

Are your cashless and digital wallets Title 31 compliant?

5 ways enhanced geolocation protects
you from fraud and BSA enforcement fines



Executive summary

Penalties for breaching the US Federal Bank Secrecy Act (Title 31), including anti-money laundering (AML) regulations and adherence to the Office of Foreign Asset Control (OFAC), are on the rise. In 2023, OFAC imposed penalties exceeding \$1.5 billion. Casinos, racinos, pari-mutuel facilities, advance deposit wagering services, and other licensed gaming operations generating over \$1 million in gross revenue annually (collectively referred to as Gaming Enterprises) are obligated to meet the stringent detection and reporting mandates of Title 31.

To effectively comply with Title 31 and mitigate the risk of fraud and financial crime, Gaming Enterprises incorporating cashless wallets on their gaming floor or digital wallets to their mobile wagering apps must accurately determine a user's true location. After all, according to the Department of Treasury, Title 31 **compliance requires Gaming Enterprises to know both the geographic location of the player, as well as the origin and source of funds.**

GeoComply's enhanced geolocation technology, which harnesses device-based signals from GPS, Wi-Fi triangulation and other sources to determine a user's location within meters, is critical for ensuring Title 31 compliance. This technology is in use in the tightly regulated U.S. iGaming and sports betting

“

We've been highlighting the importance of using geolocation tools as an effective internal control both in our sanctions compliance guidance ...but also through our enforcement actions.

Andrea Gacki
OFAC Director @ the ACAMS Sanctions Space Summit, Feb. 3, 2022

sectors enables Gaming Enterprises to integrate stringent geolocation checks into their mobile wagering applications. Enhanced Geolocation integration, applied during customer registration, and throughout the deposit and withdrawal processes, is essential for maintaining Title 31 compliance with both cashless systems and mobile wagering applications.

GeoComply helps Title 31 compliance for cashless and digital wallets in 5 key ways:



Blocks users in high-risk or sanctioned jurisdictions with verified location data from a user's device



Identifies VPNs, proxies, fraudulent IP addresses and other methods of location spoofing, which are considered regulatory "red flags"



Verifies location data to detect but also to report suspicious activities and transactions blocked due to OFAC sanctions



Prevent financial crimes by ensuring transactions are conducted within compliant and monitored environments



Protect against unauthorized access and account takeovers

Table of Contents

2 Executive summary

4 Introduction

5 IP Addresses: the main roadblock to ensure Title 31 compliance

6 Enhanced geolocation is the critical element to Title 31 compliance

7 How enhanced geolocation raises the Title 31 compliance bar

7 Block Users in High-Risk or Sanctioned Jurisdictions

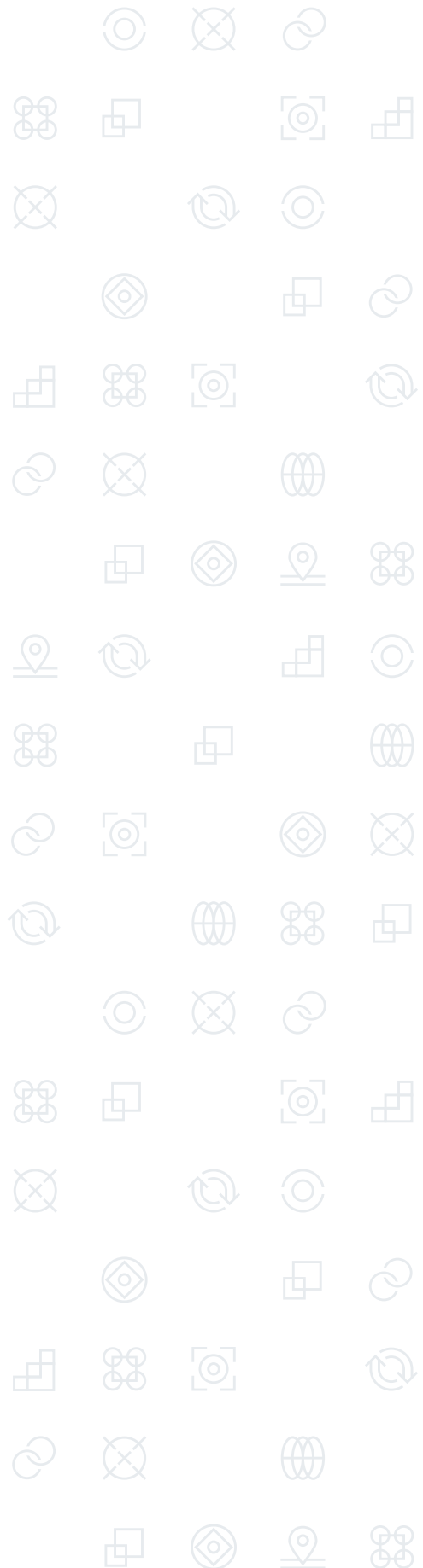
8 Detect VPN use, a regulatory “Red Flag”

