

Illuminating the Bank Secrecy Act: Key Takeaways from Recent DOJ Settlements

Client Alerts

February 12, 2024

By: Reid Schar, Wade A. Thomson, Carolyn S. Small

The Department of Justice recently announced settlements with two casinos to resolve an investigation into alleged money laundering and violations of the Bank Secrecy Act (BSA). The settlements required the casinos to pay a combined monetary fine of \$7.45 million and enhance their anti-money-laundering compliance programs. The resolutions are a signal that DOJ may be returning its BSA enforcement efforts to casinos almost a decade after many casinos were fined millions for BSA violations in what was seen as a watershed moment for the industry. The settlement agreements provide insight into potential pitfalls in anti-money-laundering compliance programs and are an opportunity for casinos and other financial institutions to examine existing programs.

The Bank Secrecy Act (BSA)

The BSA was enacted in 1970 to prevent banks and other financial institutions from being used as tools to launder criminal proceeds, finance terrorism, or commit other financial crimes. To accomplish this purpose, the BSA and related regulations require financial institutions to report suspicious transactions to the Department of the Treasury and establish anti-money-laundering programs. The statute defines “financial institution” broadly to include a wide range of businesses beyond just banks. For instance, businesses that are considered “financial institution[s]” include travel agencies, broker-dealers, and casinos with an annual gaming revenue of more than \$1 million. 31 U.S.C. § 5312(a)(2). The definition of “financial institution” also includes currency exchanges and businesses engaged in the transmission of currency. The US Department of the Treasury Financial Crimes Enforcement Network (FinCEN) issued interpretive guidance in 2019 explaining how regulations relating to money services businesses apply to businesses that transmit virtual currencies, such as cryptocurrency exchanges. Binance Holdings Limited, for instance, recently conceded in a plea agreement it qualified as a money transmitter in the United States that was required to comply with the BSA during a period in which it operated a cryptocurrency exchange in the US that served a substantial number of US users.

According to the BSA, anti-money-laundering programs must include, at minimum, internal policies, procedures, and controls; a designated compliance officer; ongoing employee training; and an

independent audit function. 31 U.S.C. § 5318(h). Department of Treasury regulations set forth additional requirements based on the type of business. The regulations governing casinos require, among other things, that anti-money-laundering programs include procedures for using “all available information” to identify and verify customers and determine whether a transaction requires the filing of a suspicious activity report. 31 C.F.R. § 102.210(b)(2)(v).

Failure to comply with the BSA can result in civil and criminal penalties. Penalties vary depending on the type of violation. For certain violations, financial institutions can be fined up to \$1 million per violation.

The DOJ Settlements

The DOJ recently reached settlements with two casinos in related matters involving BSA violations.

One of the casinos conceded in a non-prosecution agreement that the president of the casino and two casino hosts were aware that a casino patron was running an illegal bookmaking business; yet they continued allowing him to use criminal proceeds at the casino, and in fact encouraged him to do so by providing him with complimentary benefits. Despite having been trained in their responsibility to affirmatively reach out to the compliance team if they observed suspicious activity, no employee reported the source of the illicit proceeds to compliance personnel or law enforcement. As a result, the casino failed to file suspicious activity reports regarding the transactions.

Additionally, although the casino’s anti-money-laundering compliance program included a risk-based assessment to identify money-laundering risks, it did not assign any risk for situations in which its customers repeatedly conducted large cash transactions with large-dollar denominations at the casino. Moreover, internal auditors had recommended using a risk-based approach to determine whether to continue monitoring customers who were deemed suspicious, but the casino declined to adopt the recommendation, believing that its current approach was sufficient. The compliance team therefore did not conduct an analysis to determine occurrences of large-denomination cash transactions or patterns of such transactions. The team also did not continue monitoring the patron engaged in illegal bookmaking, even after becoming suspicious of his source of income in 2017.

