2025

BEST PRACTICES FOR Anti-Money Laundering Compliance

AMERICAN GAMING ASSOCIATION®

Table of Contents

Table of Contents Cont.

Preface

The American Gaming Association (AGA) is the premier national trade group representing the $261 billion U.S. casino industry, which supports 1.8 million jobs nationwide. AGA members include commercial and tribal casino operators, suppliers, and other entities affiliated with the gaming industry. It is the mission of the AGA to achieve sound policies and regulations consistent with casino gaming's modern appeal and vast economic contributions.

The U.S. gaming industry is one of the most heavily regulated and controlled business sectors across the globe. In addition to comprehensive and stringent state gaming regulations, most U.S. gaming operations are also subject to federal anti-money laundering (AML) and combating the financing of terrorism (CFT) requirements.[1]

The modern casino and gaming operation is typically an entertainment service that offers its patrons highly regulated gaming at in-person casinos or other brick-and-mortar properties and/or through online gaming and sports betting platforms. Often, brick-and-mortar casinos are also combined with retail sportsbooks, racetracks, hotels, dining options, and live entertainment. To facilitate gaming activity, casinos, as well as online and mobile gaming operators, ordinarily provide some form of financial services to their patrons. They endeavor to ensure that these financial services are used for gaming-related purposes. Although most patrons visit casinos or mobile gaming applications for entertainment, leisure, and diversion, those engaged in illegal activity may attempt to use a casino or gaming platform's financial services to conceal or transfer illicit wealth.

$261B

THE VALUE OF THE U.S. CASINO INDUSTRY REPRESENTED BY AGA, THE PREMIER NATIONAL TRADE GROUP

$1.8M

JOBS NATIONWIDE SUPPORTED BY THE INDUSTRY

This document is an attempt to distill the practices that a wide range of gaming businesses — including land-based casinos, sportsbooks, and interactive and mobile gaming operations — have adopted to comply with federal AML requirements under the Bank Secrecy Act (BSA) and associated regulatory expectations. Throughout this guide, we generally use the term "casino" to refer to any physical, online, or mobile BSA-regulated gaming or sports betting business, unless explicitly described otherwise.

This document is not intended to be a checklist of actions required or expected of every casino and should not be applied arbitrarily to any individual situation or on a blanket basis. The recommendations in this document are not exhaustive and may vary in applicability for distinct types of gaming businesses. AML/CFT Programs should be risk-based, and casinos have different risk profiles, so individual casinos will have good reasons for departing from or modifying a procedure in this document, or for developing supplemental or alternative procedures, including appropriate approvals and documentation of decision-making.

It is important to note that best practices will continue to evolve in response to innovative technologies, enhanced compliance resources, regulatory guidance and enforcement decisions, and the Administration's enforcement priorities and approach toward regulations. Moreover, in some instances, industry practices may go beyond a legal requirement established by statute or regulation. Accordingly, this document should not be considered a guide to compliance with AML legal requirements. There are also open legal questions around the applicability of the BSA to certain types of gaming businesses, such as online operators, pending further guidance from the Financial Crimes Enforcement Network (FinCEN).

[1] As used in this paper, money laundering and AML compliance also encompasses the terms terror financing and CFT.

Introduction

Since 1985, state-licensed casinos have been defined as "financial institutions" under the BSA. Accordingly, they are subject to BSA reporting, recordkeeping, and AML/CFT Program requirements. These regulatory requirements are contained in 31 C.F.R. Part 1021, and the U.S. Department of the Treasury's FinCEN periodically publishes regulatory guidance regarding those requirements on its website. Further, the industry's AML compliance programs are also influenced by guidance from the U.S. Treasury, including the National Strategy for Combating Terrorist and Other Illicit Financing (National Illicit Finance Strategy) and the National Money Laundering Risk Assessment (NMLRA).[2]

Primary BSA Requirements and Regulatory Expectations for Casinos

Casinos are required to implement and maintain an AML and CFT Program (hereinafter, AML/CFT Program or BSA/AML Program) that complies with the BSA's AML Program, reporting, and recordkeeping requirements.[3] A casino's AML/CFT Program must be risk-based and effective in practice, not just on paper, and it should include, at a minimum:

- An annual risk assessment
- A formal know your customer (KYC) program
- A system of internal controls, policies, and procedures to ensure ongoing compliance with the BSA's requirements, including suspicious activity and currency transaction reporting and recordkeeping requirements
- Internal and/or external independent assessments of the AML/CFT Program
- Appropriate, ongoing training of casino personnel
- Designation of an individual or individuals charged with ensuring day-to-day compliance with the casino's AML/CFT Program and BSA requirements (the AML Officer)
- Automated programs to aid in ensuring BSA compliance
- A compliance testing/quality assurance program for AML functions
- Approval of the AML/CFT Program by the board of directors or an equivalent oversight committee for institutions without a board

To safeguard the integrity of the casino industry and the U.S. financial system, casinos and gaming operators have developed effective risk-based programs to ensure compliance with the legal requirements of the BSA and associated AML statutes and regulations. AML/CFT Programs help protect casinos and their employees from unwittingly being involved in money laundering and terrorist financing activity.

In early 2021, the landscape of the U.S. federal AML laws and regulatory framework changed, following the enactment of the Anti-Money Laundering Act (AMLA). Designed to usher in a new era of AML effectiveness, the AMLA aims to modernize the AML/CFT laws of the U.S. pursuant to the purposes of the Act, which include, as relevant:

- To improve coordination and information sharing among the agencies tasked with administering AML/CFT requirements, the agencies that examine financial institutions for compliance with those requirements, federal law enforcement agencies, national security agencies, the intelligence community, and financial institutions
- To modernize AML/CFT laws and regulations to adapt the government and private sector response to new and emerging threats
- To encourage technological innovation and the adoption of new technology by financial institutions to more effectively counter money laundering and terrorist financing
- To reinforce that financial institutions' AML/CFT policies, procedures, and controls shall be risk-based

The AMLA mandates a range of extensive congressional reports, regulatory reviews, and reforms, as well as updates to examination manuals and regulator and examiner training programs. It also mandates beneficial ownership reporting to FinCEN, although those regulatory requirements were updated in 2025 to exclude domestic entities "[c]reated

[2] In May 2024, the U.S. Department of the Treasury announced its 2024 National Strategy for Combatting Terrorist and Other Illicit Financing. The 2024 strategy outlined priorities for the AML/CFT framework, law enforcement, and technological innovation. See U.S. Department of the Treasury, 2024 National Strategy for Combatting Terrorist and Other Illicit Financing (May 2024), available at: https://home.treasury.gov/system/files/136/2024-Illicit-Finance-Strategy.pdf; U.S. Department of the Treasury, The National Money Laundering Risk Assessment 2024 (Feb. 1, 2024), available at: https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf.

by the filing of a document with a secretary of state or any similar office under the law of a State or Indian tribe," which would generally include regulated casinos and gaming entities in the U.S. It also requires that financial institutions consider National AML/CFT priorities when designing their AML/CFT Programs, as discussed further below.[4]

State Regulatory Requirements

While federal AML/CFT laws and regulations apply across all states, each state has the authority to adopt more restrictive or additional requirements. States that grant casino licenses typically impose exacting regulations on casino operations, though specific requirements vary from state to state. State regulatory specifications can include the games that can be offered (and their rules), the financial services that can be provided, and the procedures casinos must follow in providing them. State regulation also extends to the nature of the surveillance and security measures employed at casinos, and they can include audit and/or state reporting or information-sharing requirements. This guide is designed to focus on federal BSA requirements and expectations, but casinos must additionally be aware of and ensure that their AML/CFT Programs comply with any additional and/or more stringent AML requirements that are applicable to them under state laws.

EACH STATE HAS THE AUTHORITY TO ADOPT MORE RESTRICTIVE OR ADDITIONAL REQUIREMENTS

[3] These terms are used interchangeably within this guide to refer to a casino's compliance measures to adhere to the BSA and mitigate money laundering and terrorist financing risks.
[4] FinCEN, Anti-Money Laundering and Countering the Financing of Terrorism National Priorities (June 30, 2021), available at: https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf.

BSA/AML Governance

Risk-based AML compliance efforts and a strong culture of compliance are essential to the casino industry.

Board and Senior Leadership Responsibilities

Casino leadership, including its board of directors and compliance committee, holds ultimate responsibility for the casino's compliance with the BSA.

Board and senior leadership responsibilities include:

- Establishing a culture of compliance: Boards are expected to foster an organizational culture that prioritizes compliance above revenue interests.
- Overseeing the AML/CFT Program: Boards are responsible for approving and overseeing casinos' AML/CFT Program, ensuring it is effective, appropriately resourced, and independently tested.
- Designating an AML officer: Boards should appoint a qualified individual to serve as the AML Officer, responsible for day-to-day compliance with BSA requirements.
- Ensuring adequate AML/CFT compliance resources: Boards are responsible for ensuring that the AML/CFT compliance function and the AML Officer have sufficient authority, independence, and access to resources (human and technological) to ensure the AML/CFT Program is compliant, risk-based, and effective.
- Being knowledgeable about BSA/AML requirements: Board members should receive periodic AML/CFT training, in accordance with their AML/CFT Program's training schedule. The training should cover applicable BSA/AML obligations, the elements and effectiveness of their casino's AML/CFT Program, and how their BSA reports are used.

Culture of Compliance

Casino leadership should remain engaged in compliance efforts and set a tone from the top that compliance must be prioritized above revenue and other commercial interests. A culture of compliance can be established and maintained through:

- Regular communications emphasizing the importance of compliance and promoting transparency and accountability among all staff members
- New hire and ongoing compliance training
- Periodic compliance training tailored specifically to the casino's services
- Adequate resourcing, independence, and authority granted to compliance functions
- Compensation and promotion structures that incentivize compliance and disincentivize noncompliance, including compensation and bonus clawbacks or other impairment
- Effective internal reporting and investigation mechanisms and policies

Forging effective working partnerships with law enforcement agencies is another important way to nurture a culture of compliance, ensuring that employees understand how BSA-required reports are used to achieve national policy goals that may override business concerns. Such partnerships can be formal (such as hosting roundtables or forums to share information) or informal (such as maintaining a close relationship with the local Federal Bureau of Investigation (FBI) field office and sharing suspicious activity information).

Compliance with the casino's AML/CFT Program requirements and other compliance actions of individual employees should be a factor in performance reviews. These factors should be considered in calculating compensation and bonuses, and in determining any negative personnel action, from performance improvement plans through to termination of employment.

Casinos should consult with FIN 2014 A007, which discusses FinCEN expectations for for promoting a culture of compliance.[5]

[5] FinCEN, FIN-2014-A007, Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance (Aug. 11, 2014), available at: https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2014-a007.

AML Officer

As required by the BSA, at least one employee at a casino must be designated as responsible for day-to-day compliance with BSA and AML requirements, policies, and training, and should be available to other employees to consult on related questions as they arise. This individual should be fully knowledgeable of the BSA and all related regulations and independent of casino operating departments. This individual may be known as the AML Officer or have another title/duties (for the purposes of this document, the employee with day-to-day BSA/AML responsibility on the property shall be referred to as the AML Officer).

> The AML Officer should be well-versed in the casino's products, services, patron base, entities, and geographic locations, as well as the potential money laundering and terrorist financing risks associated with those factors. It is important that the AML Officer understands how BSA-required reports are used by law enforcement agencies and functions as a liaison (partner) with those agencies. The AML Officer should be the designated point of contact for any BSA/AML-related examinations, audits, and law enforcement inquiries.

In addition, to ensure that the AML Officer has the necessary independence to execute their responsibilities, they should report to the Chief Legal Officer, Chief Risk Officer, Chief Compliance Officer, or an executive of comparable stature. If applicable, property-level leadership with oversight of AML/CFT Programs should have a direct reporting line to the centralized corporate compliance department for all AML/CFT matters. All compliance-related reporting lines within the organization should be clearly delineated and identified to employees.

The corporate board of directors, compliance committee, or other relevant committee should also receive routine briefings on the AML/CFT Program and any material changes.

The AML Officer, along with the AML/CFT compliance function more broadly, should be vested with appropriate authority and resources to implement the program and assist the casino in managing risk. This means that the AML Officer should have sufficient stature in the organization to be a member of, or otherwise be able to regularly brief, senior leadership. The AML Officer should be senior enough to effectively promote the culture of compliance at all levels of the organization.

New Product/Service, M&A, and Property Reviews

Casinos should have policies and systems in place to ensure that when new products, services, properties, or M&A deals are considered, the AML/CFT compliance function is involved early in the process and has a voice in decision-making based on AML/CFT risks associated with the proposal, as further discussed in the Risk Assessment section below.

Internal Reporting Policy

Having a clear, effective, and accessible reporting mechanism for escalating compliance issues is an integral component of establishing a culture of compliance and identifying and addressing potential noncompliance. Casinos should have policies requiring personnel to report known and suspected noncompliance with casino policies and/or laws that are supported by robust anti-retaliation policies and controls. Casino personnel should feel empowered and safe to report compliance concerns, and they should be trained on the many ways in which they can make such reports. Personnel should also be encouraged to identify compliance program concerns and recommend enhancements through informal (e.g., ad hoc verbal remarks) and/or formal (e.g., employee surveys) channels.

Casinos should provide multiple avenues for reporting, which may include emailing a designated email address, speaking with a manager and/or compliance point of contact, submitting a report via a dedicated webpage, and/or calling a third-party managed hotline. As permitted by applicable laws, there should also be an ability to submit reports anonymously.

Additionally, there should be formal procedures and timelines in place for investigating reports, and, as appropriate, based on findings, implementing remedial and/or disciplinary measures.

Reports, investigations, findings, and remedial/disciplinary measures should be fully documented and maintained for at least five years.

Risk Assessment

Risk Assessment Process

The BSA requires casinos to implement risk-based internal controls, policies, and procedures. Every financial institution is potentially at risk of being used for illegal purposes or accepting proceeds from illicit activity. Casinos should identify and assess their specific money laundering risks and adopt effective measures designed to mitigate those risks.

Conducting a risk assessment should be the first step in building an AML/CFT Program.

The risk assessment process and internal controls should be clearly documented as a part of the casino's AML/CFT Program. The risk assessment process should begin by considering, at a minimum, the following questions to assess the casino's AML/CFT risks in different parts of its business:

- What are the entry and exit points at the casino for patron funds that may come from illicit sources?
- What casino departments or employees are best positioned to detect the entry and exit of such funds?
- What are the characteristics of transactions that may involve illicit funds, or of patrons who are more likely to engage in suspicious activity?
- Is the casino's geographic location high-risk for money laundering, terrorist financing, or other illicit finance activities?
- What AML/CFT compliance measures (e.g., policies, procedures, controls, testing, third-party relationships, and systems, including automation) are in place to mitigate these risks?
- How effective are those measures?

Risk assessments should be reviewed and, as appropriate, updated at least annually, and more often, as circumstances warrant, due to new or materially changed AML/CFT risk factors, such as when a new product or service is launched. They should be reviewed and approved by senior leadership.

Risk assessments should be tailored to each casino venue by identifying, evaluating, and documenting its specific risks, considering factors such as the nature and characteristics of its geographical location, enterprise, products, financial services, patrons, and intermediaries. Casinos should also look at relevant enforcement actions and regulatory guidance to identify money laundering and terrorist financing typologies that may be used to exploit their properties, products, and/or services.

