

Regulators Clamp Down on Casinos for Noncompliance

Sareena Sawhney

BACKGROUND

BETWEEN FEBRUARY 2005 AND MARCH 2007, Las Vegas Sands Corp. received wire transfers totaling \$45 million, and cashier's checks totaling \$13 million, on behalf of one gambler. The wire transfers originated from several companies and individuals, and Las Vegas Sands Corp. did not identify the suspicious nature of these multiple transfers linked to the gambler. As a result, the casino failed to file the necessary suspicious activity reports about these payments required by federal law.¹

Following an investigation by the U.S. Department of Justice, Las Vegas Sands Corp. reached a non-prosecution agreement in 2013 that required it to pay \$47 million to the U.S. government and review its anti-money laundering policies, which should have caused it to file various reports with the government. As a result of this settlement, Las Vegas Sands Corp. now links bonuses to policy compliance and will claw back bonuses when non-compliance is discovered.²

This is just one of many examples corresponding to a recent surge in government investigations of companies' and organizations' money-laundering monitoring and compliance programs. In particular, U.S. regulators have more aggressively brought enforcement actions against casinos and banks for their failure to comply with anti-money laundering rules and regulations. The Financial Crimes Enforcement Network (FinCEN) has made it an enforcement priority to ensure compliance with the

Bank Secrecy Act (BSA) and the implementation of an effective anti-money laundering (AML) program among casinos. In addition, the U.S. Department of Justice has put casinos on notice that they must develop and implement effective AML programs. Noncompliance may result in civil penalties, criminal penalties, or both. The enforcement efforts reflect a desire to find hidden assets and accompanying unpaid income taxes, as well as to impede terrorist financing.

This heightened enforcement affects organizations and businesses licensed to operate as casinos or card clubs having gross annual gaming revenues (GAGR) greater than \$1,000,000. Title 31 of the BSA designates organizations or businesses meeting these criteria as financial institutions that are subject to the requirements of the BSA. This requires affected casinos to have an effective AML program in place that is risk-based and tailored to its own operations. As such, there is no "one size fits all" program that casinos can adopt.³ Effective AML programs are designed to prevent casinos from being used to facilitate money laundering and terrorist financing. The AML program is developed based on consideration of the risks presented by a casino's products and services, location, and customer base. Different components of risk, based on different games or customer bases, for example, should have separate risk-based compliance programs that are individually monitored by a compliance officer.

An assessment of the risks facing a casino should be based on relevant factors including the casino's

Sareena Sawhney, MBA, CFE, CAMS, MAFF, is a director in the Litigation and Corporate Financial Advisory Services Group at Marks Paneth LLP in New York, NY. Ms. Sawhney focuses on providing services in the areas of complex fraud investigations, forensic accounting examinations and AML compliance, as well as services related to commercial litigation and comprehensive damage analyses.

¹See Press Release, U.S. Attorney's Office Central District of California, Operator of Venetian Resort in Las Vegas Agrees to Return Over \$47 Million After Receiving Money Under Suspicious Circumstances (Aug. 27, 2013).

²See Alexandra Berzon, *Casinos Heed U.S. Reporting Warning*, WALL ST. J., Sept. 2, 2013.

³See 31 C.F.R. § 1010.210.

size, its location, dollar volume, types of games, and type and/or nature of its customers, as well as effective internal controls. The AML program that is developed in response to the risk assessment must include, at a minimum:

- Internal controls, policies, and procedures designed to ensure compliance with the BSA;
- Training of casino employees;
- An experienced compliance officer;
- Independent testing for compliance;
- Know Your Customer (KYC) procedures; and
- Procedures for identifying transactions or patterns that may be suspicious.