9 Detect and report suspicious activity and block OFAC transactions

10 Prevent financial crime

10 Protect cashless and digital wallets from account takeovers

11 GeoComply: enhanced geolocation provides Title 31 compliance



Introduction

The emergence of cashless and digital wallets is a significant evolution in the gaming industry, bringing with it a dynamic regulatory landscape. State gaming regulators and legislative bodies are actively developing and refining frameworks to ensure proper oversight and governance. Title 31 empowers two agencies in the U.S. Treasury Department to enforce the **Bank Secrecy Act**. These agencies remain vigilant in detecting and deterring money laundering activities and the flow of terrorist funds through Gaming Enterprises.

Financial Crimes Enforcement Network (FinCEN): administers and enforces the Bank Secrecy Act (BSA), a federal anti-money laundering (AML) and counter-terrorist financing (CFT) statute. It also serves as the financial intelligence unit for the United States.

Office of Foreign Assets Control (OFAC): is the sanctions arm of the U.S. government, administering and enforcing trade and economic sanctions that support U.S. foreign policy and national security interests. In 2023, OFAC issued more than \$1.5 billion in penalties.

The BSA mandates that Gaming Enterprises report any suspicious activity or suspected money laundering activity to **FinCEN**. Additionally, OFAC requires Gaming Enterprises to identify, block, and report any financial transactions originating from OFAC-sanctioned countries within a **10-day** timeframe. Disregarding the requirements outlined in Title 31 is not only illegal, but it carries severe penalties, including hefty fines (\$1.5 billion in 2023 imposed by OFAC alone) and potential jail time.

This regulatory landscape introduces substantial risk for Gaming Enterprises transitioning to cashless and digital wallets, a significant departure from traditional cash-based transactions at gaming tables, slot machines, betting windows, and cashier desks, which are closely monitored through surveillance systems.

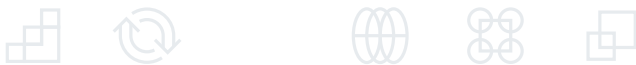
“

...strong sanctions compliance programs should be able to use geolocation tools to identify and prevent IP addresses that originate in sanctioned jurisdictions from accessing a company’s website and services for activity that is prohibited by OFAC’s regulations.

Sanctions Compliance Guidance for the Virtual Currency Industry, U.S. Department of the Treasury **Office of Foreign Assets Control (OFAC), Oct. 2021**

To navigate this challenge and ensure compliance within the evolving digital framework, Gaming Enterprises must adapt and enhance their Title 31 compliance programs.

Achieving Title 31 compliance for cashless and digital wallets can be straightforward with the right approach: By integrating advanced geolocation verification at key transaction points — registration, login, deposit, and withdrawal — within their cashless and mobile gaming apps, Gaming Enterprises can effectively monitor for and identify suspicious activities. Implementing this enhanced geolocation check ensures that Gaming Enterprises not only comply with regulatory requirements but also bolster their defenses against potential financial crimes. Adopting this strategic measure, Gaming Enterprises can seamlessly achieve compliance with Title 31 and ensure their operations are both secure and lawful.



