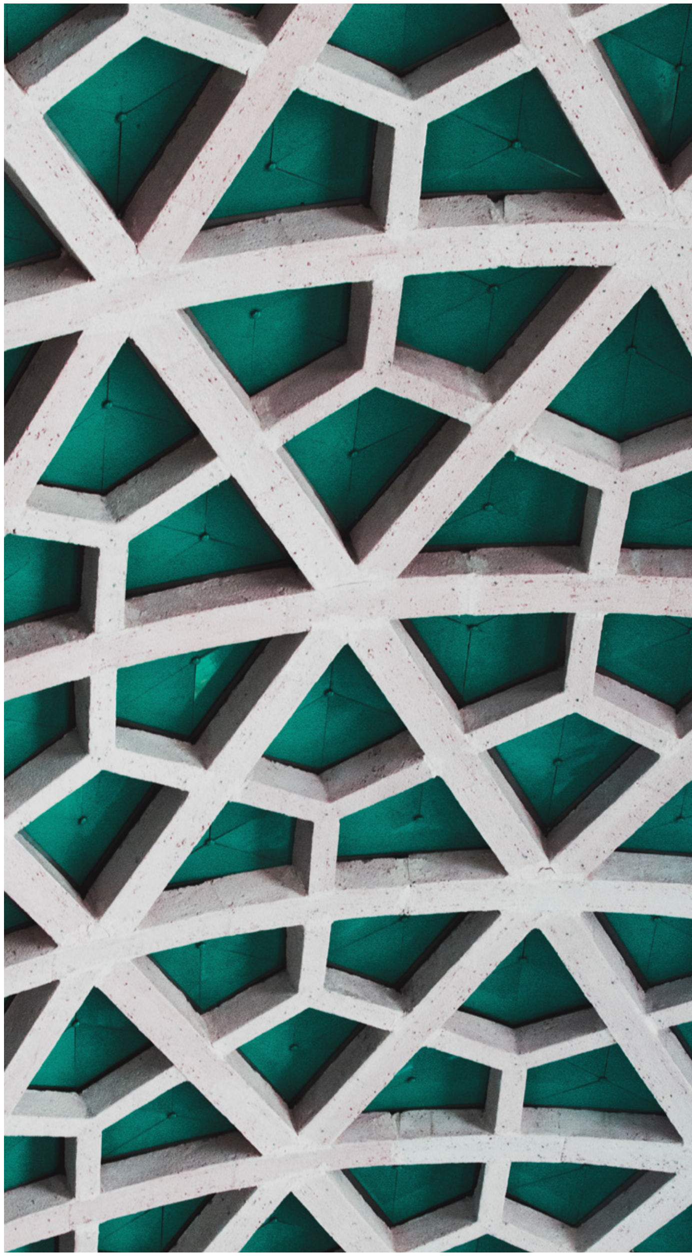
Pre-Authorization Functionality – Ability to score and/or decision a transaction prior to authorization.

Fraud Engine/Platform Functionality – Ability to score/decision a transaction post-authorization.

Non-Production Real Time Rules Testing – Ability to test real-time transactions in a non-production environment.

Identification & Data Verification

By linking people, places, and things, these services can help increase trust through a clear understanding of the person behind every transaction or interaction. Moreover, these services can go a long way in determining whether the data is directly associated with the cardholder or a friend or family member of the cardholder. These services are especially useful in cases where the user or customer is required to provide personal identity data or physical ID.



GeoComply

GeoComply provides a reliable and accurate geolocation solution for fraud detection.

GeoComply's solutions are based on the award-winning geolocation compliance and geo-protection technologies that **GeoComply** developed for the highly regulated and complex U.S. Gaming industry. The company's software is installed in over 400 million devices worldwide, putting **GeoComply** in a strong position to identify and counter both current and newly emerging geolocation fraud threats.