FinCEN's reporting requirements require that casinos file Customer Transaction Reports (CTRs) and/or Suspicious Activity Reports (SARs). A CTR must be filed by casinos to report each transaction in currency involving cash-in and cash-out of greater than \$10,000 on only one particular gaming day.⁴ Reportable cash-in transactions include: the purchase of chips, tokens, and plaques; front money and safekeeping deposits; bets of currency; and the payment on any form of credit. Less obvious are reportable transactions related to the purchase of a casino's check; exchange of currency for other currency (including foreign currency); and wire transfers from another casino on behalf of a customer.⁵

Reportable cash-out transactions include: the redemption of chips, tokens, and plaques; front money and safekeeping withdrawals; payments on bets (excluding slot and video lottery terminal jackpots); and the advance on any form of credit. Less obvious reportable cash-out transactions include: payments on wire transfers from another casino to a customer; the cashing of checks or other negotiable instruments; exchange of currency for other currency (including foreign currency); and reimbursements for a customer's travel and entertainment expenses by the casino.⁶

In addition, multiple currency transactions are treated as a single transaction if the casino has knowledge that they were initiated by or on behalf of one individual, and as long as either cash-in or cash-out transactions total more than \$10,000 in a given day.⁷ There are certain procedures that casinos must perform to gain such knowledge. CTRs must be filed electronically within 15 days following the day the reportable transaction occurs.⁸

SARs must be filed for any suspicious transactions that may be relevant to the possible violation of any law or regulation and which involve at least \$5,000 in funds or other assets.⁹ The BSA provides guidance on what constitutes a "suspicious transaction." The following excerpt is provided to demonstrate the efforts required by a casino to determine how the funds were acquired by the transferee before applying considerable judgment to determine that the transfer constitutes suspicious activity:

A transaction requires reporting under the terms of this section if it is conducted or attempted by, at, or through a casino, and involves or aggregates at least \$5,000 in funds or other assets, and the casino knows, suspects, or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is part):¹⁰

- (i) Involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any Federal law or regulation or to evade any transaction reporting requirement under Federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation;
- (ii) Is designed, whether through structuring or other means, to evade any requirements of this chapter or of any other regulations promulgated under the Bank Secrecy Act;
- (iii) Has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the casino knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or
- (iv) Involves use of the casino to facilitate criminal activity.

⁴See 31 C.F.R. § 1021.311.

⁵See 31 C.F.R. § 1021.311(a).

⁶See 31 C.F.R. § 1021.311(b).

⁷See 31 C.F.R. § 1021.313.

⁸See 31 C.F.R. § 1010.306(a)(1).

⁹See 31 C.F.R. § 1010.306(a)(2).

¹⁰See 31 C.F.R. § 1021.320(2).

Suspicious transactions are reported by completing a Suspicious Activity Report by Casinos (SARC). All supporting materials collected during the assessment and used in the determination must be maintained by the casino whether or not a transaction is (or a series of transactions are) determined to be reportable suspicious transactions.¹¹ The casino is required to make all supporting documentation available to any Federal, state, or local law enforcement agency, or to any Federal or state regulatory authority that examines the casino for compliance with the Bank Secrecy Act.¹²

IDENTIFYING SUSPICIOUS TRANSACTIONS

FinCEN Director Jennifer Shasky Calvery recently described what steps FinCEN expects casinos to take in making suspicious activity determinations and explained what FinCEN and the Internal Revenue Service (IRS) will be looking for when conducting BSA casino audits.¹³ She stressed compliance with mandatory information sharing and with AML requirements that casinos know the source of their customer's gambling funds.

KNOWING YOUR CUSTOMER

AML requires casinos to be aware of a customer's source of funds. KYC procedures dictate that casinos probe their customers for more information to help identify high-risk transactions. This designation can be based on the source of the transfer, such as an international wire transfer from a high-risk jurisdiction or from a politically exposed person (PEP), or on the type of transfer, such as a large cash deposit. Director Shasky Calvery emphasizes that "a casino's capability for knowing its customers' preferences and credit information combined with [its] security technology, can and should be leveraged to piece together relevant information to understand [its] customers' source of funds." The failure to do so puts the casino at risk.

Recordkeeping requirements state that when a deposit or account is in the name of one or more persons, the casino must obtain the name, permanent address, and social security number of *each* person having a financial interest in the deposit or account. The identity of each person must also be verified at

the time the deposit is made or the account is opened. If a person is a nonresident alien, the casino must obtain the person's passport number or a description of another government document used to verify identity.

Payout slips and currency are held in a safekeeping account with instructions that the deposit cannot be released to a customer until valid identification is provided.¹⁴

IMPORTANCE OF RISK-BASED AML COMPLIANCE

The starting point in virtually all BSA audits is the casino's written AML risk assessment. Casinos need to make sure that their assessment is current; otherwise, they will be instructed to prepare one. Additionally, if a casino doesn't have one, or if the IRS decides that its risk assessment is obsolete or incomplete, the IRS will develop its own risk assessment and use it as the starting point for that casino's audit.