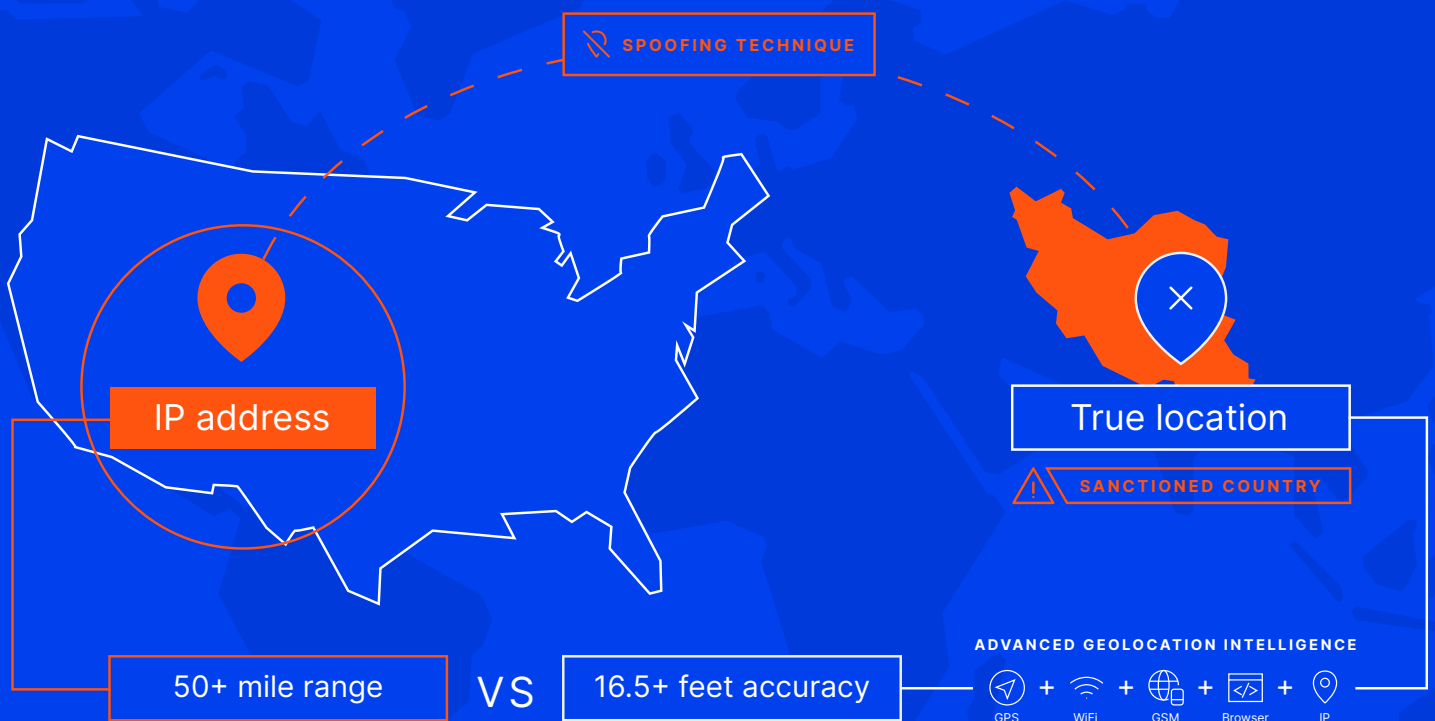
IP Addresses: the main roadblock to ensure Title 31 compliance

For cashless and digital wallets, Title 31 compliance starts with location. **Gaming Enterprises must be able to identify their customers' true location – the jurisdiction in which they reside or where their funds are being transferred.** Without this critical data point, making informed decisions on whether to permit or deny cashless transactions becomes impossible.

However, the geolocation standard in the financial services industry is antiquated, primarily relying on IP addresses. This method of determining location is vulnerable to manipulation and lacks precision. Bad actors have access to an arsenal of inexpensive location manipulation and spoofing tools – including virtual private networks (VPNs), proxies, and a host of other anonymizers. These tools make desktop and mobile IP addresses the easiest location data point to manipulate.

For example, in only six months, GeoComply detected 15 million attempted transactions where IP addresses were manipulated to appear falsely indicate users' locations were in the United States. In reality, these users were located elsewhere, including sanctioned jurisdictions like Iran and Cuba.

The gap between a user's location as indicated by an IP address and their actual location creates a significant risk to a cashless wallet and its banking and payments partners. It adds another layer of anonymity behind which bad actors can mask their true identity so they can more easily commit financial crimes. **It also raises a regulatory red flag that Gaming Enterprises offering cashless or digital wallets while aiming for AML and OFAC compliance should avoid.**