With technology proven and refined over 10 years of development and billions of transactions, **GeoComply** can accurately determine a users' true location and whether they are attempting to mask their location using various spoofing tools.

By integrating **GeoComply**, organizations are able to detect fraud earlier in a customer's engagement. This capability provides high performance fraud detection via the use of accurate, authentic, and unaltered location data acquired from a user's device.

GeoComply enables a wide range of industries including banks, fintechs, and cryptocurrency exchanges to detect and guard against geolocation-based fraud.

GEOCOMPLY

Empowering The Future Of Digital Trust

At a Glance:

- 3rd Party API Capabilities
- Account/Client Management
- Device Fingerprint Capabilities
- Professional Guidance/Services
- Pre-Authorization Functionality

Four typical use cases for GeoComply:

- **Onboarding & Account Opening** - Use geolocation for better identity verification for KYC (know your customer) and enhanced due diligence, as well as for more confident automated underwriting.
- **Transactions Fraud Mitigation** - Require location checks to discourage bad actors and improve accuracy in differentiating between real fraud and false positives, as well as reducing false negatives.

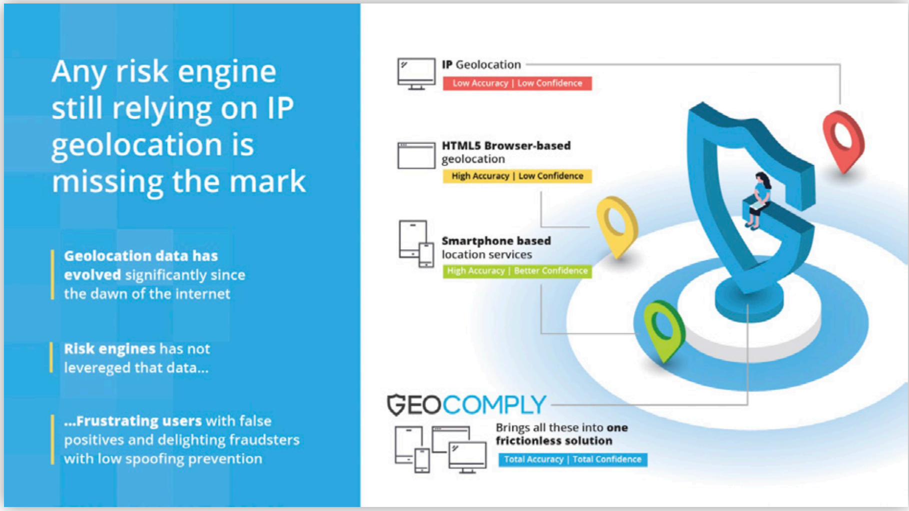
- **AML and Sanctions Compliance** - Ensure compliance with jurisdictional requirements by verifying the true location of a transaction.
- **Authentication and Account Protection** - Monitor account updates and user behaviour by adding geolocation checks to continuous authentication and protect against account takeovers and account update fraud while reducing friction.

Some of the key benefits from GeoComply:

- **Strengthen KYC and CDD** - "Spoof-proof" and accurate geolocation data (beyond a simple IP address) is a crucial component of AML and CFT processes by ensuring that KYC due diligence is robust and protected from exploitation.
- **Fraud Prevention and Risk Mitigation** - Real-time and historic analysis of geolocation transactions strengthens risk management by creating a holistic oversight of user behavior. Suspicious activity can be prevented in real-time and identified over time.
- **Reporting and Traceability** - All geolocation transactions are maintained in a secure database and archive, creating audit trail transparency and traceability. This strengthens reporting capabilities of FIs for regulators and law enforcement.
- **Sanctions Compliance** - Compliance-grade geofencing capabilities add extensive location assurance through the collection of multiple and unaltered geolocation data sources, which strengthens sanctions compliance. IP-based solutions do not constitute location due diligence.