Because AML is risk-based, there is no one program that can fit all casinos' needs. FinCEN cannot guide casinos as to what to do or issue a definitive "yes-or-no/check-the-box" form because every casino—and therefore its money laundering risk—is different. A casino's program must depend on the risks it faces, which in turn are based on the types of financial services it offers, the profile of its customers, the community in which it is located, and the internal controls it currently has in place. It is the variety, frequency, and volume of transactions that take place at a casino that makes this sector vulnerable to money laundering. Casinos are a cash-intensive business, which is why it is extremely crucial to be aware of accepting monies if the identity of the customer is unknown.

Casinos need to cultivate a "culture of compliance." While this should not be difficult for tribal governments, there is sometimes a lack of connection between the compliance mandates of tribal gaming commissions and the financial incentives

¹¹See 31 C.F.R. § 1021.320.

¹²See 31 C.F.R. § 1021.320.

¹³See Director Jennifer Shasky Calvery, Remarks at the 2014 Bank Secrecy Act Conference (June 12, 2014), <http://www.fincen.gov/news_room/speech/pdf/20140612.pdf>.

¹⁴See 31 C.F.R. § 1021.410.

of tribal casino managers. Casino management, not just tribal gaming commissioners, must set the right “tone at the top” on compliance matters.

INFORMATION SHARING MANDATES AND OPPORTUNITIES

Information sharing allows the exchange of information relating to money laundering and terrorist financing under a safe harbor that prevents the party giving information from being sued in court. The two types of information sharing are mandatory sharing under section 314(a) and voluntary sharing under section 314(b) of the USA PATRIOT Act.

Mandatory information sharing requires recipients to promptly respond to written FinCEN inquiries about accounts maintained by or transactions conducted with certain individuals or entities named in the inquiry. In the past, FinCEN has not issued 314(a) requests to casinos, but has issued more than 43,000 requests to banks and other entities. Noting in her speech that 95% of these requests have contributed to arrests or indictments, Director Shasky Calvery stressed that FinCEN will start sending 314(a) requests to casinos in the future.

Since mandatory information sharing is required by existing regulations, casinos should already have procedures in place for responding to these requests.¹⁵ However, many casinos do not because FinCEN has not issued 314(a) requests to casinos in the past. This, however, is likely to change, and casinos will need to prepare written procedures designed to receive—and properly respond to—314(a) requests from FinCEN.

Voluntary information sharing in section 314(b) allows casinos to share information (including specific customer information) with other casinos, as well as with banks and other financial institutions, for the purpose of identifying and reporting activities that the casino suspects may involve possible money laundering or terrorist information.

Casinos must consider registering for voluntary information sharing as one means of using all available information to determine the occurrence of any

transactions or patterns of transactions required to be reported as suspicious.

They also need an ongoing monitoring process in order to assess activity for all customers, which process must place emphasis on the customers and activity with the highest risk. The ongoing monitoring process should be used to identify suspicious activity that may ultimately result in the filing of a SARC. Casinos that already have an AML transaction monitoring system should consider having an independent consultant test their system in order to determine the adequacy of the monitoring system and evaluate whether changes need to be made to the system and/or policies. For this reason, it is extremely important that institutions have a program in place to continually review the performance of their transaction monitoring system and make enhancements to address any deficiencies.

It is also important that once AML activity has been flagged, AML analysts at the casino conduct adequate due diligence needed to assess whether a SARC needs to be filed or a client profile needs to be updated. Often, casinos run the risk of allocating insufficient resources to reviewing cases of suspicious activity, resulting in being deemed as having inadequate AML monitoring systems, which makes them subject to hefty fines.

CONCLUSION

An independent review of an AML transaction monitoring system may help determine whether the system is effective in comparing the customer’s account/transaction history to the customer’s specific profile information and a relevant peer group. Such a review may also compare the customer’s transaction history against established money laundering scenarios to help identify potentially suspicious transactions.

Having a monitoring system in place supplemented by employee training, compliance oversight, internal controls, and independent testing should form the components of a complete AML compliance program.

¹⁵See 31 C.F.R. § 1010.520.