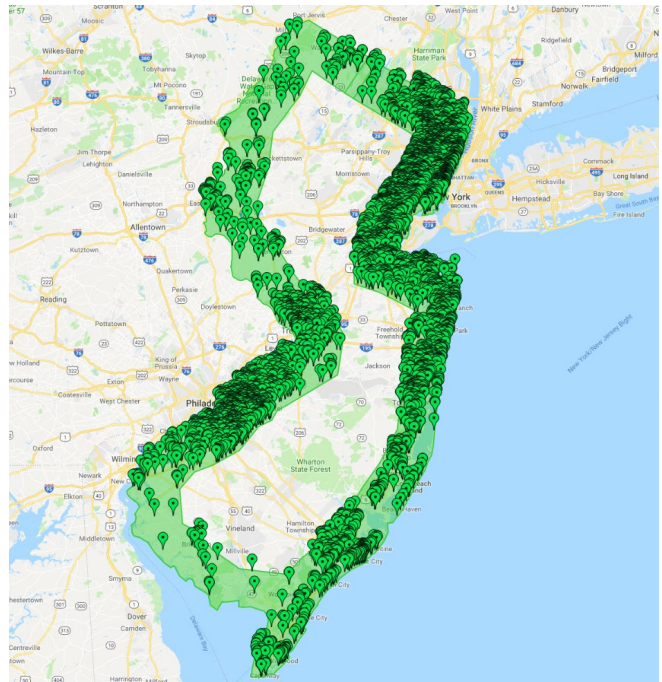


Enhanced geolocation is the critical element to Title 31 compliance

Regulators recognize the insufficiency of IP addresses for geolocation. They're calling for financial institutions – as outlined in the recent [OFAC guidance](#) – to improve their geolocation strategy to better identify and stop bad actors from exploiting the U.S. financial system.

The opportunity is now for Gaming Enterprises to blaze a new trail of compliance innovation by launching enhanced geolocation security within their cashless or digital wallets rather than wait for such guidance to become law.

By tapping into device-based geolocation data signals from multiple sources Gaming Enterprises are able to verify their off-property customer's true location. This is the same enhanced geolocation used in the highly regulated U.S. iGaming and sports betting industry, with its strict, state-specific requirements.



“

Advanced location signaling provides another critical data point that gives insight into the legitimacy and validity of transactions.

Jarod Koopman
Director, IRS – Criminal
Investigations (CI)

For example, more than 82 percent of all of New Jersey iGaming traffic is within 10 miles of the border, and approximately 44 percent is within two miles – enhanced geolocation ensures betting remains within the permitted jurisdiction (see figure above).

This enhanced accuracy is crucial to cashless and digital wallets, which also face a complex web of regulations from OFAC, FinCEN, and state regulatory agencies. Device-based geolocation security helps lift the heavy burden of Title 31 compliance by ensuring that each cashless or digital funding transaction occurs only where permitted and that the deposited funds do not originate from sanctioned countries. In turn, this ensures that their cashless and digital funds processing doesn't run afoul of Title 31 compliance.



2 Detect VPN use, a regulatory “Red Flag”

Both FinCEN and OFAC have highlighted inherent risks with illicit VPN use. As a result, in its virtual currency guidance, OFAC listed the following as a risk indicator of individuals who attempt to access a virtual currency exchange from an IP address or VPN connected to a sanctioned jurisdiction.

In addition, FinCEN and the CFTC jointly fined [BitMEX](#) \$100 million for “willfully” violating the Bank Secrecy Act. Despite BitMEX’s claims it did not transact with U.S. customers, FinCEN found the exchange did not screen for customers using a VPN to access its services and circumvent IP monitoring. In addition, BitMEX changed some U.S. customers’ information to hide their true location. With other financial markets acknowledging the power of geolocation intelligence, it’s imperative for Gaming Enterprises and gaming regulators to recognize the protections other markets are putting in place to safeguard the integrity of digital transactions.

Enhanced geolocation security analyzes IP addresses to:

- **Determine their source and potential association with malware**
- **Identify anonymizers such as VPNs and proxies**
- **Assess links to high-risk jurisdictions and activity**

“

Analytic tools can identify IP misattribution, for example, by screening IP addresses against known virtual private network (VPN) IP addresses and identifying improbable logins (such as the same user logging in with an IP address in the United States, and then shortly after with an IP address in Japan).

OFAC Sanctions Compliance Guidance for the Virtual Currency Industry, Oct. 2021

Enhanced geolocation security helps to determine the legitimacy of an IP address potentially associated with criminal activity. The gaming industry can raise the regulatory standard by proactively adopting geolocation security tools that detect VPNs and are able to pinpoint a user’s true location.

“

OFAC listed as a risk indicator, individuals who attempt to access a virtual currency exchange from an IP address or VPN connected to a sanctioned jurisdiction.



3 Detect and report suspicious activity and block OFAC transactions

Utilizing a robust “Know Your Customer” program strengthens the ability of Gaming Enterprises to create a true digital identity for their cashless or digital customers. It also enhances the ability of Gaming Enterprises to evaluate risk, understand their cashless or mobile gaming customer’s behavior, and detect potentially suspicious activity.

Yet, even if a cashless or mobile gaming customer is properly verified, their later behavior may subsequently flag their transactions as “suspicious.” For example, a verified cashless customer may use a VPN to mask their true location while depositing funds from a US bank while they are actually located in an OFAC-sanctioned country.

