Why Your ‘90s Location Data Fails at Detecting Financial Fraud

How modern location intelligence unmasks bad actors

GEOCOMPLY

Executive Summary

When it comes to verifying a client's location, internet protocol (IP) addresses are useless, a fact that delights fraudsters seeking to hide their online identity. In fact, cybercriminals are adept at exploiting IP addresses to *conceal* their location. To fight fraud, financial institutions need a way to accurately and quickly verify where and who a customer is – not where and who they say they are. And they need to do it in a way that respects privacy and doesn't add friction to the user experience.

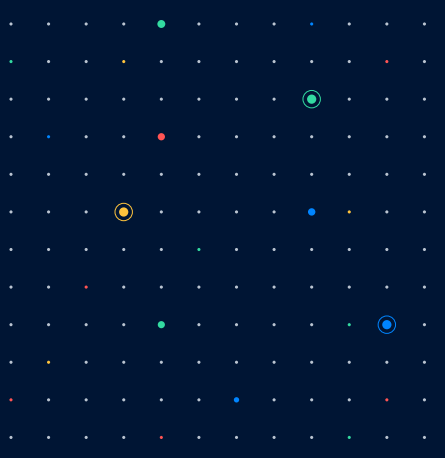
To fight fraud, financial institutions need a way to accurately and quickly verify where and who a customer is – not where and who they say they are.

Fortunately, there's a solution that goes beyond the limitations of IP: modern location intelligence. This unique approach to collecting, verifying and analyzing location data brings a new set of insights for fraud and risk management. With location intelligence, financial institutions (FIs) can:

- Identify potential fraudsters during KYC/ onboarding and at the point of a transaction by easily ingesting verified geolocation data into their existing fraud risk engines.
- Detect patterns of suspicious or fraudulent activity by analyzing both historical and real-time location behavior.

In this way, location intelligence enables FIs to protect themselves and their customers from account takeovers, unauthorized transactions and other forms of financial fraud.