Finally, the compliance program failed to instruct the compliance team to use all available information when performing “know your customer” reviews. Specifically, even though the marketing departments regularly interacted and socialized with customers, the compliance program did not require the compliance team to consult with the marketing hosts about information available to them in relation to “know your customer” procedures and procedures for determining whether a transaction warranted the filing of a suspicious activity report.

Similar to the first casino, the second casino conceded that during its prior ownership, a casino host was aware that the same patron described above was running an illegal bookmaking business, but still allowed the patron to use illicit proceeds at the casino and gave him complimentary benefits to

encourage his spending. Again, the host failed to report the source of the patron's funds to the compliance team or law enforcement, despite having been trained to do so.

Unlike the first casino, the second casino's anti-money laundering compliance program was in fact designed to use all available information; and the compliance team routinely requested information from the marketing department, including hosts. Although the compliance department became suspicious of the patron and requested additional information from the host, the documentation the host forwarded—which the compliance department accepted—did not show the source of his funds.

Notably, both casinos received cooperation credit for, among other things, voluntarily making employees available for interviews and making voluntary document disclosures. The non-prosecution agreements also expressly accounted for the fact that the casinos had timely engaged in remedial measures and no longer employed or were affiliated with the individuals implicated in the conduct at issue.

Key Takeaways

These settlements provide some key takeaways for casinos and other businesses that are subject to the BSA:

First, casinos' anti-money-laundering compliance programs must include procedures for using all available information to verify customer identity and information and determine whether any transactions or patterns of transactions must be reported. Given the requirement to use all available information, these procedures should include requirements that the compliance team consult with customer-facing departments, like marketing departments.

Second, when a compliance department at a financial institution consults with other departments to obtain information, it should ensure it is obtaining meaningful responses to its inquiries. Any information or documentation obtained should adequately address the compliance team's concerns, including, for example, showing the source of a customer's income.

Third, financial institutions should proceed with caution when declining to adopt recommendations by auditors on ways to enhance their anti-money laundering programs. The short-term savings on costs or effort may not be worth the long-term risks.

Fourth, if any BSA violations or compliance-program deficiencies are discovered, financial institutions should engage in remedial measures as soon as possible by, for example, promptly filing any suspicious activity reports that should have been filed, conducting a lookback to determine whether any previously filed reports should be updated, and considering external review of its compliance program. They should also consider instituting appropriate disciplinary action for any employee that engaged in misconduct or violated policies.

Conclusion

DOJ and regulators are likely to continue to actively enforce the BSA against individuals and financial institutions. Financial institutions should ensure that existing compliance programs not only satisfy statutory and regulatory requirements but are operating effectively to verify customer information and identify suspicious transactions, even when individual employees are being less than forthcoming.

Jenner & Block's Sports and Gaming Practice was recognized as a 2023 Practice Group of the Year by *Law360* and continues to monitor legal developments relevant to the sports and gaming industries.

Related Attorneys



Reid Schar

Managing Partner, San Francisco
rschar@jenner.com
+1 628 267 6858



Wade A. Thomson

Partner
wthomson@jenner.com
+1 312 840 8613



Carolyn S. Small

Partner

csmall@jenner.com

+1 213 239 2250

Related Capabilities

Investigations, Compliance, and Defense

© 2026 Jenner & Block LLP. Attorney Advertising. Jenner & Block LLP is an Illinois Limited Liability Partnership including professional corporations. This publication, presentation, or event is not intended to provide legal advice but to provide information on legal matters and/or firm news of interest to our clients and colleagues. Readers or attendees should seek specific legal advice before taking any action with respect to matters mentioned in this publication or at this event. The attorney responsible for this communication is Brent E. Kidwell, Jenner & Block LLP, 353 N. Clark Street, Chicago, IL 60654-3456. Prior results do not guarantee a similar outcome. Jenner & Block London LLP, an affiliate of Jenner & Block LLP, is a limited liability partnership established under the laws of the State of Delaware, USA and is authorised and regulated by the Solicitors Regulation Authority with SRA number 615729. Information regarding the data we collect and the rights you have over your data can be found in our Privacy Notice. For further inquiries, please contact dataprotection@jenner.com.

Stay Informed