Gaming Enterprises need to analyze all data and behavior related to their cashless or digital wallet customers and their funding transactions – and enhanced geolocation security helps by:

- **Excluding users who are trying to login from certain countries**
- **Providing additional information about running processes and who may be using VPNs, virtual machines or remote desktop protocols**
- **Validating the exact location of a user at the time of a funding transaction. For instance, casinos can analyze incoming deposits to help them comply with AML and OFAC mandates**



“

The recent growth of gaming activity at brick-and-mortar casinos and online gaming platforms has raised the risk profile for U.S. casinos and gaming activity in the United States... There are also continuing challenges with AML/CFT supervision of some gaming operators - including online platforms, firms offering “games of skill” (as opposed to “games of chance”), and third-party operators that may engage in casino-like activities but that are not necessarily subject to BSA obligations because they are not licensed as casinos.... The risks in this sector involve not only compliance issues by casinos and card clubs regarding their respective AML/CFT obligations under the BSA, but also the misuse of casinos by foreign illicit actors...Law enforcement reporting and criminal prosecutions suggest continuing money laundering risks associated with placing illicit proceeds in casinos...There are continuing concerns regarding covered casinos’ and card clubs’ compliance with relevant AML/CFT obligations. Federal and state law enforcement underscored the extent to which covered casinos and card clubs may be fulfilling their required obligations, including SAR and CTR filing, but not taking other forms of proactive risk-based action against suspected money laundering.

2024 National Money Laundering Risk Assessment

4 Prevent financial crime

Financial crimes include money laundering and terrorist financing, which trigger regulatory reporting and increased FinCEN and OFAC scrutiny. Recently, OFAC [sanctioned a prepaid rewards program](#) for its role in allowing reward cards to be redeemed from persons residing in sanctioned jurisdictions.

Strong geofencing capabilities, combined with pinpoint location accuracy, help Gaming Enterprises detect and prevent, in real-time, suspicious activity that may be associated with terrorist financing or other crimes. In addition, Gaming Enterprises can analyze historical geolocation transactions to detect and flag high-risk behaviors, such as location jumping.

5 Protect cashless and digital wallets from account takeovers

Cyber criminals are using sophisticated methods to obtain a customer's account information which can then lead to theft of the customer's funds within their cashless wallet. In 2011, OFAC saw this as a serious financial crime that required financial institutions (including Gaming Enterprises) to report this activity in a [Suspicious Activity Report](#) (SAR).

“

In an account takeover, the target is the cashless customer's cashless or digital wallet, and the ultimate goal is to remove and steal all funds within that digital wallet.

“

This enforcement action underscores the importance of obtaining and using all available information to verify a customer's identity or residency, including by using location-related data....

da Vinci Payments – OFAC
Enforcement Release:
November 6, 2023

By performing a geolocation check at the time of login, deposit, and withdrawal, Gaming Enterprises would be able to detect the device fingerprint, location, and block access and/or withdrawal of player account funds when suspicious activity is detected. Additionally, this activity and all the location and device data detected would be included in the necessary SAR that would be submitted to OFAC.

By using highly accurate, enhanced geolocation solutions, Gaming Enterprises can demonstrate to regulators that compliance is not a standard checklist most financial institutions follow. Rather, they prove that compliance is a commitment to empowering the future of digital trust by making their cashless or digital wallets a safe and secure place to do business inside AND outside of their gaming premises.



GeoComply: enhanced geolocation provides Title 31 compliance

Backed by Blackstone, the world's largest private equity firm, GeoComply offers a trusted and accurate solution, processing more than 10 billion transactions a year and is installed on more than 400 million devices worldwide. Since launching in the highly regulated U.S. gaming market in 2013, GeoComply has honed its technology using device-based data (accurate up to 16.5 feet).

GeoComply uses zero-friction geolocation security to deliver enhanced geolocation accuracy to the largest brands in highly regulated markets – such as DraftKings, MGM, FanDuel, Caesars and others. GeoComply's enhance geolocation SDKs can be easily integrated into a mobile gaming application or casino mobile application that has a cashless wallet.



Online, OnPremise, OmniChannel.
We protect you and your customers

[12b+]

analyzed transactions per
year and growing

98%

tested accuracy in VPN
detection

400m+

installed devices
worldwide

Contact us today to learn more about how GeoComply can help
reduce your regulatory risk and combat financial crime.

solutions@geocomply.com



© 2024 GeoComply Solutions Inc. GEOCOMPLY and the GeoComply logo are trademarks of GeoComply Solutions Inc. Other names or logos mentioned herein may be the trademarks of GeoComply or their respective owners. The absence of the symbols ™ and ® in proximity to each trademark, or at all, herein is not a disclaimer of ownership of the related trademark. All rights reserved.