The risk assessment should then identify the compliance measures that the casino has in place to mitigate each of those risks and assess the residual risks to the casino to determine whether the casino's AML/CFT measures are sufficient to adequately mitigate those risks. During these risk assessment processes, casino compliance professionals should bring to bear their judgment based on experience with casino transactions. Upon completion of a new or updated risk assessment, the compliance function should develop formal action items to be completed to reduce any insufficiently mitigated risks.

Risk Assessment

Regulatory guidance that should be considered during the risk assessment process include, among others, FinCEN's National AML/CFT Enforcement Priorities and the NMLRA.[6] The latest versions of these publications identified the following typologies, among others, as key AML/CFT threats in the U.S.:

- Corruption
- Cybercrime, including cybersecurity and virtual currency risks
- Terrorist and proliferation financing
- Fraud
- Drug trafficking activity
- Human trafficking and human smuggling
- Professional money laundering organizations

More specifically, the 2024 NMLRA highlighted specific money laundering risks impacting casinos and online gaming platforms, including:

- Criminal money laundering organizations, casino junkets, and money-mule networks using casinos to launder illicit proceeds
- Misuse of line-of-credit services to avoid currency transaction report (CTR) filings
- Misuse of private gaming salons
- Chip-walking in denominations lower than what casinos generally track (i.e., chips valued at less than $5,000)
- Foreign illicit actors engaging in intra-property transfers, wherein they deposit funds at a foreign branch of a U.S.-based casino property and then access an equivalent amount of funds at a U.S. branch of that same casino property, thereby potentially bypassing foreign currency controls and/or BSA reporting obligations
- Deposits of illicit proceeds into betting accounts and subsequently withdrawing funds after minimal gaming activity to disguise the illicit funds as gaming earnings

On an annual basis and as part of its ongoing risk assessment, the casino should review its filed suspicious activity reports (SARs) for the previous year to analyze patterns of suspicious activity. The trends may then be reviewed by the casino's AML committee, if applicable, to determine whether adjustments to the AML/CFT Program or risk assessment are warranted.

Information identified in independent assessments of a casino's AML/CFT Program should also be carefully analyzed and reviewed as part of the risk assessment process. Such assessments include evaluations of independent auditors and Internal Revenue Service examinations of the casino's AML/CFT Program. Findings from these assessments may warrant updates to a casino's risk assessment. The casino should undertake corrective actions in response to issues that arise during these independent assessments and revise its AML/CFT Program accordingly or decide that no such action is necessary. The results of these assessments should also be reported to the board.

Furthermore, as referenced above, casinos should have policies and systems in place to ensure that when new products, services, properties, or M&A deals are considered, the AML/CFT compliance function is involved early in the process and has a voice in decisioning based on BSA/AML risks associated with the proposal. Compliance should consider how the new product, service, property, or deal would impact the casino's BSA/AML risk assessment and what risk mitigation measures would be necessary to appropriately offset any intolerable increases in risk. Those considerations should factor into the casino's ultimate decisioning on whether and how to continue with the proposal.

[6] FinCEN, AML and CFT National Priorities (June 30, 2021), available at: https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf; U.S. Department of the Treasury, The National Money Laundering Risk Assessment 2024 (Feb. 1, 2024), available at: https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf. Casinos may also consider guidance identifying U.S. jurisdictions considered high-risk for certain types of illicit activity, such as High Intensity Financial Crime Areas (HIFCA) and High Intensity Drug Trafficking Areas (HIDTA). FinCEN, HIFCA regional map, available at: https://www.fincen.gov/hifca-regional-map; Office of National Drug Control Policy, HIDTA map, available at https://www.hidtaprogram.org/.

Preventive Steps for Risk Mitigation

Casinos should consider adopting policies and procedures that have the purpose of preventing patrons from attempting transactions that have a higher likelihood of money laundering, BSA violations, or other violations of law. Such policies and procedures should be tailored to the casino's specific risk factors, in accordance with the casino's risk assessment.

Some examples of preventive policies and procedures may include:

- Declining to accept a cash purchase of a casino check, monetary instrument, or initiate a wire transfer. This would not restrict the cage from issuing a check or funds transfer for documented casino winnings. Such approvals should be documented.
- Requiring ticket-in, ticket-out (TITO) redemptions at self-service kiosks to be capped at an amount below $3,000 (or an amount determined by the risk assessment) and monitoring to identify TITO redemptions of multiple tickets below that amount at the same self-service kiosk.
- Increasing surveillance at TITO machines to detect stuffing multiple low-denomination tickets to avoid CTR reporting and placing TITO machines in areas that are easily observable by staff.
- Barring cash-for-cash exchanges or only allowing them at a very low threshold, as this can be indicative of money laundering. Any cash exchanges should be consistent with the casino's risk assessment and, in rare circumstances, permit senior management to approve such exchanges above that threshold for an appropriate business purpose (e.g., foreign currency exchanges for established patrons at reasonable levels); such approvals should be documented.
- Heightened scrutiny for checks or wire transfers originating from a labor union, charitable/nonprofit organization or foundation, law firm (including from an Interest on Lawyer's Trust Account (IOLTA), accounting firm, business, third party, or any type of trust account. A casino may reject and/or reverse such checks and wire transfers and consider filing a SAR on the payment.
- Issuing casino checks and wires to a patron only for the amount of their winnings (e.g., the remaining funds from a check or wire that already has been accepted).
- A check for winnings should be payable only to the patron, and a wire transfer should be made only to the patron's account or, if applicable, to the account from which the originating wire was received. Similarly, if there is a return of front money paid by wire transfer, it should be wired back to the bank account from which the funds originated.
- To the extent casino checks and/or wires are made payable to a patron's business, another casino account, or to someone other than the patron at the patron's request, casinos must develop appropriate procedures. Procedures should require that such transactions include cage or senior management approval. Such transactions should only be allowed when the casino has been able to obtain an appropriate business purpose for the action, which is documented, and an appropriate connection is documented between the patron and the business.
- Suspending a patron's loyalty club account and/or barring the patron if the patron's activity has generated the filing of an incomplete CTR and the patron has declined to produce the required information, until the missing information is provided. Filing a SAR for the episode should also be considered. In such instances, the patron should be prohibited from further gaming and may be prohibited from the redemption of complimentaries (comps).
- Directing international branch offices of the casino to adhere to the same recordkeeping and reporting requirements under the BSA that are consistent with the laws of the jurisdiction in which the international branch office is located, as well as local law. To the extent these offices are allowed to receive cash, casinos may want to consider voluntary CTRs. The office should also be required to identify and report internally any suspicious transactions in order that SARs can be completed where required.
- Prior to travel outside the U.S., marketing executives should be trained on the laws that relate to gaming and marketing for the specific jurisdiction(s) they are visiting. If a traveling marketing executive is authorized to conduct a financial transaction in an international location, the casino may also need to report the transaction under the BSA.
- Eliminating cash play at poker tables and documenting poker chip purchases at a certain dollar threshold.

Additional Preventive Measures Specific to Online Gaming

- Requiring that accounts from which patrons deposit and withdraw funds match the name of the account holder
- Where possible, returning funds to the original payment source
- Analyzing patron activity for evidence of account sharing or attempts at evading/manipulating geolocation controls
- Monitoring patron activity for evidence of deposits and withdrawals without legitimate wagering activity
- Searching player databases for:
  - Multiple players using similar usernames and email addresses, based on geolocation data and device intelligence
  - A large number of players geolocating from a similar residential location
  - Multiple players using a shared device
- Leveraging geolocation data to detect "impossible travel" (i.e., multiple attempted transactions from jurisdictions of significant distance, which would be physically impossible and may be indicative of attempted proxy wagering or account sharing)
- Deploying device blocks in instances of repeated actions deemed to be suspicious and lacking any legitimate business purpose, aligned with an operator's risk-based approach
- Leveraging geolocation data at the time of patron funding and withdrawal to ensure funds are not being transmitted from restricted, high-risk, or sanctioned regions
- Analyzing player accounts with multiple payment methods and consecutive deposits
- Limiting the number of payment instruments that players are allowed to add (i.e., number of credit/debit cards, wallets, bank accounts, etc.)
- Limiting the total dollar amount a player can deposit or disburse from their wallets in set periods of time

Examples of High-Risk Services/ Products

GAMING VOLUME AND CHARACTER

Different gaming venues may have differing risks based on their unique product mix and patron pool. Risks may evolve over time as a venue's business model and/or patron transaction volume changes.

Because money launderers often deal with substantial amounts of money, they may be drawn to larger casinos with higher gaming activity, where large-value transactions are more frequent and less likely to draw attention.

For the same reasons, money laundering may be more likely to involve patrons bringing large amounts of money to a casino and playing games with higher dollar values. Accordingly, larger gaming venues will likely need more AML/ BSA compliance procedures than smaller casinos with lower dollar volumes.

Nevertheless, smaller volume casinos must be alert to a patron's departure from ordinary patterns of play and suspicious use of the financial services offered by the casino. Similarly, the structuring of transactions to avoid reporting requirements can occur at any casino, regardless of business volume.

RANGE OF FINANCIAL SERVICES

The broader the array of financial services available at the casino (e.g., front-money deposit accounts, markers/credit extensions, wire transfer services, check cashing, credit/debit card cash advances, and safety deposit boxes), the greater the opportunity for a money launderer to exploit several different services for illicit purposes. Casinos should strive to ensure that transactions have a legitimate gaming purpose and that other financial transactions conducted as a courtesy are prohibited or restricted to small amounts. In addition to being highly limited, such transactions should require approval by at least two individuals with an appropriate level of authority, such as the AML Officer, Cage Director, or other senior-level executive. The approval process for exceptions to the policy should be clearly documented in the casino's compliance program.

CHARACTERISTICS OF CERTAIN GAMES

The rules of certain games may increase the likelihood of money laundering. For example, if a game allows patrons to bet either side (e.g., baccarat, craps, or roulette), confederated patrons might bet both sides to launder funds through the game.

Similar risks may arise in the case of sports betting when a patron places a bet with a legally operating sportsbook on behalf of an unidentified third party, concealing the origin and owner of the funds or betting on both sides of the line.[7] In addition, race and sportsbooks may be potential targets for money launderers because confederates can bet on both sides of a game or an event, thereby offsetting their exposure.

Because poker is not a house-banked game, transactions at poker tables may occur between patrons, rather than with the casino. Accordingly, the casino may be less likely to detect potential suspicious activity because poker — unlike table games, race and sportsbook wagers, or electronic games — does not allow the casino to determine verified win/loss. If a casino does not permit cash wagering in poker rooms, the risk of money laundering may be correspondingly reduced. Nevertheless, there could be information about a poker player's source of funds or criminal associations that could raise red flags and should be escalated to Compliance.

CRYPTOCURRENCY

Cryptocurrencies use blockchain technology as a means of decentralized recordkeeping for transactions. The regulatory climate for cryptocurrency is still developing and the value of cryptocurrencies is volatile. There have been a number of cases where cryptocurrency has been involved in money laundering or other illegal activity, and its illegal use is a major government concern.

[7] See FinCEN, Correspondence with the American Gaming Association Regarding Sports Betting Conducted on Behalf of Third Parties (Dec. 24, 2014), available at: https://www.fincen.gov/resources/statutes-regulations/guidance/fincen-correspondence-american-gaming-association-regarding.

The suggested best practice is to require any virtual currency to be converted to U.S. dollars prior to use for gaming at a slot machine, table game, sportsbook, or other gaming area. By requiring virtual currency to be converted to U.S. dollars prior to usage for gaming, it will be subject to the same CTR and SAR reviews as all other cash transactions conducted within the casino.

THIRD-PARTY PAYMENTS AND SHELL COMPANIES

There has been a longstanding concern with the use of anonymous legal entities to promote money laundering and other illegal activities. These entities may be shell companies or act as unlicensed money transmitters. Contrary to popular belief, these entities are not only incorporated in offshore jurisdictions with reputations for secrecy but can also be organized under state law in the U.S. FinCEN has taken measures to address this risk. In 2018, FinCEN's Customer Due Diligence (CDD) Rule became effective, requiring banks and certain other financial institutions (excluding casinos) to obtain beneficial ownership information on legal entity customers.

Acceptance of payments for gaming or casino debt from legal entities or other third parties on behalf of patrons poses a money laundering risk for casinos. If a casino permits payments from third parties (either legal entities or persons), there should be written policies describing the types of third-party payments that are permitted and under what circumstances based on the casino's risk tolerance. For instance, casinos may restrict third-party payments to those from a business that is documented to be related to, or owned by, the patron or from relatives of the patron.

To the extent a casino allows third-party payments, the casino should understand and document the nature of the relationship between the patron and third party.

ONLINE PAYMENTS AND DIGITAL WALLETS

Online payments and digital wallets, including player account balances on online gaming platforms and cashless wagering accounts that allow cashless gaming on the casino gaming floor, can involve heightened BSA/AML risks. Digital wallets enable patrons to load cash into an account and use those funds for gaming on a casino floor or online platform, as determined by the casino operator and the functionality of the digital wallet.[8] Funding sources may include online transfers from bank accounts, credit/debit cards, deposits with a cashier within the casino, and others. Players place wagers with a mobile device or computer with access to their wagering account. The patron's identity is confirmed, and each transaction creates a digital record.

Digital wallets may be associated to a patron's player loyalty account with the casino. The best practice is to only allow accounts to be associated with one user. The casino should take reasonable precautions to ensure accounts are not shared by multiple patrons. The customer service agreement should require patrons to agree that the account is for personal use only.

> Digital wallets and online transactions, in general, can present a greater opportunity for money laundering. Bad actors can exploit these transactional methods to convert illicit funds into virtual assets (if supported) or to engage in fraudulent transactions The relative anonymity, speed, and convenience of these transactions can make suspicious activity through them more challenging for casino personnel to identify and prevent. These transactional methods may require separate or more sophisticated transaction monitoring systems and associated employee training to adequately monitor for suspicious activity. Casinos should ensure that any payment processor or digital wallet service provider also has robust BSA/AML policies and procedures, including transaction monitoring.

Since online payments are non-cash transactions, CTR requirements do not apply to them. As such, an operator should implement adequate procedures to review transactions using this payment method for suspicious activity. However, Digital wallet deposits and withdrawals in cash are still subject to CTR requirements when they occur on casino premises.

Converting deposits from one transaction type to another within the digital wallet platform should be strictly limited. Wherever possible, casinos should require the withdrawal method to match the deposit method, unless the funds have been sufficiently placed at risk. Funds deposited to a digital wallet should be confirmed to be used for a gaming purpose. A reasonable, risk-based review process should be implemented to detect patrons who frequently make deposits and withdrawals without associated gaming activity. Such instances should be considered for a SAR filing.

In addition, to mitigate BSA/AML risks that can be associated with digital wallets, the best practice is to deploy the same

[8] An important distinction is that Digital Wallets as noted here, are denominated in US dollars and the best practices in this section are not in reference to cryptocurrency which is covered in a separate section.

geolocation and KYC measures that are applicable to the online and mobile wagering environment to the cashless wagering and digital wallet environment. These measures will ensure the true identity of the patron wagering with the digital wallet and cashless payments, and ensure that the wagering funds are being deposited from an authorized jurisdiction, mitigating the risk that the wallet is being used in a fraudulent manner or as a conduit to engage in money laundering or other illicit activity.