Table Of Contents

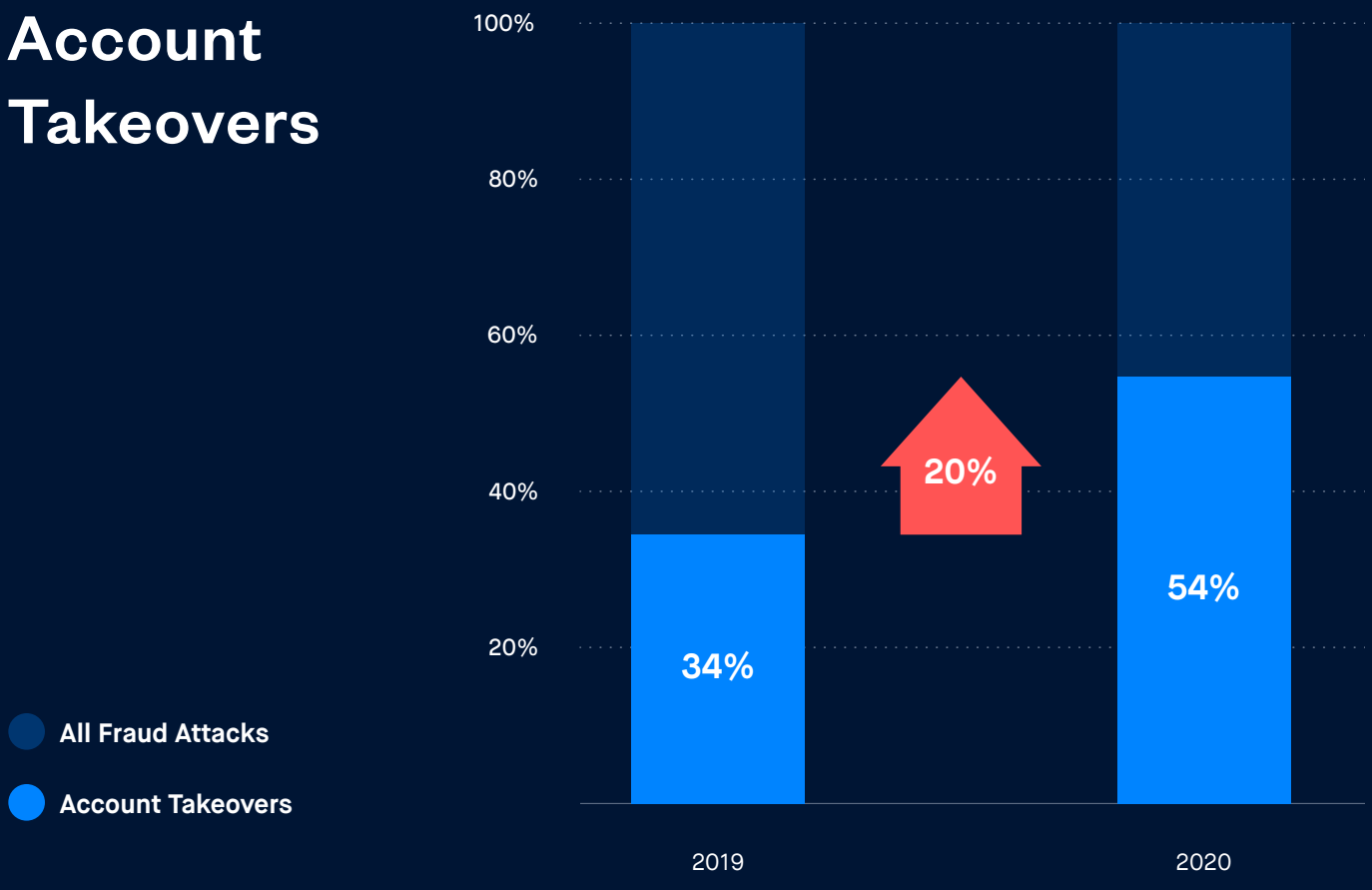


The Accelerated Move to Online Drives Financial Fraud Rates

The pandemic has accelerated digital transformation in all corners of the finance and banking industry. Mobile banking became more of the norm, and now more consumers prefer to transact online. Customer-focused neobanks continue to enjoy substantial growth, even as they compete with their legacy counterparts. And with names like Visa and PayPal enabling cryptocurrency payments, digital assets are firmly embedded into the financial mainstream.

Fraudsters thrive amid turmoil and change, so skyrocketing fraud rates are no surprise. In fact, 79% of fraud professionals said they've seen overall levels of fraud rise in the wake of the pandemic. More specifically, account takeovers are up, comprising 54% of all fraud attacks in 2020, up from 34% in 2019. The cost of fraud is increasing as well: payment fraud losses have more than tripled since 2011 and are expected to exceed $40 billion by 2027. To right these financial wrongs, banks and other FIs need to understand the limitations of IP addresses in fighting fraud and why modern location intelligence is a better way.

Account Takeovers



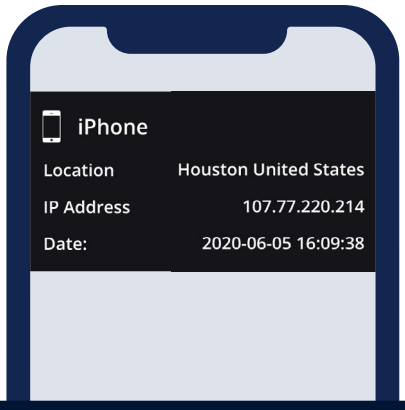
Why IP Addresses Are Useless in Fighting Financial Fraud

For decades, internet protocol (IP) addresses have been the default standard for verifying a user's location. That worked just fine in the 1990s, but not today. Fraudsters now have access to an arsenal of cheap and easy spoofing tools, including VPNs and proxies, making both desktop and mobile IP addresses the easiest location data point to manipulate.

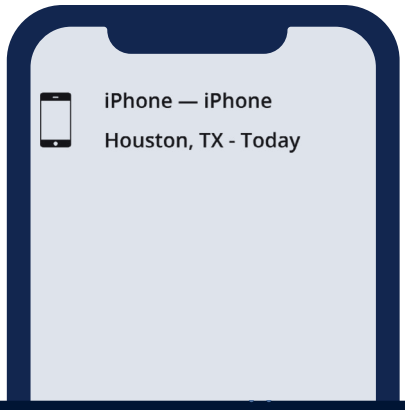
Safely hidden online, bad actors are free to commit all manner of financial crimes – account takeovers, synthetic identity fraud and payment fraud, to name a few. No wonder today's tech-savvy cybercriminals are making out like bandits.

To test the accuracy of IP for geolocation, GeoComply audited the location checks of several major financial services apps. In two instances, the location indicated Houston, Texas, and the other auto-filled the location as California. The true location during the audit was Vancouver, British Columbia. This blatant inaccuracy creates large security holes that fraudsters are eager to exploit.