Products and Services

GeoComply represents considerable advancement in fraud detection as it relates to historically available geolocation and location-based signals. While direct competition for **GeoComply** is limited, they do consider they are competing against the notion that an IP address is sufficient for location-based risk management.



Any risk engine still relying on IP geolocation is missing the mark

Geolocation data has evolved significantly since the dawn of the internet

Risk engines has not levereged that data...

...**Frustrating users** with false positives and delighting fraudsters with low spoofing prevention

IP Geolocation
Low Accuracy | Low Confidence

HTML5 Browser-based geolocation
High Accuracy | Low Confidence

Smartphone based location services
High Accuracy | Better Confidence

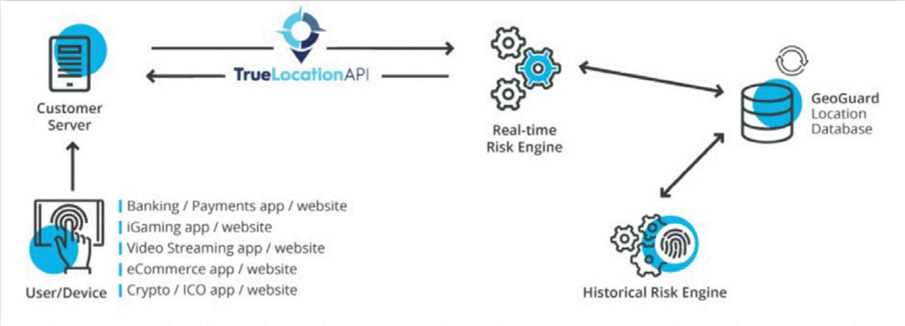
GEOCOMPLY
Brings all these into **one frictionless solution**
Total Accuracy | Total Confidence

In addition to geolocation, **GeoComply** uses a proprietary device fingerprinting technique to enhance its fraud detection capabilities. Traffic filtering and flexible rules can be configured to meet specific business needs.

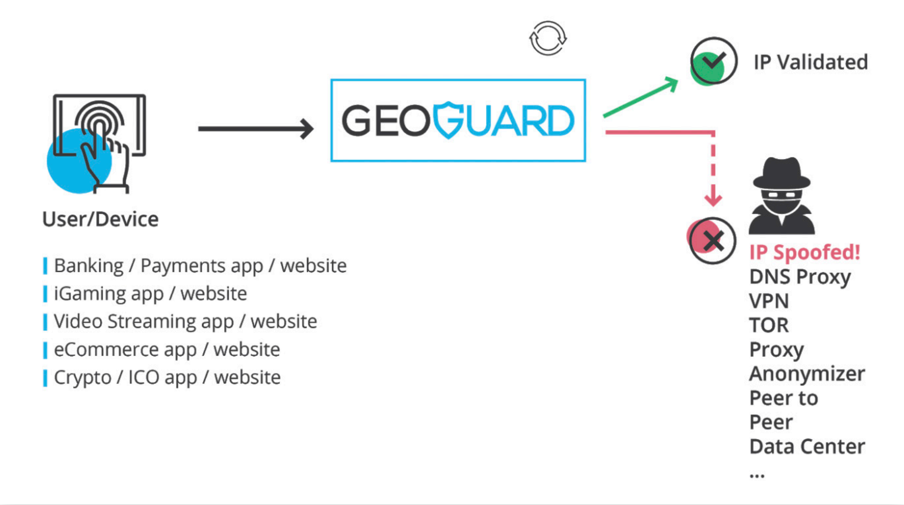
GeoComply

GeoComply Mobile and Desktop SDKs represent a high standard in geolocation security for risk and compliance management, ensuring continued high performance and accuracy for location compliance. It is embedded in native mobile apps or desktop applications, providing geolocation identification during a user's session.

GeoComply offers a geolocation solution that works directly within the client's website for all devices and user interfaces. For frictionless and spoof-proof geolocation within the browser, this geolocation experience can be customized according to the business and compliance needs of the client, with adaptable end-user prompts and secure collection of location data.