ONLINE GAMING

Online gaming has many of the same risks associated with in-person casino gaming. Although there remains uncertainty regarding BSA coverage for certain online operators, those subject to the BSA must comply with AML Program and suspicious activity reporting requirements.

Accordingly, appropriate reviews should be put into place to detect similar types of suspicious activity. The types of suspicious activity for online gaming include, but are not limited to, minimal gaming with large transactions, structuring, and identification issues. Additionally, prior to signing up for an online gaming account, new patrons should be subject to identity verification as well as compared against the Office of Foreign Asset Control (OFAC) and Specially Designated Nationals (SDN) sanction lists. If a patron appears on one of the sanction lists, the online gaming provider should block the creation of the account.

Identity and credit card theft fraud rings may target the online gaming environment to establish fraudulent accounts with stolen identity information and fund those accounts with fraudulent payment instruments. Such fraud rings attempt to establish multiple online accounts and, if successful, typically make large deposits with minimal game play and then quickly try to withdraw those funds. Online casino and sports betting operators should establish tools to mitigate such fraud, which may include the methods described under the Preventative Steps section of this document.

HIGH-STAKES/LIMIT POKER ROOMS

High-stakes/limit poker rooms can be particularly vulnerable to illicit financial activity, which may warrant heightened BSA/AML risk mitigation measures. These rooms tend to implicate a heightened risk of collusion between players and circumvention of a casino's BSA/AML compliance controls. Another risk factor is third parties introducing illicit funds into these rooms by funding or backing patrons' gaming activity. Risk mitigation strategies may include additional surveillance and source of funds confirmation at certain monetary thresholds.

Patron Identification and Diligence

Patron Identification and Verification

Before conducting any BSA-reportable transaction or opening a front money or market limit/credit account, digital wallet, other online patron balance account, or issuing a safety deposit box for a patron, casinos must collect and verify the patron's full name, permanent address, and Social Security Number (SSN), if applicable. However, this requirement does not apply to the establishment or use of player loyalty accounts. If a patron asserts that their only permanent address is a post office box, the casino should confirm this assertion by examining available databases and acquiring the patron's attestation to this fact. In addition, as part of these identification verification processes, patrons should be required to provide a valid, current, government-issued photo identification, which may include a:

- Driver's license[9]
- Passport
- Alien registration card
- State-issued identification card (including Real IDs)[10]
- Global Entry card[11]
- Tribal identification card

These identification collection and verification procedures should apply to any transaction that would trigger a CTR requirement and requests to open a front money or market limit/credit account, digital wallet, other online patron, balance account, and safety deposit box.

A casino's AML/CFT policies and procedures may specify additional information that must be collected and verified in certain situations. For instance, casinos should request a patron's occupation, phone number, and email address prior to the patron exceeding the CTR threshold. Casinos should also consider the implementation of risk-based measures to verify such additional information. While the inability of a casino to obtain such additional information need not prevent a CTR transaction from occurring, if the nature of the patron's refusal or inability to provide the information is suspicious, it should be escalated for SAR consideration.

DOCUMENTARY REVIEW

Other than a driver's authorization card, for in-person transactions, a casino generally may rely on viewing a valid, government-issued photo identification as verification of a patron's identity; however, if a document shows obvious indications of fraud, the casino must consider that factor in determining whether it can form a reasonable belief that it knows the patron's true identity.

In some instances, information in the casino's records will suggest that certain information on the official identification document — most often the patron's permanent address — is no longer accurate. In those situations, if the casino can verify by reasonable inquiry the more recent information, it may wish to report the more recent information on any CTRs and SARs filed for that patron. Documentation supporting the verification and use of an address other than the one on the patron's government-issued ID should be maintained in the casino's records and is commonly requested by IRS examiners during a BSA examination.

If the patron is a U.S. citizen or resident, an SSN is required for certain transactions, including CTRs and taxable events. Patrons may verbally provide an SSN. In such cases, it is recommended that the patron complete a W-9 Form to attest to the validity of the SSN. If the casino knows or has reason to believe that a previous SSN provided by the patron was incorrect, then the patron may also be required to complete and sign a W-9 Form before any pending transaction can be completed. Casinos should consider filing a SAR if inconsistencies in identifying information are suspicious.

If a patron declines to provide an SSN when one is required, the casino must not complete any reportable transactions or

[9] This does not include driver authorization cards or international driver's licenses/permits, which are not an acceptable form of identification.
[10] All state-issued IDs that are compliant with the Real ID Act are sufficient for BSA reporting purposes, even those that contain the disclaimer, "Not for Federal Identification."
[11] Global Entry cards are compliant with the Real ID Act.

open an account for that patron. If the patron has exceeded the reporting threshold for a CTR without providing an SSN, a casino should attempt to acquire that information from publicly available sources. Declining to provide an SSN may warrant completion of a SAR.

More generally, if a patron is missing or refuses to provide the required information, the patron should be barred from further gaming activity until the required information is provided. Documentation of the incident should be added to the patron's account in the management system, detailing the missing information. A SAR should also be considered, as appropriate.

NON-DOCUMENTARY REVIEW[12]

In many states, casinos also offer online gambling options, including online sports betting and online casinos. Before any patron can make an online wager, they must first establish an online wagering account with the casino or sports betting operator. For some operators, such accounts may be established in person, in which case, identification information is collected and verified as described above.

However, in most cases, such accounts are established remotely through the internet, making it impossible to verify identity through in-person review of physical documentation. In such cases, operators must rely on non-documentary methods of ID verification.

Non-documentary methods require the patron to input or download personal information about themselves, which typically includes some combination of name, address, date of birth, government-issued ID number, phone number, email, and all or part of the patron's SSN. Some operators may also require the submission of a photo or scan of a government-issued photo ID, and in some circumstances, they may require uploading a selfie of the prospective patron. This information is then independently verified by comparing it against information obtained from a consumer reporting agency, public database, or other third-party electronic ID verification service. If the patron's identity cannot be reliably verified, the operator should deny the creation of an online wagering account until sufficient additional documentation is provided that can be reliably verified.

BEFORE ANY PATRON CAN MAKE AN ONLINE WAGER, THEY MUST FIRST ESTABLISH AN ONLINE WAGERING ACCOUNT WITH THE CASINO OR SPORTS BETTING OPERATOR

[12] FinCEN, FIN-2021-R001, Exceptive Relief for Casinos from Certain Customer Identification Verification Requirements (Oct. 19,2021), available at: https://www.fincen.gov/sites/default/files/2021-10/Casino%20Exceptive%20Relief%20101921_0.pdf. This relief was granted by FinCEN in response to the casino industry's request to allow verification by non-documentary means, which is not currently provided for in the BSA regulations.

Sanctions Screening

Although separate from BSA/AML requirements, casinos should ensure they are not conducting transactions with individuals and entities on the list of Specially Designated Nationals and Blocked Persons (SDN List) maintained by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) or those ordinarily residing or organizing in jurisdictions comprehensively sanctioned by OFAC.[13] Casinos should not open accounts for, or conduct transactions with, patrons who are on the SDN List or who provide addresses or are otherwise known to be ordinarily resident in comprehensively sanctioned jurisdictions.[14] In order to mitigate the risk of engaging in such activities, casinos should conduct sanctions screening of patron information it obtains in the normal course of business against the SDN List, and have controls in place to block account creation for patrons with addresses or other geolocation information indicating they reside in a comprehensively sanctioned jurisdiction.

Sanctions screening of patron information should be conducted at onboarding (or when otherwise first collected) and at regular intervals thereafter during the course of the patron relationship, in accordance with the casino's AML/CFT Program requirements. A risk-based approach to the use of "fuzzy" matching logic should be used to limit the occurrence of false positives. For online gaming platforms, these measures should include geoblocking controls for authenticated patron IP and other electronic data associated with comprehensively sanctioned jurisdictions. Geoblocking controls will further decrease the risk of proxy betting as well as heighten AML and CFT compliance.

U.S. persons are required to block property in which a blocked person has a present, future, or contingent property interest. Blocked persons include individuals on OFAC's SDN List and, at the time of publication, those ordinarily resident in Cuba. This means that if a casino has funds on account for a blocked person, it must segregate those blocked funds into a separate, interest-bearing account and file a blocking report with OFAC. Although at the time of publication, there is not a blocking obligation with respect to persons ordinarily resident in Iran, North Korea, or the Crimea, Donetsk, or Luhansk regions of Ukraine, casinos must reject any attempted transactions involving these persons and file a reject report with OFAC. In practice, this will typically mean that casinos should return any funds they receive or have on account for such patrons and file a reject report with OFAC. Casinos should also consider their SAR obligations and how they intersect with these OFAC requirements.

In addition, casinos should ensure that sanction issues are woven into the fabric of compliance, including:

- Management commitment
- Risk assessment
- Internal controls
- Testing and audit
- Training (Appropriate employees will be trained on OFAC compliance responsibilities.)[15]

Know Your Customer/ Customer Due Diligence[16]

In addition to the identification collection and verification and sanctions screening measures discussed above, casinos are expected to implement and maintain a risk-based know your customer (KYC) program that includes patron identification and due diligence procedures for patrons that present increased AML/CFT risks. These KYC reviews may be triggered based on information obtained at initial onboarding of a patron or based on information or patron activity that arises during the course of the patron relationship. Information that may trigger enhanced customer due diligence can arise from a number of sources, including publicly available data, law enforcement agencies, casino personnel, third-party service providers, and other financial institutions. It may include negative media, court filings, subpoenas, informal law enforcement inquiries, and Section 314(b) requests, among other types of data.

The casino's KYC program should identify the scenarios that would trigger a KYC review and the types of customer due diligence that should be conducted as part of those reviews, on a risk basis. These procedures should be calibrated to increase scrutiny of patron play, transactional activity, and background in situations that pose greater risk of money laundering and the use of funds that may derive from criminal activity. For patrons who do not trigger these higher risk reviews, their KYC file should be subject to a refresh at certain cadences (e.g., two years or as otherwise supported based on a casino's risk assessment).

For instance, risk-based KYC reviews should be required for the below patrons, among others. A more detailed discussion regarding certain patron risk factors is provided at the end of this chapter.

[13] U.S. persons and entities (including casinos) are prohibited from doing business with persons or entities designated by OFAC, and any assets of the designees generally must be frozen immediately.
[14] The list of comprehensively sanctioned jurisdictions is updated from time to time by OFAC. At the time of publication, these jurisdictions included Iran, Cuba, North Korea, and the Crimea, Luhansk, and Donetsk regions of Ukraine. Up-to-date information regarding OFAC's sanctions programs, including comprehensively sanctioned jurisdictions, can be found at: https://ofac.treasury.gov/sanctions-programs-and-country-information.
[15] For more information on OFAC compliance, see OFAC, A Framework for OFAC Compliance Commitments (May 2, 2019), available at: https://ofac.treasury.gov/media/16331/download?inline.
[16] The terms "customer" and "patron" are used interchangeably throughout this guide.

Patron Identification and Diligence

- High-volume patrons (those whose activity in terms of bills-in, marker play, or total play exceeds an actual and/or theoretical level determined by the casino's risk assessment).
  - Based on recent enforcement actions, casinos should determine their top aggregated cash patrons and their top aggregated gaming volume patrons from the prior calendar year to complete enhanced due diligence case files.
- High-loss patrons
- Patrons with an unexplained sudden and sustained increase in play
- Foreign nationals of jurisdictions regarded as high-risk for narcotics trafficking, human trafficking, money laundering, terrorism, or other forms of illicit finance
- Politically exposed persons (PEPs)
- Repeated SAR subjects
- Patrons conducting high-risk transactions, such as third-party payments, foreign financial transactions, and domestic wires above a certain amount, as determined by the casino's risk assessment
- Patrons with high-risk occupations, such as marijuana-related or virtual currency businesses
- Patrons who have been the subject of recent law enforcement or regulatory subpoenas or other government inquiries
- Patrons with high decline or chargeback ratios
- Patrons engaged in high-risk gaming activities
- Patrons using payment instruments with multiple state associations
- Patrons who have been the subject of a 314(b) request
- Patrons who are the subject of substantial tax liens or who have gone through recent personal bankruptcy proceedings
- Patrons with financial fiduciary obligations (e.g., trustee, accountant, attorney, or nonprofit/charity executive) that may create a risk of misappropriation or other illicit financial activity
- Patrons who recently received government stimulus or support payments
- Patrons associated with individuals or entities known to be connected with the illicit generation of funds, including unlawful gaming
- Patrons who may otherwise present an unacceptable risk of money laundering or violating the casino's AML/CFT policies

A critical component of KYC reviews is assessing a patron's source of funds and source of wealth to assess whether funds being used by the patron for gaming may derive from illegal activity or from legitimate sources. Source of funds refers to the origin of funds that a patron uses for a particular transaction or series of transactions at the casino. Assessing a patron's source of funds entails tracing that particular transaction or series of transactions back to a legitimate source, such as a bank account in the patron's name to which the patron's paychecks are deposited or a patron account at the casino that was funded by winnings from previous gaming activity at the casino. These assessments will generally entail asking the patron for information and documentation regarding their source of funds, which may include bank account records, paychecks, tax records, or credit records. Casinos should then assess whether the provided information supports the level and nature of play associated with the transactions.

Source of wealth, on the other hand, refers to the origin of a patron's overall wealth and assets. These assessments involve looking at how the patron accumulated their assets over time and whether that information supports their overall level of play at the casino. To determine a patron's source of wealth, casinos may obtain information regarding the patron's employment and salary over time, inheritance, investments, and broader gaming activity at various casinos to assess

whether that information supports the level of play at the casino during the course of the patron relationship.

Casinos may also consult public records and third-party databases to verify a patron's source of funds and/or source of wealth. Such databases may provide casinos with negative news information concerning the patron's potential criminal activity or doubtful business practices, as well as any prior criminal history. Databases that may be relevant to consult in such situations include records of court activity, such as PACER, the antifraud website maintained by the Federal Trade Commission (FTC), and commercial screening products offered by third-party vendors, though such resources are considerably more limited for persons and activity located in non-U.S. jurisdictions. Casinos may also wish to consult social media (such as LinkedIn or Facebook) or other public source information.

In addition to querying available databases, leveraging Section 314(b) information sharing with other financial institutions is a critical tool to obtain more information and reach judgments on whether the patron:

- Has sources of legal wealth or income commensurate with their gaming activity
- Has provided the casino with identification information and business-related information that can be readily confirmed

> In accordance with risk-based principles for KYC reviews, if, during the course of conducting customer due diligence on a patron, the casino learns of additional AML/CFT risk factors or red flags, further due diligence may be warranted. If a casino cannot determine a patron's source of funds or source of wealth during a KYC review, a SAR should be considered.