Crypto exchange
Location Indicated:
Houston, Texas, US



Investment website
Location Indicated:
Houston, Texas, US



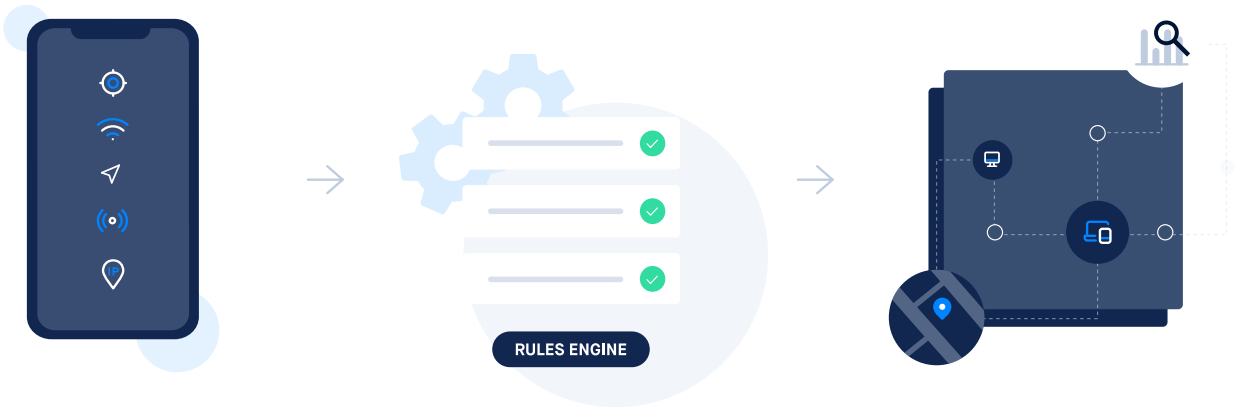
International money transfer website
Auto-filled Location:
California, US

The user's true location is Vancouver, BC, Canada.

To Stop Fraud, Find the Fraudster

Location spoofing is one of the most common ways a fraudster will mask their identity online. In fact, there's a strong correlation between stopping location fraud and stopping other types of fraud.

FIs need a solution that mitigates fraud risks by detecting and stopping bad actors who spoof their location. Modern location intelligence achieves this through three key steps:



1. Gather multi-source location data

Collects geolocation signals from multiple sources, including GPS, WiFi, GSM, browser/HTML5 and IP addresses.

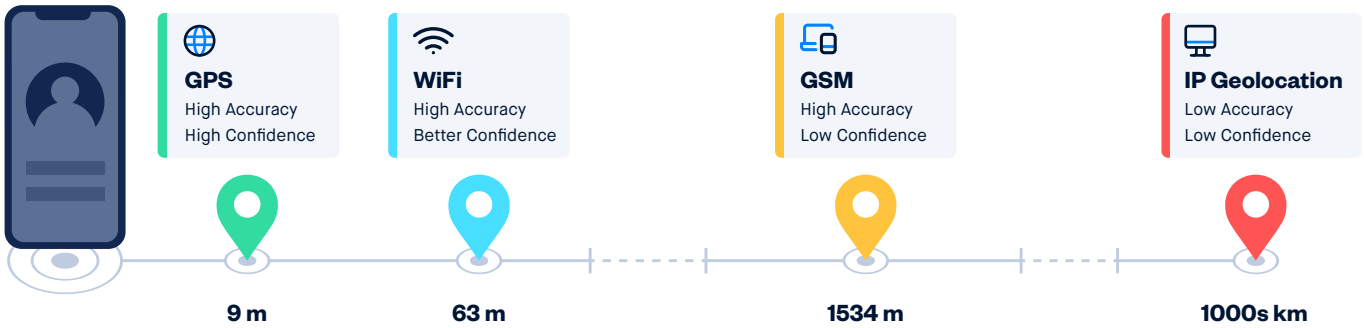
2. Verify location accuracy

A rules engine runs hundreds of checks on every transaction to analyze suspicious activities – from spoofing apps to device and user integrity.

3. Analyze location behavior

Real-time and historical data are combined to detect and flag patterns of location fraud. Models are constantly updated with the use of machine learning and human intelligence.

Geolocation data collected from multiple sources and verified for authenticity increases the confidence that a user's location is accurate.



