



STRENGTHENING
AML COMPLIANCE:

The Role of OFAC Sanctions in Nevada's Gaming Industry

By Sam Basile & Raichel Feenan

Navigating the expanding gaming and casino sector requires exceptional diligence from operators in establishing a robust program to address anti-money laundering (“AML”) laws and counter the financing of terrorism (“CFT”).¹ The rise of online gaming, coupled with the adoption of cashless and digital wallet technologies, has created a complex regulatory landscape. This evolution requires meticulous adherence to compliance requirements, highlighting the need for Nevada gaming operators to stay ahead. The gaming industry faces increasing pressure to enhance AML/CFT programs to combat sophisticated fraud and money laundering schemes, compelling the use of advanced technology and the development of enhanced customer due diligence protocols.

Nevada casinos with gross annual revenues exceeding \$1,000,000 must comply with Title 31 of the Bank Secrecy Act (“BSA”), which mandates that gaming enterprises develop and maintain an AML compliance program. As non-banking financial institutions (“NBFIs”), casinos must report suspicious activity to FinCEN to aid associated agencies in uncovering financial crime. Concurrently, the Office of Foreign Assets Control (“OFAC”) enforces economic and trade sanctions, prohibiting transactions with specified foreign entities and individuals posing national security threats.

Beyond federal reporting obligations, some states impose additional state-level requirements. In Nevada, the Nevada Gaming Commission (“NGC”) Regulation 5A.160 reinforces federal requirements by mandating that gaming operators file suspicious transaction reports related to online poker operations.² Historically, Nevada casinos were regulated by the NGC under NGC Regulation 6A for transaction reporting and recordkeeping, not by the federal government. However, NGC Regulation 6A was repealed in the face of pending amendments that would make the state regulations identical to those in the BSA.³ Following that repeal, in July 2007, FinCEN and the IRS became responsible for regulating and enforcing the BSA for Nevada gaming operators.

Although the AML requirements under the BSA are technically separate from the CFT requirements imposed by OFAC, they are interrelated obligations that Nevada casinos should view holistically to establish a robust AML/CFT compliance program. OFAC regulations, which apply universally to any U.S. individual and business, highlight the importance of CFT compliance while not explicitly outlined in BSA regulations. This universality underscores the critical role of OFAC compliance within an AML framework. By aligning OFAC



and BSA requirements, Nevada casinos can enhance their ability to prevent money laundering and other financial crimes, thereby upholding a high standard of integrity and security.

In 2023, OFAC imposed fines totaling \$1.5 billion, demonstrating the severity of penalties for non-compliance.⁴ Approximately two-thirds of these came from enforcement actions based, at least partly, on companies failing to detect and block transactions originating from OFAC sanctioned countries. Punitive measures for violating OFAC regulations are imposed under a strict liability standard, holding U.S. entities liable even if they are unaware their transactions have violated OFAC-administered sanctions. Therefore, adherence to OFAC is an essential component of AML/CFT compliance programs, protecting the integrity of the Nevada gaming industry and mitigating significant legal and financial risk for Nevada casinos.



The 2024 National Money Laundering Risk Assessment (“NMLRA”) highlights the vulnerabilities exploited by foreign actors in the U.S. gaming sector, who capitalize on regulatory variance across federal, state, and tribal jurisdictions, thus enabling opportunities for jurisdictional arbitrage.⁵ The rapid growth of online gaming, including sports betting and virtual slot and table gambling, introduces additional challenges and opportunities for illicit financial activities. These online gaming platforms typically operate in two primary models: as third-party operators under licensing agreements with land-based casinos or independently licensed by state regulatory authorities for online gaming. The NMLRA⁶ identifies how both models can facilitate money laundering. For instance, online gaming platforms may lack robust AML/CFT controls, operate independently of a BSA-covered casino, and be unaware of BSA obligations under licensing arrangements. Consequently, BSA-covered casinos might have limited visibility into potential criminal activity occurring on these third-party platforms.⁷

To address these challenges, Nevada casinos should closely evaluate the interactions between their land-based and digital offerings and assess the risks of whether their digital offerings have the equivalent AML/CFT protections as their established land-based compliance programs. Further, given the online presence of their digital offerings, Nevada casinos should consider integrating advanced technologies and best practices to enhance their AML/CFT compliance programs. One example is deploying state-of-the-art technology to identify their online customers’ location when wagering or depositing/withdrawing funds to their digital wallets.

As the gaming industry undergoes digital transformation, the financial industry’s guidance for virtual currency serves as an informative framework for Nevada, given its shared rapid growth and susceptibility to financial crime. The OFAC Sanctions Compliance Guidance for the Virtual Currency Industry emphasizes the need to employ geolocation tools to detect and prevent IP addresses originating from sanctioned jurisdictions. Failure to implement these controls can expose virtual currency companies and, by implication, Nevada casinos to AML/CFT compliance risks and potential legal consequences.

However, relying solely on IP addresses to determine location has limitations. The proliferation of inexpensive location spoofing tools such as virtual private networks (“VPNs”), proxies, and other anonymizers makes desktop and mobile IP addresses particularly vulnerable to manipulation. The OFAC Guidance noted that “analytical tools can identify IP misattribution, for example, by screening IP addresses against known 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).”