When conducting KYC reviews, a casino should obtain and consider all available information relating to the patron and transaction(s) at issue, including, as applicable:

- Patron gaming, identification, and diligence records (retail and interactive)
- Credit history and associated records
- Prior CTR/SAR filings
- Incident report history (surveillance/security)
- Publicly available information, including internet searches, court filings, and news articles, and information from commercial database services, such as LexisNexis and WorldCheck, that identify negative news, criminal history, sanctions hits, and/or PEPs
- Employee statements/interactions
- Hotel records
- Cyber and other technical data (e.g., geolocation, IP information, device data, etc.)
- Section 314(b) inquiries, subpoenas, and any other law enforcement, regulator, or third-party request relating to the patron
- Information from marketing personnel, including at international branches, that have interacted with the patron or may otherwise have additional information about the patron
- Information from casino operations, cage personnel, surveillance, or any other department that has interacted with the patron or otherwise observed the patron at the casino
- Surveillance data
- Information and records obtained from the patron and any third parties on the patron's behalf

As made clear in recent BSA enforcement actions, ensuring that information is shared between departments and functions, and that all available information about a patron and transaction(s) is obtained and reviewed as part of KYC reviews is integral to maintaining an adequate KYC program and suspicious activity monitoring and reporting function.

All KYC reviews must be fully documented, including identification of all records reviewed as part of the diligence. Patron files and risk ratings should be updated, as appropriate, based on new information identified and findings from KYC reviews. Casinos should additionally have procedures requiring KYC refreshes at various intervals, depending on the patron's risk.

Examples of High-Risk Patron Types

COUNTRY RISK

Some patrons may be deemed to present a higher risk if the casino learns that they are non-resident aliens or foreign nationals or residents of countries that have been identified by the U.S. as jurisdictions of concern for narcotics trafficking, human trafficking, money laundering, terrorism, or other forms of illicit finance. Casinos should also monitor if the foreign national has been has been identified by the Financial Action Task Force (FATF) as high risk requiring a call to action or as subject to increased monitoring because of deficiencies in its AML regime, or if the foreign nation has been identified by Transparency International or a similar reputable organization as having a high level of public corruption.[17]

Online operators should ensure they have implemented sufficient controls to prevent individuals located in comprehensively sanctioned locations from accessing their platform and should perform sanctions screening as part of onboarding, as further discussed above.

MONEY BROKERS

Certain countries, such as China, have capital flight restrictions (currency controls) that impose limits on the amount of funds in local currency that an individual may take out of the country during a specified time period. This restriction presents a money laundering risk to casinos. For example, Chinese law prohibits citizens from converting more than the equivalent of $50,000 in Chinese yuan into foreign currency per year. This may incentivize individuals operating within the U.S. to offer illicit cash brokerage services to Chinese nationals traveling abroad. The broker offers cash in the U.S. in exchange for a domestic transfer in the patron's home country. Money remitters outside the U.S. may offer foreign exchange services to avoid currency restrictions and could make payments to casinos by wire on behalf of casino patrons.

Casinos should be aware of this risk in relation to patrons subject to these restrictions and direct casino staff to report any activity indicative of this behavior.

PEPs

Also known as senior foreign political figures, PEPs are individuals who have been entrusted with a current or past prominent public function, and individuals who are close relatives or known close associates of such persons. PEPs and their transactions may warrant further inquiry and consideration by the casino, such as investigating their source of wealth or funds. The concern is that their source of funds for gaming could be from corrupt activities. As appropriate, casinos should identify and assess the risks of both foreign and domestic PEPs, as well as consider part-time versus full-time PEPs. A part-time PEP is someone holding a part-time position within a government role, state-owned enterprise, or a political party. Even in a part-time capacity, these individuals may still have the potential to access financial resources, making them susceptible to bribery and corruption. A part-time PEP generally has another job/business that may need to be identified and considered. A casino may need to conduct open-source research to identify PEPs, and a casino operator may opt to use a commercial service or third-party provider to do so. Online operators should perform PEP screening as part of onboarding and periodically thereafter.

INDEPENDENT AGENTS/JUNKET OPERATORS

Casinos should also be attentive to the influence and impact of third-party marketing programs and relationships (e.g., independent agents/junket operators). To the extent such entities may bring a meaningful number of patrons to a casino property, casinos should undertake a review of the marketing entities' practices and procedures and conduct appropriate due diligence on third-party marketers or firms.

MARIJUANA (CANNABIS)

Despite being legal at the state level in multiple jurisdictions, the sale and distribution of marijuana remains illegal at the federal level. It may come to a casino's attention, for instance, in a KYC due diligence review, that a patron has ties to a state-licensed and regulated marijuana (cannabis) business (e.g., is an owner or employee of the business). Since the sale and distribution of marijuana is still prohibited federally, casino compliance programs should include a policy regarding how to address patrons with ties to such marijuana-related businesses and whose source of funds for gaming may be from these businesses.

[17] State Department, Annual International Narcotics Control Strategy Report (Mar. 2025), available at: https://www.state.gov/wp-content/uploads/2025/03/2025-International-Narcotics-Control-Strategy-Volume-2-Accessible.pdf; FinCEN, Financial Action Task Force Identifies Jurisdictions with Anti-Money Laundering, Countering the Financing of Terrorism, and Counter-Proliferation Finance Deficiencies (Feb. 23, 2025), available at: https://www.fincen.gov/news/news-releases/financial-action-task-force-identifies-jurisdictions-anti-money-laundering-3.

Suspicious Activity Reporting

Suspicious Activity Reporting Requirements

The BSA requires casinos to file a SAR if the casino knows, suspects, or has reason to suspect that a transaction or attempted transaction aggregating at least $5,000:

- Involves funds derived from illegal activity
- Is intended to disguise funds or assets derived from illegal activity
- Is designed to avoid BSA reporting or recordkeeping requirements
- Involves the use of the casino to facilitate criminal activity
- Has no economic, business, or apparent lawful purpose
- Is not the sort in which the patron would normally be expected to engage, and the casino knows of no reasonable explanation for the transaction after examining the available facts

Given that the SAR rule encompasses attempted transactions, casinos must ensure that they monitor both attempted and completed transactions for potential SAR filings.

Timeline for Filing a SAR

The regulations require that a SAR be electronically filed through the BSA e-filing system no later than 30 days from the date of the initial detection of facts that constitute a basis for filing a SAR. If no suspect is identified on the date of such initial detection, a casino may delay filing a SAR for an additional 30 calendar days to identify a suspect, but in no case shall reporting be delayed more than 60 calendar days after the date of such initial detection.

The phrase "initial detection" should not be interpreted as meaning the moment a transaction is highlighted for review. There are a variety of legitimate transactions that could raise a red flag simply because they are inconsistent with a patron's account activity. The casino's automated account monitoring system or initial discovery of activity, such as system-generated reports, may flag the transaction for review; however, this should not be considered the initial detection of potential suspicious activity. Casinos should establish what they consider to be the trigger for starting the clock and apply this consistently.

Type of Filing: Continuing Activity Report

The Continuing Activity Report filing type should be utilized in a SAR if a patron is subsequently recognized as having additional or repeated suspicious activity related to, or similar to, activity that has already been reported on a SAR filing with a filing type of Initial Report. The Continuing Activity Report filing type allows the casino to monitor a patron for up to 90 days before filing an additional SAR, which can then be inclusive of all subsequent SAR activity since the date of the initial SAR. A Continuous Activity SAR has a filing deadline of 120 calendar days from the date of the last SAR filing. SARs for continuous activity may be filed earlier than the 120-day deadline if the casino believes the activity warrants earlier review by law enforcement or there is not an expectation of additional activity (e.g., patron has been trespassed).

The type of filing determination of Initial Report versus Continuing Activity Report lies in the activity of the individual(s). If the same suspicious activity has been discovered within 90 days from the initial activity, the type of filing selected would be Continuing Activity Report. If the same individual(s) are involved but in a different type of suspicious activity, the type of filing would be Initial Report (with reference to other SARs in the narrative by inclusion of associated BSA ID number).

For filings where a subject has been identified, the timeline is as follows:

Day 0: identification of suspicious activity and subject

Day 30: deadline for initial SAR filing

Day 120: end of 90-day review

Day 150: deadline for continuing activity SAR with subject information (this is 120 days from the date of the initial filing on day 30)

If the activity repeats a third time, another 90-day period is allowed before requiring the third SAR filing with the filing type of Continuing Activity Report, which would result in three SARS filed over a 12-month period. If the activity does not recur within 90 days of the previously filed SAR but occurs again after the 90-day timeframe, the next SAR would be filed with a filing type of Initial SAR but would include reference to the prior SARs in the narrative along with associated BSA ID numbers.

In appropriate cases, such as ongoing suspected illegal activity that requires immediate attention, the casino should reach out to the appropriate law enforcement agency in addition to filing a SAR.

A Continuous Activity SAR has a filing deadline of 120 calendar days from the date of the last SAR filing.

Suspicious Activity Monitoring and Reporting Procedures

Suspicious activity monitoring and reporting policies and procedures should include a variety of potential suspicious activity examples for team member awareness and should be covered in department-specific ongoing training. Compliance should be monitoring industry and BSA/AML regulatory and enforcement news for awareness and to implement risk mitigation measures as needed to minimize exposure.

Casinos should consult with FinCEN's guidance in FIN-2008-G007, which discusses red flags for suspicious activity at casinos.[18] Casinos also should develop their own lists of red flags based on information from law enforcement, the casino's own experience, recent enforcement actions, and criminal cases involving money laundering, as well as BSA violations and other criminal activity involving casinos and their patrons. The list should be updated as needed and included in training. Additionally, casinos should routinely engage with law enforcement to obtain a clear understanding of evolving criminal trends and typologies/relevant risks.

Casinos must ensure they have a holistic view of patron behavior across business lines and all gaming verticals. Casinos must also have information sharing systems in place to ensure that potentially suspicious activity typically identified and investigated by other departments, such as fraud and security, flows to Compliance for SAR filing consideration. Casinos, particularly online platforms, may want to consider having discrete SAR monitoring and reporting procedures specifically for fraud and cyber-events. Casinos should also consider the extent to which it may be appropriate to leverage information across the entire enterprise in investigating and reporting suspicious activity, including attempted suspicious transactions.

In examining SAR procedures, the casino's review should consider the following components for a complete SAR compliance effort:

INTERNAL ESCALATIONS OF SUSPICIOUS ACTIVITY

Casinos should incorporate a clear, easy to understand, and prompt internal escalation process for potentially suspicious activity that is reinforced in BSA/AML training and compliance communications. The process should include the reporting individual providing all available information about the transaction(s) or action(s) (e.g., patron name, SSN, player's card number, and observed suspicious activity with any supporting documentation) without alerting the patron that their activity has been reported as potentially suspicious.

Communication with other departments, such as surveillance, fraud, and marketing personnel, is crucial in ensuring all information is captured surrounding the activity. Each department involved should be providing their account of the potentially suspicious activity to allow the individual responsible for investigating the activity for a potential SAR filing to have a complete picture.

> Casinos should refrain from naming these internal escalations as SARs to avoid unintentional disclosure by employees. A SAR is the final document filed with FinCEN and only those making the final determination will know of the actual filing; whereas these internal notifications are simply the first step in the investigation process.

TRANSACTION MONITORING AND DATA MINING

Transaction monitoring provides comprehensive and consistent risk-based observation of patron transactions, activity, and behavior, enabling the casino to better detect and report suspicious activity. Transaction monitoring scenarios should be developed based on a casino's risk profile, with specific thresholds related to gaming activity that will generate suspicious activity alerts when those thresholds are triggered. A dedicated compliance team should complete a review of those transactions alerted at or above thresholds, reviewing all patron information available as discussed further below.

As highlighted in recent BSA enforcement actions, transaction monitoring scenarios should be regularly reviewed, tested, and updated as appropriate to ensure they remain risk-based, effective, and comprehensive, covering all of the casino's products and services, and appropriately tailored to the casino's specific risk factors and general high-risk typologies. Transaction monitoring should also be supported by automated technology that is appropriately validated, tested, and updated to ensure its continued effectiveness and efficiency. Casinos are increasingly incorporating artificial intelligence technology to enhance their suspicious activity monitoring programs by, for instance, enabling predictive analytics to identify aberrant or otherwise potentially suspicious patron and transaction activity in real-time and improving efficiencies through automation.

Behaviors or practices considered to be red flags for

[18] FinCEN, Recognizing Suspicious Activity – Red Flags for Casinos and Card Clubs (July 31, 2008), available at: https://www.fincen.gov/resources/advisories/fincen-guidance-fin-2008-g007.

potential suspicious activity may be entirely legitimate, but casinos should be attentive to the risk that they are not. Given that licit and illicit activity may look the same to the casino's compliance team, application of data analytics and technology should be considered, as these resources may help identify certain specific types of illicit activity, such as bill stuffing in slot machines, minimal gaming, chip walking, front money deposits in cash, large cash buy-ins and/or redemptions to avoid reporting, and revolving markers.

BRICK-AND-MORTAR TRANSACTION MONITORING

Unusual patterns of patron behavior on the gambling floor that may suggest a risk of money laundering or other illicit activity may include:

- Patrons with large cash-in transactions with no cash-out transactions and/or little or no gaming, which cannot be reasonably explained through transaction review
- Patrons with large cash-out transactions with limited cash-in transactions, which cannot be reasonably explained through transaction review
- Patrons that deposit money into their account and immediately request a withdrawal (of the same or similar amount)
- Patrons with large cash-out transactions (in the aggregate) with little or no CTR out filings
- Patrons with large chip-outs with limited redemptions or table buy-ins with chips
- Patrons with large check cashing transactions and/or credit card advances with limited play
- Patrons who unexpectedly use multiple sources or multiple destinations for funds or abruptly change the methods used for bringing money into or out of the casino
- Patrons with significant increases in betting or financial transaction activity without explanation
- Patrons with cash transactions, such as deposits or withdrawals, including aggregated transactions, that are just below the CTR reporting threshold
- Patrons using wagering kiosks for multiple small wagers on the same event
- Un-carded or unrated patrons with large redemptions and jackpot winnings
- Un-carded or unrated patrons with large, aggregated slot buy-ins with redemptions equaling the buy-ins
- Several redeemed gaming vouchers (i.e., TITO), in a short period of time, at the same (or adjacent) redemption kiosk not associated with a player's card account
- Checks or wire transfers received for the benefit of a patron (or multiple patrons) from third parties whose connection to the patron is suspect or unclear (or if the maker of the check or initiator of the wire transfer is high risk, such as the holder of an IOLTA account or a PEP)
- Multiple apparently structured transactions over a period of time with the apparent purpose of avoiding BSA reporting requirements, such as transactions under reporting thresholds, with or without using an agent, or around the business day
- A single payment received by the casino (e.g., negotiable instrument or wire transfer) for the benefit of multiple patrons if the casino cannot determine a relationship or business association between the source of the payment and the beneficiaries
- Patron accounts with large account balances that remain dormant or inactive for an extended period of time
- Patrons who pass winning tickets to others to cash out
- Patrons who request multiple monetary instruments for a jackpot or wager win
- Patrons who wager on both sides of a transaction in ways that are not explainable as hedging
- Patrons who demonstrate no concern for the tax consequences of uncarded play, which may generate large documented income that is not offset by losses
- Patrons who appear to be coordinating their gaming with another patron or patrons (e.g., passing chips or cash back and forth) to evade notice

To maximize incentives (comps, promotional chips, airfare, discounts, and allowances), a player, or group of players working in concert, may often display a number of suspicious behaviors (e.g., passing chips, offsetting wagers, masking their activity, distorting their average wager, or walking with chips). For commercial reasons, casinos may work aggressively to curtail these behaviors with the help of surveillance, operations, and casino marketing. Casinos should exercise caution in assuming these behaviors are simple advantage play strategies that may not be illegal

and remain attentive to the risk that these same behaviors may be employed for money laundering purposes. In some cases, this behavior should be escalated to Compliance as potentially suspicious activity.