The banking or finance app uses this data at key steps in the customer journey, such as during account opening, at login, when account data is being updated or a transaction is being made.

The use of verified geolocation data at these critical points creates barriers that have been proven to keep bad actors out. Frustrated by such roadblocks, online fraudsters will flee and find another, easier target to exploit. In addition, this data can increase approvals for new-customer applications by accurately determining a user's true location.

Protecting customer privacy

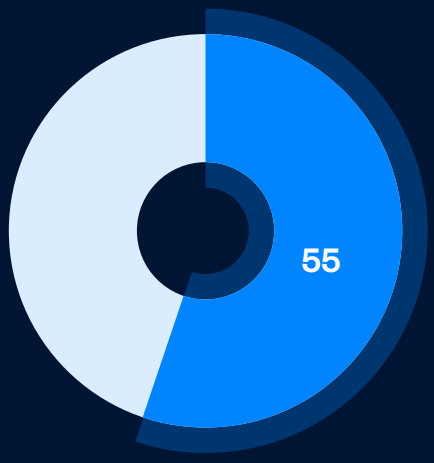
Location checks are designed to respect customers' privacy – only anonymized geolocation data is collected and processed after user consent, without other personally identifiable information (PII) such as names or addresses.

Customers are willing to share location

Asking for customers to share their location often raises privacy concerns. But the data shows customers are willing to do so, as long as it's for the right reasons.

In fact, 80% of smartphone users have enabled location services on their devices. And 55% of Millennials and Gen Z would switch to a bank that uses location data to secure their accounts.

- **80%** of smartphone users have enabled location services on their devices



- **55%** of Millennials and Gen Z would switch to a bank that uses location data to secure their accounts

3 Ways Location Intelligence Helps Combat Financial Crime

Verified geolocation data complements an FI's existing fraud tools. By ingesting these location signals into their fraud risk engines, FIs can safeguard against location spoofing attacks and unauthorized attempts to manipulate data. In addition, real-time and historical analysis of geolocation transactions strengthens risk management by creating a holistic oversight of user behavior. Suspicious or fraudulent activity can be prevented in real-time and identified over time.

Here are three use cases:

1. Detect suspicious behavior at onboarding and verify more good customers

Establish a customer's true digital identity by collecting geolocation data during account creation and KYC/onboarding.

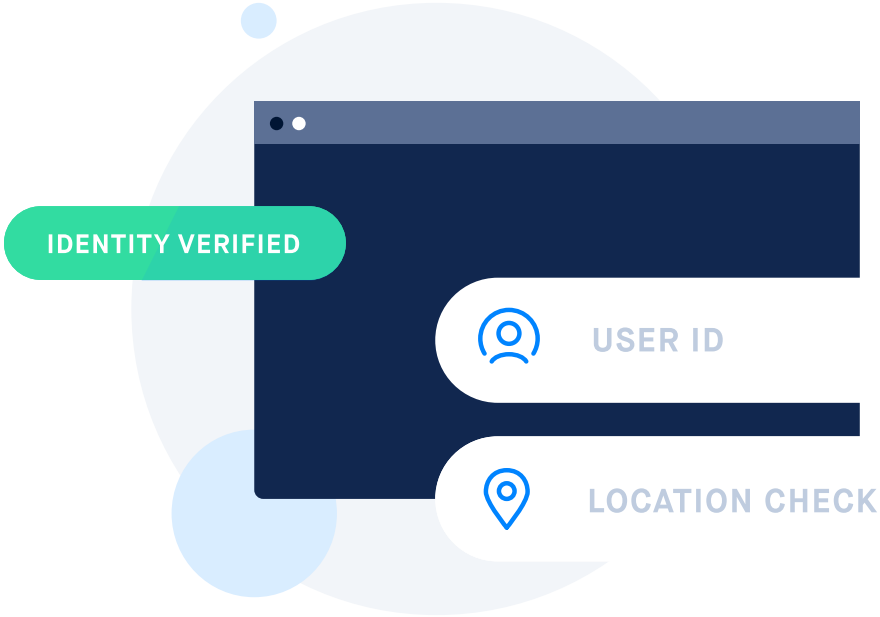
This data enhances an FI's ability to evaluate risk, understand user behavior and detect potentially suspicious activity. Not only that, requiring a location check at the onboarding step is often enough to send a fraudster – both human and bot – elsewhere to commit their crimes.

Just as importantly, verifying location helps FIs to better identify "good" customers they may not have otherwise onboarded.