Additionally, OFAC’s 2023 enforcement actions demonstrate how companies that fail to block users from sanctioned jurisdictions put themselves at risk of significant financial penalties. One such enforcement action involved CoinList. CoinList is a virtual currency exchange platform that facilitates investments in cryptocurrencies. The company had various OFAC sanctions compliance measures in place, including screening customers against OFAC sanctions lists, conducting transaction monitoring, and using blockchain



analytics tools to detect interactions with high-risk jurisdictions. Yet their procedures failed to identify that some users were located in sanctioned countries. Specifically, some users claimed residency in a non-sanctioned country, but they conducted transactions from Crimea, a region under sanctions related to the Russia/Ukraine geopolitical conflict. This oversight led to CoinList processing 989 transactions for users in Crimea.⁸

Consequently, OFAC took enforcement action against CoinList for violating the Ukraine-/Russia-Related Sanctions Regulations, 31 C.F.R. § 589.207. The company agreed to pay a settlement of \$1,207,830. This enforcement action illustrates the importance of stringent OFAC sanctions compliance measures. In response to the enforcement action and as part of their remediation efforts, CoinList implemented additional measures. These included:

1. IP geo-blocking: Introducing technology to “detect IP addresses in sanctioned jurisdictions and prevent users from accessing their accounts from those IP addresses.”
2. Enhanced vendor partnerships: Investing in “new vendors for review and verification of identity documents and restricted party screenings.”
3. VPN detection: Employing tools “to detect the use of VPNs that can obscure users’ location,” thereby enhancing their ability to comply with sanctions.⁹

Nevada casinos can reduce the risk of violating OFAC regulations and protect their businesses from enforcement action by deploying advanced technologies within their digital platforms, whether cashless or online. Leveraging device-based geolocation data and validating it with multiple trusted sources will enable Nevada casinos to accurately verify their customers' true location while wagering or depositing/withdrawing to their digital wallets. This technology has already demonstrated its efficacy in the highly regulated U.S. iGaming and sports betting sectors, offering enhanced accuracy for all gaming industry segments.

Nevada casinos utilizing digital wallets in their cashless and online platforms face a complex regulatory landscape involving the BSA, OFAC, FinCEN, and the NGC. These new digital environments present challenges that their traditional land-based operations have not previously navigated. Given the scrutiny surrounding the gaming industry, it is crucial for

Nevada casinos to prioritize robust AML/CFT compliance programs to protect the integrity of Nevada gaming.

In light of the evolving nature of financial crimes, particularly in the digital era, and recent OFAC enforcement actions for sanctions violations, Nevada casinos should conduct comprehensive reviews of their AML/CFT compliance programs. Nevada casinos should evaluate whether they have the appropriate measures and technology to detect, block, and report digital suspicious activity effectively. ■



Sam Basile previously served as outside legal counsel to GeoComply, a cybersecurity and fraud prevention company that delivers geolocation and user authentication technologies, just after its launch in 2012 and is now GeoComply's Vice President of Business Development - North American Gaming. Sam has 30-plus years as a gaming industry executive and attorney, including serving as Global Chief Compliance Officer, independent audit committee member, and member of several gaming compliance committees. Further, Sam's experience includes working at or consulting for such renowned gaming companies as Aristocrat Technologies, Aruze Gaming America, American Gaming & Electronics, Bragg Gaming Group, Gaming Arts, LVDC, Mirage Resorts, NYX Gaming Group, Spin Games, and Zitro Gaming.



Raichel Feenan is a Political Advocacy Specialist at GeoComply. She joined the company in early 2023 after graduating from the University of British Columbia with a bachelor's degree in political science and a minor in law and society. Although she has recently entered the gaming industry, her desire to work in a dynamic and fast-paced environment drew her to GeoComply, where she is quickly advancing her skills in regulatory analytics and business development.

¹ See, 31 C.F.R. §1021.200, et seq. (2024), and Office of Foreign Asset Control (OFAC), *A Framework for OFAC Compliance Commitments* (<https://ofac.treasury.gov/media/16331/download?inline>), U.S. Dep't of Treas., (Undated).

² See, Nev. Gaming Comm'n Reg. 5A.160.

³ Gannon, K., Goodbye 6A, Hello BSA (https://www.nvbar.org/wp-content/uploads/Goodbye_6A_Hello_BSA_0.pdf), *Nevada Gaming Lawyer*, (Jul 2007).

⁴ OFAC, *2023 Enforcement Information* (<https://ofac.treasury.gov/civil-penalties-and-enforcement-information/2023-enforcement-information>), U.S. Dep't of Treas., (2023).

⁵ U.S. Dep't of Treas., *2024 National Money Laundering Risk Assessment* (<https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf>), (February 2024).

⁶ *Id.*

⁷ *Id.*

⁸ OFAC, *OFAC Settles with CoinList Markets LLC for \$1,207,830 Related to Apparent Violations of the Ukraine-/Russia-Related Sanctions Regulations* (<https://ofac.treasury.gov/media/932406/download?inline>), U.S. Dep't of Treas., (Dec 13, 2023).

⁹ *Id.*

BALLARD GOES BEYOND.

Ballard Spahr
LLP