Compliance personnel can take additional measures to review the potentially suspicious activity, such as reviewing relevant daily audit summaries, logs, and reports, including marker summaries, front-money/safekeeping summaries, multiple transaction logs (MTLs), negotiable instrument logs (NILs), check logs, and wire reports. Third-party transaction summaries should be requested and reviewed when working in partnership with a financial service offered by third parties, such as credit card cash access companies or check guaranty services. When reviewing transactions that cannot be explained through summaries and reports, a secondary review using surveillance should also be considered, if available.

As discussed above, apart from a patron's activity at the casino, a casino may learn about red flags for potential suspicious activity from third-party sources during the course of a patron relationship. Those third-party sources might include negative media, court filings, law enforcement, and/or other financial institutions. Casinos should also consistently evaluate relevant subpoenas that are received, especially those associated with financial crimes. While receipt of a criminal subpoena generally will be a trigger for a KYC or SAR review, receipt of a subpoena alone does not require filing of a SAR, unless one of the SAR triggers is satisfied.

When red flags are identified during the course of a patron relationship, casinos may wish to review any previous transactions with the patron that may appear suspicious in light of the new information and consider whether a SAR is warranted.

ONLINE TRANSACTION MONITORING

As the gaming industry expands from traditional brick-and-mortar casinos into the online space with interactive slots, table games, peer-to-peer games, and sports wagering, potential money laundering risk factors are also expanding. To keep pace with these activities, compliance personnel should have adequate research capabilities to focus on where transactions originate, how transactions are sent, and the true identity of the people involved.

Unusual activity in the online gaming space that may suggest a risk of money laundering or other illicit activity may include:

- Online cash or digital wallet deposits with minimal or no play followed by a withdrawal request(s)
- Cash deposits and withdrawals from a patron's online account or digital wallet at a casino cage that appear to be intended to circumvent CTR recordkeeping requirements
- Excessive deposits (based on risk) made from different bank accounts, payment processors, or prepaid access cards
- Deposits originating from one payment method but withdrawing to a different payment method that is not registered to the igaming account (does not apply to credit card deposits)
- Numerous deposits and/or declined deposits from multiple payment processors or prepaid access cards in a short amount of time
- Withdrawal requests to multiple bank accounts or payment processors
- A player account that is accessed using a universally unique identifier (UUID) from multiple devices and/or IP addresses
- Multiple user accounts using a UUID on the same device and/or IP address
- Geolocation reports identifying individuals who have violated multiple anti-fraud checks, such as running fake GPS apps along with having mock location settings enabled or using other spoofing methods
- Repeated deposit and withdrawal requests attempted from outside the authorized state (as detected through geolocation in states where this is prohibited)
- Player account access and wagering attempts from outside the authorized state (as detected through geolocation)
- Attempts to make cash deposits and withdrawals from a player account at a casino cage with conflicting or counterfeit identification

Suspicious Activity Reporting

SAR INVESTIGATION PROCESS

It is important to maintain a consistent approach to the decision-making around SAR investigations and filings, and to ensure such decisions are aligned with the casino's risk profile. Accordingly, casinos should have a documented procedure for how potentially suspicious activity is investigated and decisioned. In addition, it is vital to memorialize those investigations and decisions (including cases in which the casino decides not to file a SAR).

An SAR investigation consists of examining all available information to determine whether a SAR should be filed for an escalated or alerted incident(s). The reviews may be prompted by direct observations by employees, system alerts, after-the-fact data analysis performed through back-of-house procedures, or other means (e.g., incoming law enforcement inquiry, 314(b) requests, or public negative news).

The AML Officer and/or staff should begin their investigation promptly upon receipt of the internal notification. In doing so, the compliance team should request additional patron data held by relevant casino departments and functions, including but not limited to marketing, to facilitate a proper investigation that includes all available information across the casino relating to the patron and transaction. As made clear in recent BSA enforcement actions, ensuring that information is shared between departments, and that functions and all available information about the patron and transaction is obtained and reviewed by investigators is integral to performing adequate investigative analyses on potentially suspicious activity. Investigators should review and consider, as applicable, the same types of patron records discussed in the preceding section for KYC reviews, all available and relevant transactional records, and any prior KYC reviews conducted on the patron. If a casino does not already have source of funds or source of wealth information for the patron or an update to such information is warranted, the casino should have procedures for collecting the information and considering it as part of the SAR investigation process.

The purpose of the investigation is to gather a complete profile of the individual(s) to understand any possible logical purpose for the transaction(s)/action(s) and whether there is, in fact, suspicious activity occurring. Accordingly, as warranted by the nature of the investigation, the compliance team may find it necessary to gather and review additional patron information to understand the patron's behavior and transactions at issue and make SAR filing decisions or, if relevant, recommendations to restrict or terminate a patron relationship.

Regardless of the final determination of whether to file a SAR, SAR investigations should be fully documented, and all investigation materials should be retained for a period of at least five years. Even if records are housed in other systems within the casino, those utilized for the investigation should be saved in a separate location pursuant to the individual investigation.

DECISION TO FILE OR NOT FILE

Based on the investigation findings, the AML Officer/designee will determine if the information warrants a SAR being filed. It may be determined that there is a reasonable, non-suspicious explanation for the transaction(s)/action(s) and that no SAR should be filed. In the event such a determination is made, the reasoning for that decision must be documented and retained. In either event, the designated individual should make a record of the determination and the date the determination was made.

AML Officers should either be responsible for reviewing and making SAR filing decisions or have full autonomy to approve or overrule those decisions. Anyone with a direct conflict (e.g., operations, marketing, and finance personnel) should not have decision-making authority for these determinations.

COMPLETING/FILING A SAR

The individual responsible for completing a SAR should ensure that the form is completed correctly and thoroughly utilizing all available information. To the extent a casino has the data, optional data fields should be completed, particularly including, email addresses, phone numbers, and occupation. The narrative should clearly and concisely identify the essential elements of the suspicious activity answering the who, what, where, when, and why of the situation being reported. Filers should ensure that all information in the narrative aligns with the other sections of the form, such as dates, amounts involved, and the reported suspicious activity type(s).

FinCEN has issued guidance directing financial institutions to include specific terms within SAR narratives (and/or other SAR fields) for certain types of reported activity. Filers should be familiar with that guidance and ensure those terms are appropriately included on SARs involving those typologies. FinCEN maintains a list of those guidance documents and key terms on its website.

Casinos should refrain from using the SAR subject's name within the filing title of the report to avoid potential disclosure of the individual's identity.

A secondary review of the drafted SAR is recommended prior to filing. Individuals responsible for completing and reviewing SARs should receive training on writing quality SAR narratives.

In general, SAR information should be shared within a casino, and as permitted, across a corporate enterprise, only on a need-to-know basis.

SAR Confidentiality

Casinos must establish controls for maintaining the confidentiality of SARs and any information that reveals that a SAR was filed or not filed or even considered to be filed. Care must be taken to ensure that no person involved in the transaction is tipped-off that a SAR has been filed or may be filed.

SARs and information regarding whether or not a SAR was filed can be shared with federal, state, and local law enforcement and generally with a casino's gaming regulators. However, under 31 C.F.R § 1021.320(e)(1)(ii)(A)(1), a casino may share a SAR with a state or tribal authority only if that agency or authority examines the casino or requires the casino to comply with the BSA. A casino is not permitted to share a SAR with other regulatory authorities that do not have express BSA oversight authority over the casino. Casinos should have procedures in place to verify that a requestor of information of this nature, in fact, has the authority to receive it. If there is any doubt, the gaming regulator should be asked to request the information from FinCEN. Best practice is to require that all SAR requests be in writing.

Any casino, and any director, officer, employee, or agent of any casino that is subpoenaed or otherwise requested to disclose a SAR or any information that would reveal the existence of a SAR, must decline to produce the SAR or such information, citing 31 C.F.R. § 1021.320(e)(1)(i) and 31 U.S.C. §5318(g)(2)(A)(i), and must notify FinCEN of the request and response.

SAR Sharing

In general, SAR information should be shared within a casino, and as permitted, across a corporate enterprise, only on a need-to-know basis. Other personnel should not have access to databases or records containing SAR information. While third-party service providers may be utilized to assist in SAR monitoring and investigation efforts, as a best practice, they should generally not be involved in SAR decision-making or reporting, nor have access to SARs and information relating to whether a SAR was or was not filed. To the extent such sharing is permitted, it should only be on a strictly need-to-know basis based on the services they provide to the casino and supported by clear and robust contract terms, security systems, and processes to protect against unauthorized disclosures, further sharing by the third party, and data breaches that may compromise the confidentiality of the SAR information.

According to FinCEN guidance, under the BSA and its implementing regulations, a casino that has filed a SAR may share the SAR, or any information that would reveal the existence of the SAR, with each office or other place of business located within the U.S. of either the casino itself, a U.S. parent of the casino, or a U.S. affiliate subject to SAR reporting obligations under the BSA.[19] Casinos may not share SARs or SAR information with foreign parents, affiliates, or offices, nor with U.S. affiliates that do not have BSA SAR obligations. In addition to having a documented policy and process for permissible SAR sharing within a corporate organization, casinos should also have protocols and systems in place to maintain the confidentiality of shared SAR information and restrict further sharing of the information by the recipient.

In order to assist law enforcement and safeguard the confidential and sensitive information contained in and that support SARs, casinos should establish a protocol for receiving and responding to authorized requests for SAR supporting documentation without a subpoena. The protocol should address how the casino will respond to subpoenas requesting SARs, and requests for SARs by individuals and agencies not authorized to receive SARs.

[19] See FinCEN, FIN- 2017-G001, Sharing Suspicious Activity Reports with U.S. Parents and Affiliates of Casinos (Jan. 4, 2017), available at: https://www.fincen.gov/resources/statutes-regulations/guidance/sharing-suspicious-activity-reports-us-parents-and.

High-Risk Suspicious Activity Typologies

The following categories are examples of potentially suspicious situations that often will prompt consideration of whether a SAR should be filed under the casino's risk assessment criteria.

GAMING FLOOR ACTIVITY

- Minimal gaming despite large financial transactions with the casino
- Structuring of transactions to stay at or slightly below the $10,000 reporting threshold for CTRs
- Placing currency in a slot machine, then cashing out after minimal or no play and redeeming the TITO ticket at a kiosk on the gaming floor (bill stuffing)
- A transaction that has no apparent economic, business, or lawful purpose (e.g., confederated gamblers placing offsetting bets on red and black on a roulette wheel)
- Patrons passing a large quantity of chips, cash, or TITO tickets between themselves, in an apparent effort to conceal the ownership of the chips, cash, or TITO tickets (although if patrons are closely related, such activity may not be suspicious)
- A patron's gaming activity dramatically increases with no known substantiation for the source of those funds
- A patron uses another patron's player card to disguise their identity and/or evade reporting requirements
- A patron leaves the casino floor with a significant amount of chips without offsetting chip redemptions or chip buy-ins at another table, and there is no known disposition or whereabouts of the chips (although this may not be deemed suspicious if there is a reasonable, experience-based expectation that the patron will return to the casino in the near future)
- A patron that accesses a safety deposit box at the casino with a frequency that is disproportionately high when compared to the time and frequency of their play
- A patron identified as a loan shark is observed approaching patron(s)
- A patron requests large amounts of cash from an ATM but has no gaming activity

RACE AND SPORTSBOOK ACTIVITY

- Inquiring with race and sportsbook staff about reporting and identification thresholds either before or after a wager and possibly adjusting wagering activity to fall below the applicable thresholds
- At a racing venue, inserting cash into a tote machine, cashing out for vouchers and then cashing vouchers at a teller's station with little or no wagering
- Structuring wagers across multiple tickets/locations so the payout of each ticket is under the reportable identification thresholds, but in the aggregate, would have exceeded the thresholds
- Behavior that may be indicative of coordinated betting (or betting on both sides of a game or an event)
- Indications of insufficient wealth or income to support betting patterns
- Significant changes in wagering patterns or unusual spikes in play that are unexpected or unreasonable
- A patron misrepresenting themselves by presenting false or multiple identities or providing inconsistent SSNs on completed W-9s
- Presenting a large amount of money in an unusual volume of small denominations ($1, $5, $10, and $20)
- Placing a bet on both sides of the line
- Information indicating that a patron may be betting on behalf of an unknown third party
- Ticket redemption by an individual that is not known to have placed the initial bet

INTERACTIVE GAMING ACTIVITY

- Multiple gaming accounts being set-up from the same device, IP address, or physical address
- Unusual wagering activity that appears to lack any legitimate economic purpose
- Significant changes in wagering patterns or unusual spikes in play that cannot be readily explained

- Deposits and withdrawals into an online account without sufficient play to account for such activity
- Unusual patron behaviors based on geolocation data, such as traveling between jurisdictions in a relatively short period of time or multiple attempts to anonymize geolocation data
- Deposit(s) to a gaming account that are determined to be from stolen credit, debit, or pre-paid access cards

CAGE-FOCUSED ACTIVITY

- Presenting a third-party check or wire transfer — whether apparently deriving from a business or an individual — for payment of markers or for use in gambling-related activity in an amount at or above a threshold determined by the risk assessment for that casino
  - In such situations, the casino should ascertain whether the beneficiary (patron) has a documented connection to the sender (e.g., spouse or immediate family member or business), either in the casino's records or by means of a database search or other reasonable inquiry. If no appropriate connection can be established between the source of the funds and the patron, those employees responsible for deciding whether to file a SAR also may consider whether or not to proceed with the transaction.
- A negotiable instrument or wire transfer is presented for the benefit of multiple patrons, or multiple patrons engage in play on a single patron account
- A negotiable instrument or wire transfer is presented for the benefit of an individual and originates from a law firm account, or is from a charitable/nonprofit organization or foundation, another type of trust or labor union account
- A patron refuses to provide required information for the completion of a CTR or identifying information
- A patron from a country with currency controls (e.g., China) has significant cash-in transactions
- A patron deposits funds into a front money account or receives a wire transfer, does not play a substantial amount of the funds, then requests a withdrawal or wire out
- A patron deposits large sums of cash into a front money account and their known occupation is not a cash-intensive business
- A patron requests information about how to avoid BSA reporting requirements
- A patron requests establishment of an AKA account in a name other than the one by which the casino knows the patron
- A patron attempts to deposit front money or make payments using complex means, such as multiple sources of funds or multiple methods of transmission, which could mask the true source of the funds transmitted
- A patron presents funds that the casino has a basis for suspecting to be the proceeds of illegal activity
- A patron requests a cash advance from a credit card that has been identified as possibly fraudulent
- A patron uses multiple credit cards to request cash advances
- A patron is observed requesting large amounts of cash from an ATM but has no gaming activity
- A patron presents funds in any form that derive from a foreign jurisdiction declared by the U.S. government to be a jurisdiction of concern for narcotics trafficking, human trafficking, money laundering, terrorism, or other illicit activity; or if the foreign jurisdiction has been identified as high risk or subject to increased monitoring by the Financial Action Task Force; or by Transparency International or similar reputable organization as a country with a high degree of public corruption[20]
- A patron provides a wire transfer, cashier's check, or other form of payment and such instrument reflects that the transaction is being made for a purpose other than gaming
- A patron presents chips for cashing and there is little or no gaming activity recorded for the patron in the casino's system to establish the source of the chips

INFORMATION FROM BACK OF THE HOUSE

- Law enforcement or regulatory agencies deliver to the casino a formal request for records concerning the patron
- News articles or other media reports allege acts of financial wrongdoing or other illegal conduct by the patron

[20] See State Department, Annual International Narcotics Control Strategy Report (Mar. 2025), available at: https://www.state.gov/wp-content/uploads/2025/03/2025-International-Narcotics-Control-Strategy-Volume-2-Accessible.pdf; FinCEN, Financial Action Task Force Identifies Jurisdictions with Anti-Money Laundering, Countering the Financing of Terrorism, and Counter-Proliferation Finance Deficiencies (Feb. 23, 2025), available at: https://www.fincen.gov/news/news-releases/financial-action-task-force-identifies-jurisdictions-anti-money-laundering-3.