Finally, geolocation data provides additional confidence in automated underwriting when opening merchant accounts. An example would be checking a merchant's verified location against their physical address. A wide discrepancy between the two could signal a fraudulent merchant trying to access the system.

Fast and frictionless

Location verification happens in the background – in milliseconds – without requiring customer input. FIs can deliver on their customer promise of a smooth and seamless user experience without sacrificing security.



2. Mitigate transaction fraud and slash false positives

Increase your ability to detect real fraud while reducing false positives and false negatives with embedded location checks.

Verified location data increases the certainty that a customer is who they say they are, which improves pass rates and cuts back on false positives. Greater confidence in a user's identity also reduces false negatives, closing the security holes bad actors use to access an FI's platform and commit fraud.

This verified data, along with the reduced false positives and negatives, allows FIs to better tune their automation process and models. This is because greater uncertainty about the validity of data can narrow the automation window or increase risk exposure after onboarding.

Best of all, increased assurance means people are less likely to have to deal with client fraud and identity theft on their accounts.

Take charge against chargebacks

Verified geolocation data fights chargeback fraud by:

1. Deterring fraudsters from the start.
2. Raising red flags that indicate a fraudulent transaction.
3. Providing evidence when defending a chargeback dispute.

3. Prevent account takeovers and account update fraud

Monitor account updates and user behavior by adding geolocation checks to continuous authentication. This protects against account takeovers and account update fraud.

For higher confidence, location checking can be employed throughout the customer's session – at login, when updating account and banking details or at other sensitive times. These location checks occur in the background, reducing the friction that occurs with traditional authentication methods, such as multi-factor authentication apps or frequent logins.

Continuous authentication ensures that certain data points collected during an online interaction, such as geolocation, typing cadence and mobile device orientation match "what should be expected" during the entire session.

Geolocation authentication throughout an online session, combined with the power of a real-time and historical risk engine, helps detect patterns of behavior that may indicate fraud. For example, a user's latitude/longitude or IP-based location coordinates jumping a large distance in a short period of time can indicate account sharing or account takeovers.

Enrich your risk modeling

Financial institutions can draw on alternative, high-quality data sources such as customer location and device information to validate the authenticity of a transaction.

Integrating verified geolocation data into risk models significantly improves the effectiveness and efficiency of fraud management.

When Unmasking Bad Actors, GeoComply Outsmarts IP-based Solutions

Bad actors are always finding new and more sophisticated ways to hide online in order to commit fraud. FIs that rely solely on IP addresses are missing out on critical location intelligence they need to protect themselves and their customers from fraud.

That's where GeoComply comes in. Our solution uses both a real-time and a historical risk engine to identify and flag potentially fraudulent activity. By analyzing both real-time and historical data, GeoComply enables organizations to identify and stop a wide variety of fraud including chargeback fraud, account sharing, card not present (CNP) fraud, account takeovers, and location fraud via the use of VPNs or other location spoofing tools.

Combat fast-evolving fraud threats with the most intelligent fraud detection solution

Location intelligence

Verify the true location of a user or a device. Detect location spoofing methods and suspicious location behaviors like location jumping.

Device intelligence

Identify suspicious behavior like multiple users from the same device or a device located out of a "regular" location.

Identity intelligence

Reduce account takeovers, identify synthetic identity fraud and help validate a customer's real identity.

3 billion+
analyzed transactions per year, and growing

400 million+
installed devices worldwide

350+
checks run on every transaction

Location Fraud Detection and Security for Every Type of Financial Institution

Banking

Improve risk management and compliance, while reducing fraud and customer friction.

Payments

Fight chargeback fraud, reduce false positives, and decrease risk exposure.

Crypto

Protect your platform by effectively blocking users from sanctioned or restricted jurisdictions.

Merchant Acquirers

Combat fraud by onboarding only legitimate merchants.

> "GeoComply's advanced geolocation system reduced our fraud and chargeback costs by over 80%."
>
> **JOSEPH PAPPANO,** Former SVP, Worldpay

GEOCOMPLY **The global market leader in geolocation security**

Location spoofing

Identifies sophisticated location spoofing methods such as VPNs, data centers, anonymizers, proxies and Tor exit nodes.

Account takeover

Detects whether an account was taken over by hackers after a long period of dormancy.

Synthetic identity

Detects when "home" location data from a smartphone is being spoofed as part of a synthetic identity at account creation.