TrueLocation API provides location-based fraud detection, utilizing both a real-time risk engine and a historical risk engine to identify and flag potentially fraudulent activity. By analyzing both real-time and historical data, TrueLocation API enables organizations to identify and stop a wide variety of fraud including chargeback fraud, account sharing, card not present (CNP) fraud, account takeovers, and detecting VPN usage.



GeoGuard provides multilayered fraud protection against VPNs, proxies, peer-to-peer networks, and other types of IP data manipulation. Their solution is continuously updated as new threats and data centers are identified and mitigation methods are developed.

GeoComply achieves advanced and accurate geolocation security through three key steps:

1. **Step 1- Collect data:** Collect geolocation data from multiple sources, including: GPS, WiFi, GSM, Browser/HTML5, and IP address.

2. **Step 2 - Ensure accuracy:** Validate data points are trustworthy by ensuring they are:
    - Not being altered via spoofing apps,
    - Accurate, by combining multiple location signals in the location algorithm, and
    - Physically there by monitoring for remote access apps/ signals.
3. **Step 3 - Analyse behavior:** Conduct real-time and historical analysis on the collected dataset to detect and flag likely patterns of location fraud. **GeoComply** uses both machine learning and human intelligence with dedicated fraud and data analyst teams.

Additionally, **GeoComply** has a KYC solution focused on regulated markets:

- **IDComply** allows businesses to query multiple vendors for both ID and age verification, allowing banks, payment processors, and other transaction-based businesses to move from a single vendor of ID and age verification to a multi-vendor model, through one API call. By integrating IDComply into user onboarding processes, companies working in multiple jurisdictions can also manage the patchwork of compliance requirements – not only for age and ID verification but also anti-money laundering (AML), know your client (KYC), enhanced due diligence (EDD), PEP/Sanctions Watch List/Adverse Media, child support, and other requirements.

Reporting and Analytics

Most users consume **GeoComply's** ingested signals from within their existing tools, **GeoComply** also provides a single portal with a wide range of out-of-the-box reporting and dashboards.

Users can access detailed logs and information about each transaction through real-time monitoring or with after-the-fact drill-down reporting. Examples of reports include but are not limited to:

- Transaction level reports (archived for 7+ years)
- Visualization of user location with Pin Drop Maps
- Detailed device attributes to support incident review
- Users per IP address and device, and IP addresses and device per user
- Reasons for inability to pass the geolocation check
- Chargeback Report shows the location and device used for all of a client's transactions within a certain timeframe.

Analytical insights are available through GeoComply's client Kibana analytics tool, which contains dashboards and custom reporting for detailed analysis of potentially fraudulent transactions. Additional real-time data is also provided via RESTful APIs.

Integration process

GeoComply has a well-established implementation process, with fully supported integration and launch phases. The company works closely with each client to map the entire user experience and identify where the use of location data can reduce fraud. A comprehensive white-glove onboarding process covers everything from integration design through certification and launch support. The integration process also includes a set of onboarding support hours.

Level of support

Standardized ongoing support is also available and meets SLA commitments. Organizations are assigned a primary point of contact who provides weekly catch-up sessions to address any issues and provide a "health check," calling out potential issues before they happen, as well as round-the-clock contact numbers for urgent issues.

GeoComply's pricing model is based on:

- Tiered pricing by transaction volume
- A monthly minimum fee

Key developments on the calendar for the next 12 months:

- Use TrueLocation API for clients capturing their own in-app geolocation information
- Focus on partnerships with complementary platforms to integrate with your existing tool stack and enhance your team's incident review and reporting flows.

paladinfraud

Paladin Fraud would like to thank all of the participating vendors for their time and availability during the discovery and post-writing processes. We also would like to remind all readers of this report that they can email us at info@paladinfraud.com to let us know which vendors they would like to see participate in the report next year.