- A patron is the owner of a business, the nature of which has been profiled by the FTC as high risk for fraud schemes
- A patron is an owner, employee, or otherwise associated with a marijuana-related business
- A patron raises their financial transactions to levels well above the ordinary levels for that patron with no reasonable explanation
- An external actor attempts to compromise or gain unauthorized electronic access to the casino's electronic systems, services, resources, or information in pursuit of illegal activities[21]

This list is by no means exhaustive; other patron activities may trigger BSA/AML concerns due to the circumstances in which they arise. Each casino should develop its own scenarios tailored to its business.

Further, the SAR requirement encompasses suspicious activity conducted by employees/insiders. Therefore, casinos should have adequate communication lines between the group(s) responsible for employee-related investigations and disciplinary issues, and the team(s) responsible for filing SARs to ensure detection of potential collusion between an employee and patron to circumvent internal policies or ordinary practices, or an employee's violation of casino policies and procedures. In addition to filing SARs, casinos should be aware of and comply with state reporting requirements for insider abuse activity, as applicable.

[21] FinCEN, FIN-2016-A005, Advisory to Financial Institutions on Cyber – Events and Cyber – Enabled Crime (Oct. 25, 2016), available at: https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf.

FinCEN Suspicious Activity Report (Form 111)

EXHIBIT 1: FILINGS BY YEAR & MONTH FROM CASINO/CARD CLUB INDUSTRY*

January 1, 2014 through December 31, 2024

MONTH	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
January	3,223	4,219	4,366	4,515	4,924	4,633	4,519	3,653	5,422	5,186	5,840
February	2,950	3,757	4,485	4,629	4,047	3,889	4,418	4,029	4,603	5,192	4,666
March	3,222	3,774	5,269	6,303	4,694	4,710	4,067	4,286	5,833	5,690	6,061
April	3,239	4,099	5,093	5,238	4,556	4,605	1,024	4,195	5,067	4,903	5,692
May	3,501	4,110	4,358	5,156	4,700	4,753	352	4,269	5,163	5,741	5,292
June	3,438	4,201	4,662	4,952	4,436	3,886	1,298	4,609	5,254	5,313	5,140
July	4,415	4,376	4,910	4,440	4,476	4,285	3,659	4,982	4,866	4,887	5,373
August	4,663	3,986	5,607	5,257	4,517	4,138	3,697	4,742	5,546	5,735	5,521
September	3,999	4,447	5,130	4,875	4,195	4,240	4,067	5,139	5,064	5,024	5,106
October	4,327	4,348	4,379	4,705	4,361	4,173	4,360	4,682	5,119	4,939	6,155
November	3,917	3,844	4,587	4,391	4,469	3,949	3,914	5,045	5,099	4,747	4,952
December	4,291	4,398	4,472	4,706	4,216	4,038	4,105	5,306	4,966	5,124	5,297
Subtotal	**45,185**	**49,559**	**57,318**	**59,167**	**53,591**	**51,299**	**39,480**	**54,937**	**62,002**	**62,481**	**65,095**
Total Filings	**600,114**										

* Statistics generated for this report were based on the Bank Secrecy Act Identification Number (BSA ID) of each record within the Suspicious Activity Report (SAR) system. The BSA ID is a unique number assigned to each SAR submitted. Numeric discrepancies between the total number of filings and the combined number of filings of states and/or territories are a result of multiple locations listed on one or more SARs.
Note: Statistical data for SARs is continuously updated as information is processed. For this reason, there may be minor discrepancies between the statistical figures contained in the various portions of this report.

Restricting and Terminating Patron Relationships

Restricting and Terminating Patron Relationships

Based on information obtained regarding a patron, a casino may consider whether to terminate or restrict its relationship with the patron. There should be a documented process for making these decisions that addresses, at a minimum:

- When and how patron relationships should be escalated to be considered for restriction or termination
- Who is responsible for reviewing and making restriction/termination decisions (typically, the AML Officer)
- What factors will be considered when making restriction/termination decisions
- Timing for reviewing and decisioning a restriction/termination escalation
- Any procedures to appeal, rereview, or overrule restriction/termination decisions
- A requirement that restriction/termination escalations and decisions, including reasoning, are fully documented and maintained for at least five years after the patron relationship ends

AML Officers should either be responsible for reviewing and making restriction/termination decisions or have full autonomy to approve or overrule those decisions. Anyone with a direct conflict (e.g., operations, marketing, and finance personnel) should not have decision-making authority for these determinations.

The following are examples of factors that may trigger a review of a patron relationship for potential termination or restriction or otherwise be considered when making patron termination and restriction decisions:

- Multiple SAR filings on the same patron
- Severity and recency of alleged criminal activity (e.g., terrorist financing)
- Suspected versus confirmed criminal activity
- Use of all available information
- Indication that the patron has an illegal source of funds for gaming or is using the casino for an illegal purpose
- Risk to the casino if the patron is not excluded

While multiple SAR filings on the same patron is one factor as to whether a relationship should be terminated, other factors, such as the severity of the conduct, should also be considered. Consequently, one SAR filing may be sufficient to terminate the relationship with a patron if the patron has an illegal source of funds or is using the casino for an illegal purpose. The assessment should consider whether the activity prompting the SAR is merely suspicious or known criminal conduct, with the understanding that decisions on restrictions or terminations may still be warranted based on suspected but not confirmed activity, depending on the facts and circumstance. The greater the likelihood of known criminal activity, the greater the risk to the casino if the relationship is not terminated. As noted, the assessment process should be documented in the casino's policies and procedures for performance consistency, along with a list of factors that would require the assessment to occur.

Termination of a patron relationship will be warranted if the patron's activities present an actual or unacceptable risk of violation of federal or state law or regulation, the casino's compliance policies, or pose significant concerns that a patron's source of funds used for gaming stems from illegal activity or that a patron is using the casino to facilitate illegal activity. AML bans should be enforced across the entirety of a corporate enterprise's properties and gaming platforms.

Law enforcement may utilize a specific request to "keep open" accounts and/or request casinos to maintain patron relations as part of their investigative efforts to identify and combat money laundering, terrorist financing, and other illicit financial activities. Law enforcement "keep open" requests to the casino should be in writing and detail that the law enforcement agency is requesting the casino to maintain the account, as well as include the purpose and duration of the request. The BSA includes a safe harbor that protects financial institutions, including casinos, that comply with such a keep open request from liability and adverse supervisory action under the BSA for maintaining the account or transaction consistent with the parameters and timing of the request.[22]

While casinos generally will endeavor to accommodate keep open requests, casinos are not obligated to agree to do so. The decision to maintain a patron relationship, keep open accounts, and/or terminate a patron relationship is ultimately up to the casino, based on its risk tolerance. Record retention policies should address how long the casino will maintain the request, including after the request duration period has expired.

Casinos are still required to comply with all applicable BSA requirements even when the casino agrees to "keep open" the account/patron relationship as requested from law enforcement, including suspicious activity monitoring and reporting requirements.

[22] 31 U.S.C. 5333.

Currency Reporting Requirements

Currency Transaction Reports

Casinos are required to currency transactions reports (CTRs) on each transaction in currency involving cash-in or cash-out of more than $10,000.

Transactions in currency involving cash-in include, but are not limited to:

- Purchases of chips, tokens, and other gaming instruments
- Front money and digital wallet cash deposits
- Safekeeping deposits
- Payments on any form of credit, including markers and counter checks
- Bets of currency, including money plays
- Currency received by a casino for transmittal of funds through wire transfer for a patron
- Purchases of a casino check
- Exchanges of currency for currency, including foreign currency

Transactions in currency involving cash-out include, but are not limited to:

- Redemptions of chips, tokens, and other gaming instruments
- Front money and digital wallet currency withdrawals
- Safekeeping withdrawals
- Advances on any form of credit, including markers and counter checks
- Payments on bets
- Payments by a casino to a patron based on receipt of funds through wire transfer for credit to a patron
- Cashing of checks or other negotiable instruments
- Exchanges of currency for currency, including foreign currency
- Travel and complimentary expenses and gaming incentives
- Payments for tournaments, contests, or other promotions

Multiple currency transactions must be treated as a single transaction if the casino knows they are by or on behalf of the same person and result in either cash-in or cash-out totaling more than $10,000 during any gaming day. A casino is considered to have such knowledge if any director, partner, or personnel, acting within the scope of their employment, knows that multiple currency transactions have occurred from reviewing available information. Transactions in and out do not offset each other for reporting purposes. In addition, transactions in and out are separately aggregated but can be reported on a single CTR form for the same gaming day.

Before concluding any transaction for which a CTR must be filed, casinos must collect and verify the patron's identity using the ID&V processes, as discussed above. Casinos should have processes and systems in place to ensure that they are properly tracking and aggregating transactions using all available transaction data sources to enable them to identify when a CTR will need to be filed and to either verify that ID&V information for the patron is already on file or, if not, complete ID&V processes prior to conducting the transaction that would trigger the reporting requirement. If the transaction is being performed for or on behalf of someone other than the person engaging in the transaction, ID&V should be performed for both individuals.

Casinos must file a CTR within 15 calendar days following the day the reportable transaction occurs, and they should be maintained for at least five years.

Currency or Monetary Instrument Reports

Casinos must file CMIRs if they transport, mail, ship, or has someone else transport, mail, or ship currency or monetary instruments in excess of $10,000 into or out of the country or receives such items into the U.S. from abroad. A CMIR is filed with the Bureau of Customs and Border Protection. Casinos should have processes and controls in place to ensure they properly file CMIRs whenever engaging in such activity. Alternatively, if a casino has policies against engaging in such activity, it should be documented in the AML/CFT Program and reinforced by controls, as appropriate.

8300

All U.S. trades and businesses — that are not subject to the BSA's CTR reporting requirements — must file 8300 reports for currency transactions aggregating over $10,000 that they receive from or on behalf of a person within a 24-hour period, or in related transactions over a rolling 12-month period. Currency for purposes of this reporting requirement includes cash, and for certain transactions — including those involving retail sales of entertainment or travel — a cashier's check, traveler's check, or money order in an amount less than $10,000.

Casino enterprises should have, as part of their AML/CFT Program, 8300 reporting procedures and controls for their non-gaming businesses (e.g., hotels, live entertainment, catering, restaurants, and shops). Similarly, any gaming or sports betting entities that are not BSA-regulated financial institutions subject to CTR requirements should have procedures and controls designed to ensure their compliance with 8300 reporting requirements.

Information Sharing

Information Sharing Across an Enterprise

As discussed above, it is imperative that casinos have effective and easily accessible information-sharing mechanisms across their various departments, business lines, and verticals. This is necessary to enable Compliance to have and consider all available information relating to patrons and transactions, as required to comply with BSA suspicious activity monitoring and reporting requirements. These information-sharing processes and systems to Compliance should include, but not be limited to, Marketing, Surveillance, E-Commerce/Cage, Human Resources, Operations, Surveillance/Security, Fraud, Legal, Customer Support, Risk, and Internal Audit. Information sharing mechanisms should also ensure that internal audit, independent assessment, and exam findings and recommendations are timely shared with the AML Officer, senior leadership, and, as appropriate, others responsible for reviewing and updating AML/CFT Program functions. Casinos should also consider the extent to which it may be appropriate to leverage information across the entire enterprise in investigating and reporting suspicious activity, including attempted suspicious transactions.

Personnel should receive regular compliance training and communications regarding their duty to use information-sharing mechanisms and how to use them.

See the SAR Confidentiality section above for internal sharing restrictions and best practices for SAR information.

Information Sharing with Partners/Service Providers

Casinos should have clear and detailed contract terms and supporting procedures around information-sharing requirements for third-party relationships that address, at a minimum:

- A casino's full and timely access to all patron information and other records associated with BSA-related functions
- The third party's obligation to promptly notify the casino of potentially suspicious activity or other illicit activity
- Minimum security measures that the third party must maintain for information it has or receives
- Restrictions on the third party's disclosure to other third parties and use of information
- Recordkeeping requirements that the third party must implement for casino information

Casinos should have clear privacy terms for their patron relationships that authorize them to use and share patron information as necessary to comply with laws/regulations, cooperate with law enforcement, and provide the casino's products and services. Likewise, casinos should ensure that any information sharing with third parties, including partners and service providers, is permissible under their patron terms and does not violate applicable laws or regulations.

As mentioned above, SARs and information regarding whether or not a SAR was filed should generally not be shared with third-party partners and services providers, and to the extent permitted, it should only be on a strictly need-to-know basis based on the services they provide to the casino and supported by clear and robust contract terms and security systems and processes to protect against unauthorized disclosures, further sharing by the third party, and data breaches that may compromise the confidentiality of the SAR information.

314(b) Information Sharing

Casinos are encouraged to participate in the valuable voluntary information-sharing program with other entities defined as financial institutions under Section 314(b) of the USA PATRIOT Act and who are required to maintain AML/CFT Programs under the BSA regulations. This program, and other formal and informal information sharing mechanisms, are a FinCEN priority and are vital to ensuring casinos and other financial institutions can obtain necessary information about their patrons/customers.[23]

In its most recent 314(b) fact sheet, FinCEN highlights the following benefits of the information-sharing program[24]:

- While information sharing pursuant to Section 314(b) is voluntary, it can help financial institutions enhance compliance with their AML/CFT requirements, most notably with respect to:
  - Gathering additional information on patrons or transactions potentially related to money laundering or terrorist financing, including previously unknown accounts, activities, and/ or associated entities or individuals
  - Shedding more light upon overall financial trails, especially if they are complex and appear to be layered among numerous financial institutions, entities, and jurisdictions
  - Building a more comprehensive and accurate picture of a patron's activities that allows for more precise decision-making in due diligence and transaction monitoring processes for that patron
- Alerting other participating financial institutions of patrons with suspicious activities they may not have been previously aware of
- Facilitating the filing of more comprehensive SARs
- Identifying and aiding in the detection of money laundering and terrorist financing methods and schemes
- Facilitating efficient SAR reporting decisions — for example, when a financial institution obtains a more complete picture of activity through the voluntary information sharing process and determines that no SAR is required for transactions that may have initially appeared suspicious

Casinos that participate in 314(b) should have protocols in place regarding when 314(b) information sharing should be utilized, the timing and manner for responding to 314(b) requests, and verifying that a financial institution or association of financial institutions is on the 314(b) participant list, prior to requesting information from or sharing information with that institution or association. Participating casinos must also have protocols in place to safeguard the security and confidentiality of shared information. They should implement policies and training designed to ensure that they only share information when they have a reasonable basis to believe that the information relates to activities that may involve money laundering or terrorist financing, and that shared information is only used for the purpose of:

- Identifying, and where appropriate, reporting on activities that may involve terrorist financing or money laundering
- Determining whether to establish or maintain an account, or to engage in a transaction
- Assisting in compliance with AML requirements

All 314(b) requests and responses should be fully documented and maintained for at least five years.