Location jumping

Detects whether a user/device jumps a long distance in a short period of time.

Chargeback fraud

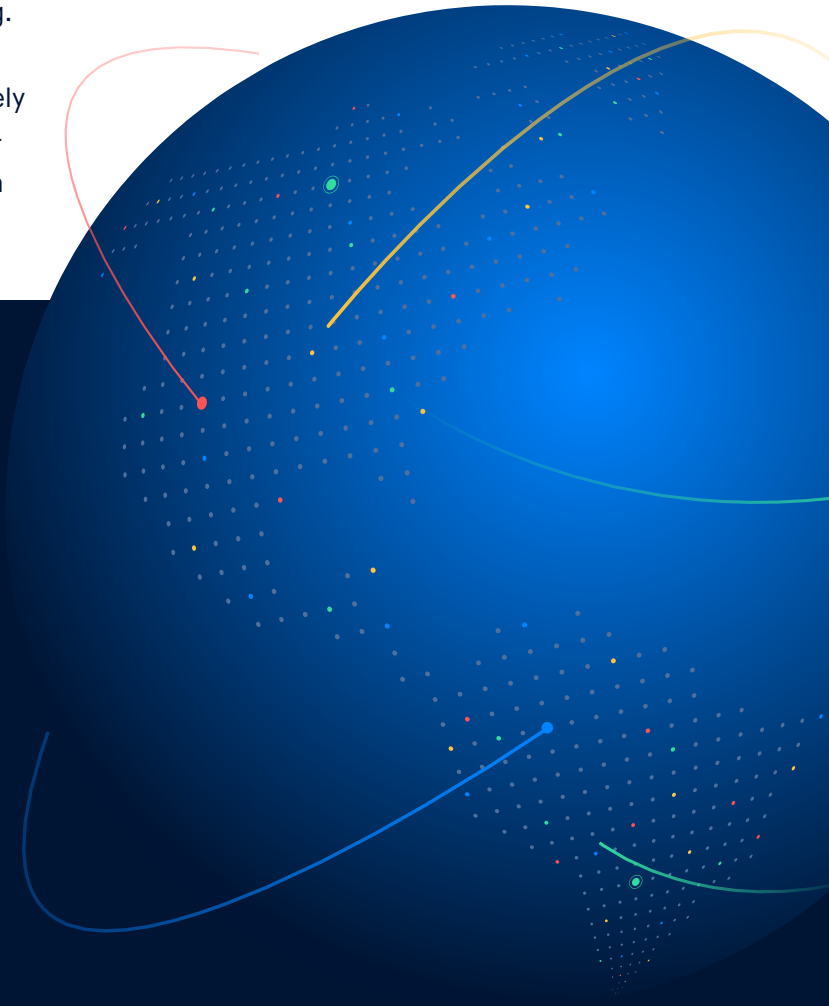
Provides historical location information of a device/user when defending chargeback disputes.

Fraud fingerprint

Creates a fingerprint for each location fraud method identified. You can flag future transactions with similar behavior.

Conclusion

Fraudsters are clever, relentless and remorseless, and the tools they use to commit crime are rapidly evolving. To combat emerging fraud risks, financial institutions must abandon the decades-old practice of relying solely on IP addresses for location. It's time to embrace 21st-century solutions – like the next generation of location intelligence. GeoComply is here to help.



About GeoComply

Founded in 2011, GeoComply provides fraud prevention and cybersecurity solutions that detect location fraud and help verify a user's true digital identity. Our award-winning products are based on the technologies developed for the highly regulated and complex U.S. online gaming and sports betting market. Beyond iGaming, GeoComply provides geolocation fraud detection solutions for streaming video broadcasters and the online banking, payments and cryptocurrency industries, building an impressive list of global customers including Amazon Prime Video, BBC, Akamai, Sightline, DraftKings, FanDuel and MGM.

The company's software is installed on over 400 million devices worldwide and analyzes over 3 billion transactions a year, placing GeoComply in a unique position to identify and counter both current and newly emerging fraud threats.

Proven and refined over 10 years of development, GeoComply's solutions incorporate location, device and identity intelligence along with advanced machine learning to detect and flag fraudulent activity. By integrating GeoComply's solutions into their processes and risk engines, organizations are able to identify fraud earlier in a user's engagement, better establish their true digital identity and empower digital trust.

GEOCOMPLY

solutions@geocomply.com | geocomply.com