Other Information Sharing Resources

Casinos may also benefit from information sharing on suspicious activity trends and typologies impacting the industry or of particular interest to law enforcement by participating in local, regional, and national working groups and attending BSA/AML and industry conferences.

[23] See also FinCEN, Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance, FIN-2014-A007 (Aug. 11, 2014), available at: https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2014-a007; Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the 11th Annual Las Vegas Anti-Money Laundering Conference and Expo (Aug. 2018), available at: https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-11th-annual-las-vegas-1. A 2016 study by Ernst & Young for the American Gaming Association surveyed officials from twenty-three law enforcement and gaming regulatory agencies and found that the casino industry has made concerted efforts to enhance AML compliance and reporting. Investing in America's Financial Security: Casinos' Commitment to Anti-Money Laundering Compliance, p. 27, available at: https://www.american- gaming.org/wp-content/uploads/2018/12/AGA-AML-Research-Report-Final-011916.pdf.

[24] FinCEN, Section 314(b) Fact Sheet (Dec. 2020), available at: https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.

Independent Reviews

Independent Reviews

The BSA regulations require periodic, risk-based independent testing of the casino's AML/CFT Program by qualified independent auditors. Independent testing may be conducted by Internal Audit, outside auditors, consultants, or other qualified independent parties. In either case, the party testing the program must be independent, experts in BSA regulatory requirements and conducting audits, unbiased, and without conflicting business interests that may influence the outcome of the independent review. Internal auditors should not have operational responsibilities or be involved in or report to teams responsible for AML/CFT functions. For instance, Surveillance is typically integral to the casino's AML/CFT Program, so their required audit could be viewed as a potential conflict of interest. Similarly, external auditors should not be involved in developing, testing, or performing AML/CFT functions. Additionally, a regulatory examination of the casino's AML/CFT Program by governmental authorities does not qualify as independent testing under the BSA. Safeguarding the integrity and independence of the compliance program testing enables an institution to locate and take appropriate corrective actions to address AML/CFT deficiencies.[25]

The independent testing must cover all elements of the casino's AML/CFT Program, including but not limited to:

- KYC and customer due diligence processes
- Transaction monitoring
- SAR and CTR reporting
- Recordkeeping
- Training
- The AML Officer function

The scope and frequency of independent testing should be proportionate to the money laundering and terrorist financing risks posed by the products and services provided by the casino.[26] Casinos should generally conduct independent testing at least annually, and more frequently when there are significant changes in the casino's risk profile, systems, compliance staff, or processes. More frequent independent testing may also be appropriate when errors or deficiencies in some aspects of the AML/CFT Program have been identified or to verify or validate mitigating or remedial actions.

The independent auditors should report their findings directly to the AML Officer and any other senior management officials who have the authority to remediate the audit findings and ensure corrective action is taken. Casinos should have protocols in place to ensure the AML Officer's prompt and adequate subsequent reporting of the results of independent testing to the board of directors and other senior leadership with oversight responsibilities for the AML/CFT Program. The casino should undertake corrective action or make a specific documented determination that no such action is necessary for each audit finding.[27]

All audit procedures performed by independent auditors and their reports and findings, as well as corrective actions taken by a casino, should be fully documented and maintained for at least five years.

[25] FinCEN, FIN-2014-A007 Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance, at p. 4 (Aug. 11, 2014), available at: https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2014-a007.
[26] 31 C.F.R. § 1021.210(b)(2)(ii).
[27] FinCEN, FIN-2010-G003, Casino or Card Club Compliance Program Assessment (June 30, 2010), available at: https://www.fincen.gov/resources/statutes-regulations/guidance/casino-or-card-club-compliance-program-assessment.

Independent Testing Procedures for CTRs

Separate from the independent testing of the program, on a scheduled basis, the casino's independent auditor, or audit team for CTR filings, should review currency transactions by using all relevant records, including but not limited to MTLs, player-rating records, and patron deposit and withdrawal records, that were prepared during the gaming day reporting period, as well as all system reports for the period.

An initial audit should ensure:

- That a CTR has been prepared for all reportable transactions — either single or aggregated — that exceed $10,000
- That the information recorded on the CTR is complete and accurate
- CTRs were electronically filed within 15 days of the transaction date

If the initial findings indicate possible weaknesses in the AML/CFT Program, the audit may need to be expanded to confirm or disprove those indications.

The monetary/negotiable instrument log (MIL/NIL) should also be reviewed by independent auditors for proper completion and for retention for at least five years.

A system query should identify any patrons that completed transaction(s) in currency involving either cash-in or cash-out higher than the threshold determined by the casino's risk assessment. For patrons who have reached the log threshold for the gaming day, the total of the currency paid or received shall be entered into the MTL for reporting when required by law.

All currency transactions above an amount established by the risk assessment for the casino will be logged, with the exception of slot jackpots, which are not reportable on CTRs.

Exception notices will be prepared for all instances of noncompliance noted during the daily audit, including but not limited to, logging errors, MIL/NIL completion errors, inaccurate identification, missing information, and other requirements not met.

The exception notices should be sent to applicable casino supervisory personnel at the conclusion of the independent audit and secondary review. Exception notices should be returned within a reasonable, time indicating corrective action taken, and the results of these periodic audits should be part of the firm's overall independent testing.

Independent Testing Procedures for SARs

The independent testing function should establish testing parameters for both SAR and no-SAR decisions. This review will evaluate the completeness of investigation processes and documentation, timeliness of review and reporting, record retention, and safeguards from disclosure.[28] In instances where SARs were filed, the independent auditors should test the completeness of SAR fields, narratives, and the timeliness of filings.

This review should also test the casino's monitoring systems, including how the system(s) fits into the casino's overall suspicious activity monitoring and reporting processes, as well as their programming methodology and algorithms, to ensure the scenarios are adequately detecting potentially suspicious activity. When evaluating the effectiveness of the casino's monitoring systems, independent auditors should consider the casino's overall risk profile based on its products, services, patrons, entities, geographic locations, volume of transactions, and adequacy of staffing. Independent reviews should also test information flow across the casino, including but not limited to fraud, security, marketing, and human resources functions, to compliance personnel responsible for SAR monitoring, investigation, and reporting processes.

[28] See FinCEN, FIN-2012-A002, SAR Confidentiality Reminder for Internal and External Counsel of Financial Institutions (Mar. 2, 2012), available at: https://www.fincen.gov/sites/default/files/advisory/FIN-2012-A002.pdf. Additional risk-based measures to enhance the confidentiality of SARs could include, among other appropriate security measures, limiting access on a "need-to-know" basis, restricting areas for reviewing SARs, logging of access to SARs, using cover sheets for SARs or information that reveals the existence of a SAR, and/or providing electronic notices that highlight confidentiality concerns before a person may access or disseminate the information. See also IRS, Examination Techniques for Bank Secrecy Act Industries: 4.26.9.3.7 Review of Records, at (7)(c), available at: https://www.irs.gov/irm/part4/irm_04-026-009.

Employee Training

Employee Training

Casinos are required to provide ongoing BSA/AML training to personnel. The extent and intensity of the training should vary according to the responsibilities of the employee but should always address, at a minimum:

- BSA/AML requirements
- Recent BSA/AML regulatory guidance and enforcement actions
- The casino's AML/CFT Program components and commitment to compliance
- CTR and SAR reporting and confidentiality requirements and associated internal procedures
- Identifying and escalating relevant red flags for suspicious activity
- How BSA reports are used by government agencies

Training should be department-specific, so that trainees understand their role in the overall AML/CFT Program's success and how the particular transactions they conduct and the patron interactions they have fit into it. Trainees should gain an understanding of red flags for suspicious activity that may arise from the transactions they handle and the patron interactions they are likely to encounter, consistent with the risks identified in the casino's risk assessment. Training for personnel who regularly interact with patrons, such as those in marketing, should include focused emphasis on SAR confidentiality requirements.

Employees who may encounter transactions governed by the BSA should receive training before functioning alone in that capacity, when newly hired or promoted, and on an ongoing annual basis. Training should take place more frequently, as needed, to address changes in the law or the casino's AML/CFT Program that impact their role and responsibilities. Likewise, training materials should be updated regularly to reflect regulatory and enforcement developments under the BSA and any changes to the casino's AML/CFT policies and procedures.

Training should also be appropriate for the level of seniority and responsibilities of employees and management. Consequently, senior leadership should receive different AML/CFT training than frontline supervisors and employees. The responsibilities of more senior personnel may tend to involve more oversight and assessment of risk, so AML/CFT training should be tailored to these roles accordingly.

At a minimum, AML/CFT training should extend to the following general categories of employees:

- Those engaged in the operation of casino games (table games, poker, slots, keno and bingo, and racing and sports betting — both retail and online), beginning at minimum with supervisors and above. If a casino elects to not train dealers, they should consider messaging for recognizing and reporting suspicious activity
- Casino marketing employees whose job requires direct contact with patrons, including domestic and international hosts, branch office employees, and special events employees
- Cage employees
- Credit, Collections, and other Payments department employees
- Surveillance employees
- Employees in BSA/AML, Fraud, Responsible Gaming, and other Compliance departments
- Audit employees, including Internal Audit
- Senior leadership, including the board of directors, senior gaming management, audit committee, and compliance committee, as applicable
- Any other employee(s) with a responsibility to AML compliance

Training on BSA/AML policies and Form 8300 reporting for non-gaming employees (high-end retail, nightclubs, convention sales, hotel, and food and beverage) should be incorporated into their respective job training, as relevant to their functions.

BSA/AML training programs may include a variety of formats, including in-person training, live remote training, and interactive online training. Training should be interactive and offer participants the opportunity to ask questions, either during or following the training. On-the-job training is also an important component and provides real-life context to supplement official training materials. There should also be a testing component that ensures comprehension of the material, and a signed acknowledgement form agreeing to comply with the casino's BSA/AML policies.

Casinos should have procedures and controls for tracking and ensuring training completion, including measures to ensure employees who are on leave during regularly scheduled training complete the training upon return. All training materials, including material provided or shown to trainees, test scores, trackers, and signed acknowledgements, should be maintained for at least five years.

Recordkeeping and Retention

Record Keeping and Retention

Casinos must have procedures to maintain and retain the specific transactional, patron, and other records required under the BSA and must retain records about the execution of all aspects of its BSA program.

The casino shall adopt a recordkeeping system to preserve, among other BSA-related records, the following records for at least five years:

- MTLs
- MILs/NILs
- CTRs
- SARs, and SAR supporting documentation, including surveillance records, records of SAR investigations and SAR decision-making
- Training and testing materials and records of who was trained and when
- Patron KYC and due diligence records, including:
  - A record of specific procedures performed to analyze a patron's gaming patterns and financial transactions
  - Any due diligence reports created
  - Any risk determination
  - Any action taken as a result, including termination or monitoring of the patron, reports to law enforcement agencies, or changes in casino services available to the patron
- Records of independent testing, quality assurance testing, and actions taken in response to each

Patron due diligence records should be maintained for at least five years after the relationship is terminated or the patron is no longer active.

Anti-Human Trafficking

The gaming industry plays an important role in combating human trafficking.

Human trafficking, with an estimated 25 million global victims annually, is a pervasive human rights offense and a form of modern-day slavery. It is one of the most profitable forms of transnational organized crime with far-reaching impacts. Traffickers do not discriminate as to where they operate — human trafficking has been reported in all 50 states — and can also be family members or known to their victims.

Traffickers take advantage of legitimate industries and supply chains to find, exploit, and traffic victims. This is especially true for the travel and tourism industry — including casino gaming — when properties are unwittingly used to facilitate criminal activity. Human trafficking may be linked to other illegal enterprises such as narcotics or firearms trafficking, terrorist organizations, and money laundering.

Eradicating human trafficking is a complex process that requires government, law enforcement, business, and the public to work together on proactive solutions that identify traffickers, address the underlying causes of these crimes, and provide support for victims. The gaming industry plays an important role in combating human trafficking.

Gaming operations have been used to facilitate human trafficking. In particular, physical casinos or resorts can be locations for actual trafficking to take place, while casinos and online gaming apps can be used to launder money related to trafficking operations.

RED FLAGS FOR POTENTIAL HUMAN TRAFFICKING

Casino employees should be aware of different warning signs that could indicate human trafficking. One indicator does not necessarily equate to trafficking, but it is important to be aware of red flag indicators that include, but are not limited to:

- Signs of abuse (verbal or physical)
- Signs of poor hygiene, malnourishment, or fatigue
- Fearful, anxious, or submissive behavior
- Individuals not allowed to control their cell phone, ID, hotel key, or money
- Guests overly concerned about surveillance or security on premises, avoiding interactions with security personnel or the sightlines of cameras, or scoping out the perimeter of the casino floor
- Individuals approaching patrons whom they do not seem to know, who appear inebriated, or are winning big at gaming tables
- Individuals or groups making recurring and frequent trips between the casino floor and hotel rooms
- Rooms booked for large numbers of people and/or rooms booked in the name of guests with a local address
- Excessive requests for sheets and/or towels
- Multiple individuals going in and out of one room
- Individuals speaking in a scripted, repetitive manner
- Refusing to cooperate with security or floor personnel when approached or giving evasive or non-responsive answers to questions
- Individuals of similar age, ethnicity, tattoos, or dress accompanied by a potential trafficker
- Individuals who appear unfamiliar with casinos, seem unsure of how games work, where to congregate, or floor rules
  - Conversely, individuals may also frequent the casino and are intimately aware of how the operation runs, show aggressive behavior in response to questions, or flee at the first sign of security or law enforcement personnel.
- Individuals monitoring or controlling the movements of another person or using hand signals to communicate
- Multiple visits to the property by an individual with multiple different accompanying patrons
- Disparity in age between individuals that are together
- Someone dropping off or picking up other individuals multiple times or waiting onsite at parking structures, facility exits, or drop off locations to meet people

Anti-Human Trafficking

HUMAN TRAFFICKING AND AML

Team members whose role includes observing for signs of money laundering should be aware of the following behaviors.

At the cage, watch for the involvement of a third party who insists on:

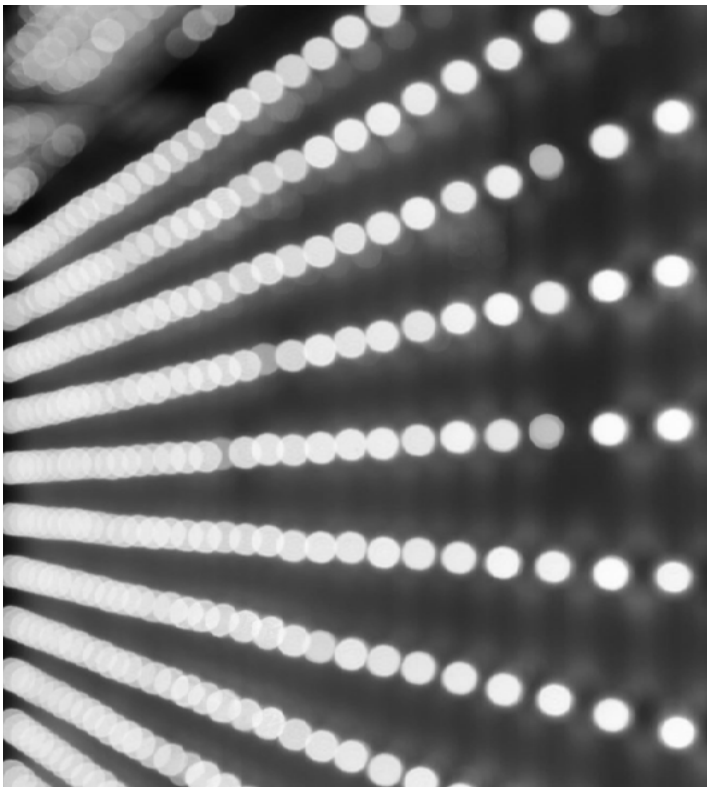
- Being present for another person's money transactions, or who speaks on behalf of the customer conducting the transaction.
- Filling out paperwork for another customer, without consulting that person.

Other financial transactions related to human trafficking operations could involve a customer who:

- Uses or attempts to use third-party identification for a financial transaction.
- Transaction history that shows different geographic locations.
- Frequently makes cash deposits with no Automated Clearing House (ACH) payments.
- Frequently purchases and uses prepaid access cards.
- Has an account that shares common identifiers, such as a telephone number, email, and social media handle, or address, associated with escort agency websites and commercial sex advertisements.

STEPS TO TAKE

- Should you or any team member observe signs or behavior that suggests exploitation or trafficking, or if concerns arise for someone's welfare, you must follow your company's procedures. Be sure that you have reviewed a copy of those procedures.
- If you observe suspicious activity, take note of all parties involved, including the perceived trafficker, any possible victims, the time and location within the casino, and any statements that may have been made.
- Should you have any direct contact or conversation with someone you suspect may be a trafficking victim, exercise great care. Victims fear being arrested and possible retribution and abuse from their traffickers. Some victims may not immediately respond to assistance and may be resistant. In those cases, local anti-trafficking organizations



may be the most effective route for assistance, and it is essential that they are integrated into your company's response plan.

- Never try to intervene on your own; always wait for support from those who have experience dealing with similar situations.
- If someone on your team notices that the victim speaks a language other than English and recognizes the language they speak, find someone who can inform them that there is help available in their language.
- If the victim reaches out directly for help and wants to be hidden from their traffickers because they are scared to be found asking for help, then you can offer to take them into a safe place until law enforcement or your local anti-trafficking provider arrives.

Conclusion

Conclusion

These practices reflect the continuing efforts of AGA members to mitigate the risks of potential money laundering and illegal activity connected with their businesses. The guidelines in this document must be adapted to match the specific risks and environments of individual casinos and companies.

Casinos should evaluate their AML/BSA compliance risks and mitigation strategies on a routine basis to ensure they account for new risks and emerging patterns of illegal activity. When dealing with businesses as complex as modern casinos, and with judgments as subjective as those required by the BSA, no compliance effort can be perfect or immune from retrospective reevaluation.

Though perfection cannot be expected of a process that involves so many variables and periodic shifts in financial practices and regulations, effective AML/BSA compliance programs should ensure that the gaming industry continues to effectively combat money laundering and illicit financing threats.

The AGA appreciates the participation and collective expertise of our members in the conception, drafting, and revisions of this guide. Their commitment to compliance is strong, and we applaud them for sharing these best practices with the industry.

Glossary

Glossary

Agent: A person acting on behalf of another person

Bank Secrecy Act (BSA): Adopted in 1970 and amended several times since, the statute authorizes the U.S. Secretary of the Treasury to impose on U.S. financial institutions the requirement to keep and submit such reports that have a high degree of usefulness in criminal, tax, and regulatory matters, and in the conduct of intelligence activities to protect against international terrorism. (31 U.S.C. §§ 5311, et seq.)

Cage: A secured area adjacent to the gambling floor of a casino where casino cashiers conduct financial transactions for the guest. This includes the redemption of gaming instruments, cash advances, marker/credit, front money, and other gambling-related transactions, and where currency and chips are often kept. Safety deposit boxes are often available at the cage. A large casino may have more than one cage location.

Casino: A venue or interactive platform that offers its patrons highly regulated gaming activities, such as traditional casino-style games, house-backed games, and sports betting

Chip Walk: When a patron leaves the casino floor with a significant amount of chips in their possession, without offsetting chip redemptions or chip buy-ins at another table, and there is no known disposition or whereabouts of the chips. A chip walk may not be deemed suspicious if there is a reasonable, experience-based expectation that the patron will return to the casino in the near future and that the departure with chips was not done in an attempt to structure.

Credit: Under the regulations of many state licensing authorities, casinos are authorized to issue gaming chips or other representatives of value to patrons for gambling purposes up to the amount of a "marker" (see below), a negotiable instrument signed by the patron and made out to the casino. Although state regulations refer to such arrangements as credit transactions, the markers may be negotiated immediately at the discretion of the casino.

Digital Identification: Some states may issue a digital form of identification (e.g., driver's license, state ID card) instead of or in lieu of a physical government-issued picture ID card. This development may assist in online, internet, or mobile gaming applications as part of the KYC process, as new technology continues to expand and be acceptable for certain digital wagering account applications. Absent of specific FinCEN guidance forbidding the use of digital IDs for AML purposes, casinos should include whether or not they will accept digital IDs in their written AML/CFT Program.

Digital Wallet: A software-based system that securely stores users' payment information and passwords for payments and withdrawals

Front money: Cash, wired funds, or negotiable instruments that are deposited with the casino by a patron who will draw down on those funds for gambling. Front money accounts are sometimes described as safekeeping accounts.

Geolocation: The identification of the geographic location of a user or computing device via a variety of data collection mechanisms, typically using network routing addresses or internal GPS devices

Interactive Gaming: Interactive gaming comprises traditional internet gaming (e.g., casino games, poker), mobile wagering (e.g.,casino games), and account wagering (i.e., funding an account whether at a brick-and-mortar location or via the internet or smartphone that can be used in digital channels).

Interest on Lawyer's Trust Account (IOLTA): A financial account set up by a law firm in which the funds are held in trust for the benefit of the firm's clients and are, by state law or supreme court rule, to be held separate and apart from the funds belonging to the law firm

Internet Protocol (IP) Address: A unique address that identifies a device on the internet or a local network

Marker: A negotiable instrument (sometimes called a counter-check) executed by a casino patron that authorizes the casino to recover the amount of the marker from the patron's bank account. The casino will advance funds to the patron up to the amount of the marker. Under state casino regulations, casinos are not required to conduct full credit investigations before issuing a marker, but will confirm that the patron's bank account contains sufficient funds to cover the requested marker.

Glossary

Monetary/Negotiable Instrument Log (MIL/NIL): Required by the BSA, it must reflect transactions of monetary instruments (e.g., money orders, cashier's checks, traveler's checks, and bank drafts) between the casino and the patron with a value of $3,000 or greater.

Money Laundering: Money laundering is the process of hiding the original source of money obtained from illegal activity by making the funds appear as if they were legally earned or won. In the eyes of the government, money laundering also includes the act of spending (or gambling) the proceeds of illegal activity. Money laundering, which is illegal, supports many types of illegal activity, such as drug trafficking, terrorist financing, tax evasion, and fraud. It is a crime to allow a patron to transact or gamble with funds if you have knowledge that the funds are proceeds from illegal activity. It is also a crime if you suspect a patron is using funds from illegal activity, but you deliberately avoid confirming your suspicion (you cannot "put your head in the sand" or be willfully blind).

Multiple Transaction Log (MTL): This is a record of cash-in and cash-out transactions at or above a predetermined amount, which also records identifying information about the patron used to determine when a person is approaching or has exceeded a reportable threshold.

Risk Assessment: The formal process of examining a casino's mix of gambling activity, patrons, and overall economic environment to identify activities, levels of play or other transactions that pose a risk of money laundering and should be addressed by the casino's AML compliance procedures.

Safekeeping: A patron's non-claimed gaming funds, overages from deposits, and other funds not falling under front money are placed in safekeeping. These funds are not redeemed or tied to casino markers.

Structuring: When a person acting alone, in conjunction with, or on behalf of another person, conducts, or attempts to conduct, one or more transactions. This is the case for any amount, at one or more locations, on one or more days, in any manner for the purpose of evading the CTR requirements.

Third-Party Transactions: Deposits, withdrawals, payments, and transfers of funds to and from a casino account by anyone other than the primary account holder

Ticket-in, Ticket-Out (TITO): A system for slot machine play that uses a barcoded paper ticket. The ticket may be purchased in advance of slot machine play or issued from the slot machine if there are credits remaining at the conclusion of the patron's gaming session. When the patron has completed their play, balances on the ticket can be redeemed for cash at a kiosk or casino cage and used for further play at the casino that issued the ticket.

Sports Wagering: With the repeal of the Professional and Amateur Sports Protection Act (PASPA) in May 2018, sports wagering is permissible in certain U.S. states that have legalized it. A casino may offer sports wagering over the counter via a sportsbook kiosk, an internet browser, and/or a mobile app. If offered via an internet browser or a mobile app, the patron will have a separate wagering account apart from any casino wagering account for slots, table games, and keno, as the sports wagering system is its own self-contained proprietary system.

Universally Unique Identifier (UUID): An identification number that will uniquely identify an electronic device

Appendix

APPENDIX A:

ANTI-MONEY LAUNDERING PROGRAM QUESTIONNAIRE

A compliance program may be satisfactory even if some of the answers to these questions are not in the affirmative, as long as the company can explain why its policies provide adequate AML vigilance.

A. GENERAL POLICIES, PRACTICES, AND PROCEDURES

1. Is the AML/CFT Program approved by the company's senior management or board of directors?
2. Does the company's legal and regulatory compliance program include a designated officer who is responsible for coordinating and overseeing the AML compliance framework, as well as sufficient staff to provide support to the designated officer?
3. Do you have written policies documenting the processes in place to prevent, detect, and report suspicious transactions across all games and financial services offered?
4. Do you perform periodic training on AML policies and practices for those employees covered by your compliance program?
5. In addition to inspections by government regulators, does an internal audit function or other independent third party periodically assess AML policies and practices?
6. If a patron proposes a transaction with a corporation on their behalf, do you have a policy for inquiring into the identity of the beneficial owners of the corporation involved and its relationship to the patron?
7. Do you have policies to reasonably ensure that you will not conduct transactions with shell banks or corporations?
8. Do you have policies for identifying politically exposed persons (PEPs), their family, and close associates, and for controlling transactions with such individuals?
9. Do you have record retention procedures that comply with applicable law?
10. Are your AML policies and practices being applied to all associated entities, both in the U.S. and in foreign locations?

B. RISK ASSESSMENT

1. Do you have a risk-based assessment of your patron base and their transactions?
2. Do your risk-based assessments consider:
   a. The volume and character of overall gaming activity at a gaming venue
   b. The characteristics of the games and financial services offered at a gaming venue
   c. A patron's country of origin
   d. The gambling patterns or financial transactions favored by a patron
   e. Third-party information about a patron, including negative information regarding the patron's integrity
   f. Whether a patron has sources of wealth or income commensurate with their gaming activity
   g. Whether a patron has provided verifiable identification information
   h. Whether a patron has financial fiduciary obligations (e.g., trustee, accountant, attorney, or nonprofit/charity executive)

ANTI-MONEY LAUNDERING PROGRAM QUESTIONNAIRE

i. Whether a patron is associated with individuals or entities known to be connected with the illicit generation of funds or legalized marijuana-related activity

j. Whether a patron claims connections with businesses that have no apparent operations

k. Whether a patron is the subject of substantial tax liens or has gone through a recent personal bankruptcy proceeding

3. Does your compliance program identify and explain the proper responses by employees to patrons and transactions that you have reason to believe pose a heightened risk of illicit activities at or through your casino?

C. KNOW YOUR CUSTOMER/PATRON AND DUE DILIGENCE

1. Have you implemented processes for securing identification for those patrons whose transactions fall within the AML/CFT Program?
2. Do you have a requirement to collect information regarding a patron's business activities and connections?
   a. If so, under what circumstances does that requirement apply?
   b. What steps should be taken in that effort?
3. Do you have a process to review and update patron information relating to high-risk relationships and activities?
4. Do you complete a risk-based assessment to understand the normal and expected transactions of patrons?

D. REPORTABLE TRANSACTIONS

1. Do you have policies or practices for the identification and reporting of transactions that must be reported?
2. For currency reporting purposes, do you have procedures to identify multiple transactions that have been structured to avoid such reporting?
3. Do you screen patrons and transactions against lists of persons, entities or countries issued by the OFAC or other government authorities?

E. TRANSACTION MONITORING

1. Do you have a monitoring program for unusual and potentially suspicious activity that covers funds transfers, engaging in financial transactions without significant gaming activity, coordinating activity with other patrons, and the like?
2. In order to identify AML concerns, do you review daily audit summaries, logs, and reports, such as marker summaries, front-money/safekeeping summaries, MTLs, MILs, check logs, and wire reports?

F. PREVENTIVE MEASURES

1. Do you cap TITO redemptions at slot machine kiosks?
2. Do you cap the level of cash-for-cash exchanges?
3. Do you accept currency to purchase a casino check, other monetary instrument, or wire transfer?
4. Will you issue casino checks or wires to a patron for an amount greater than their winnings? Under what circumstances?

ANTI-MONEY LAUNDERING PROGRAM QUESTIONNAIRE

5. Do you issue checks for winnings only in the name of the patron?
6. Do you require supervisor review of checks or wires made payable to a patron's business or other account or another individual?
7. If a patron declines to provide identifying information when required (e.g., for CTRs), do you suspend the patron's loyalty club account or bar the patron?
8. Do you allow cash play at poker tables?
9. Do you accept virtual currency?
10. Do you protect patron information to prevent social engineering, software vulnerability exploits, and network attacks?

G. EMPLOYEE TRAINING

1. Is your AML Officer at each gaming venue educated on the requirements of the AML/CFT Program, including suspicious activity reporting and currency transaction reporting, and the requirements of state and federal regulators for AML compliance?
2. Do you provide AML training to other relevant employees? If so, does that training include:
    a. Identification and reporting of transactions that warrant a suspicious activity report or a CTR
    b. Examples of different forms of suspicious or illegal activity involving the casino's business and services
    c. Correct methods for completing currency transaction and SARs
    d. Internal policies to prevent money laundering
    e. Do any of the following employees receive AML training:
        i. Those engaged in the operation of casino games, beginning at least at the supervisor level
        ii. Casino marketing employees
        iii. Cage employees
        iv. Surveillance employees
        v. Property compliance and AML compliance employees
        vi. Audit employees, including Internal Audit and/or Fraud department employees
        vii. Senior gaming management, members of the board of directors, audit committee, or compliance committee
3. Do you retain records of training sessions, including attendance records and the training materials used?
4. Do you update relevant employees on changes in AML law, policies or practices?
5. Do you provide training on the red flags of human trafficking, as well as financial red flags associated with human trafficking?

AMERICAN GAMING ASSOCIATION®

AMERICANGAMING.ORG

american-gaming-association

AmericanGaming

@AmericanGaming

@AmericanGaming