Best Practices for

Anti-Money Laundering Compliance

2022

AMERICAN GAMING ASSOCIATION®

Table of Contents

INTRODUCTION

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 venue that offers its patrons highly regulated gaming, often combined with hotels, multiple dining options and live entertainment. Frequently brick and mortar casino operators also have digital operations, offering interactive games or mobile sports betting offerings. To facilitate gaming activity, casinos, as well as online and mobile gaming operators, ordinarily provide some financial services to their patrons. They endeavor to ensure that these financial services are used for gaming related purposes. Although the vast majority of 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.

This document is an attempt to distill the practices that a wide range of gaming operators – including land-based casinos, sports books, and interactive and mobile gaming sites - have adopted to meet these challenges. This document uses the term "casino" to cover in-person and lawful interactive and mobile gaming operations as well as sports betting, because the BSA/AML compliance effort applies to all forms of casino-style gambling.

This document is not intended to be a checklist of actions required of every casino and should not be applied arbitrarily to any individual situation, or on a blanket basis.

> AML programs are 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.

Moreover, in some instances, industry practices may go beyond a legal requirement established by statute or regulation, so this document should not be considered a guide to those legal requirements.

The goal of this document is to provide a resource for the gaming industry as well as other financial sectors subject to the BSA, the government and law enforcement to help guide their efforts to protect the gaming industry and the broader financial system from money laundering, illicit financing and other illegal activity.

To safeguard the integrity of the casino industry and the U.S. financial system, casino companies and gaming operators have developed effective risk-based programs to ensure compliance with the legal requirements of the federal Bank Secrecy Act and associated AML statutes and regulations. AML programs also protect the casino and its employees from even unwittingly being involved in money laundering criminal conduct.

[1] As used in this paper, money laundering and anti-money laundering compliance (AML) also encompasses the terms terror financing and combatting the financing of terrorism (CFT).

BACKGROUND

Since 1985, state licensed casinos have been defined as "financial institutions" under the Bank Secrecy Act (BSA). Accordingly, they are subject to BSA reporting, recordkeeping and AML program requirements. Casinos must file currency transaction reports (CTRs) when a patron conducts a cash-in or cash-out transaction in currency by or on behalf of a patron of more than $10,000 in currency during a casino's defined 24-hour gaming day.

Casinos also must file suspicious activity reports (SARs) when a 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;
- Uses the casino to facilitate criminal activity;
- Has no economic, business, or apparent lawful purpose; or
- Is not the sort of transaction in which the particular patron would be expected to engage, and the casino knows of no reasonable explanation for the transaction after examining the available facts.

More broadly, the BSA also requires casinos to design and implement risk-based AML programs that include an annual risk assessment and a formal know your customer (KYC) program in addition to the following measures (at a minimum):

- A system of internal controls, policies, and procedures to assure ongoing compliance;
- Procedures for using all reasonably available information to determine:
  - When required by BSA regulations, the name, permanent address, Social Security number, and other information, and verification of the same, of a person;
  - Whether SARs need to be filed and which information to include in the SAR filing when available;
  - Whether any other record required under the BSA must be made and retained;
- Internal and/or external independent testing for compliance;
- Appropriate, ongoing training of casino personnel;
- An individual or individuals charged with assuring day-to-day compliance (the "AML officer"); and
- Lastly, to assure compliance by using automated programs to aid in assuring compliance.

BACKGROUND

In the interest of maintaining the integrity of gaming and complying with the above requirements, each casino company should implement a comprehensive, risk-based, robust anti-money laundering compliance program that ensures that it submits appropriate CTRs and SARs as required.

A discussion of criteria for casino compliance programs appears at the website of the Financial Crimes Enforcement Network of the U.S. Department of the Treasury (FinCEN).

Further, the industry's AML compliance programs are also influenced by guidance from the U.S. Treasury, including the National Strategy for Combatting Terrorist and Other Illicit Financing (National Illicit Finance Strategy) and the National Money Laundering Risk Assessment (NMLRA).[2]

The 2022 NMLRA identified the following seven principal threats related to money laundering in the United States:

- Fraud
- Drug trafficking
- Cybercrime
- Professional money laundering
- Corruption
- Human trafficking and human smuggling
- Wildlife trafficking

Moreover, as stressed in previous NMLRAs, "most often criminals who use casinos to launder illicit proceeds do it through gambling and spending on entertainment"[3] – the exact same activities that the casino's other patrons are pursuing.

Consequently, there is often little observable basis for distinguishing between those patrons "laundering funds" in the casino and all other casino patrons.

In early 2021, the landscape of the U.S. federal AML laws and regulatory framework changed, following the enactment of the federal 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 United States pursuant to the following purposes of the Act:

- To improve coordination and information sharing among the agencies tasked with administering anti-money laundering and combating the financing of terrorism 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 anti-money laundering and combating the financing of terrorism 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 the financing of terrorism;
- To reinforce that the anti-money laundering and combating the financing of terrorism policies, procedures, and controls of financial institutions shall be risk-based;
- To establish uniform beneficial ownership information reporting requirements to (A) improve transparency for national security, intelligence, and law enforcement agencies and financial institutions concerning

[2] On May 13, 2022, the U.S. Department of the Treasury announced its 2022 National Strategy for Combatting Terrorist and Other Illicit Financing. The 2022 strategy outlined priorities for the AML/CFT framework, law enforcement and technological innovation. See 2022 National Strategy for Combatting Terrorist and Other Illicit Financing (May 13, 2022). https://home.treasury.gov/news/press-releases/jy0779.

[3] U.S. Department of the Treasury, The National Money Laundering Risk Assessment 2015, https://home.treasury.gov/system/files/246/National-Money-Laundering-Risk-Assessment-06-12-2015.pdf, page 75, (June 2015).

corporate structures and insight into the flow of illicit funds through those structures; (B) discourage the use of shell corporations as a tool to disguise and move illicit funds; (C) assist national security, intelligence, and law enforcement agencies with the pursuit of crimes; and (D) protect the national security of the United States; and

- To establish a secure, nonpublic database at FinCEN for beneficial ownership information.

The AMLA mandates a range of extensive congressional reports, regulatory reviews and reforms as well as updates to the examination manuals and regulator and examiner training programs. As part of its implementation, FinCEN was required to issue National AML/CFT Priorities. In June of 2021 the priorities were stated as follows[4]:

- Corruption
- Cybercrime, including relevant cybersecurity and virtual currency considerations
- Terrorist financing
- Fraud
- Transnational criminal organization activity
- Drug trafficking organization activity
- Human trafficking and human smuggling
- Proliferation financing

FinCEN plans to issue regulations in the near future about how the priorities should be integrated into AML programs of financial institutions.

TAILORING AN EFFECTIVE RISK-BASED AML COMPLIANCE PROGRAM FOR CASINO OPERATIONS

Casinos' risk-based compliance effort involves many complexities. For patrons, casinos are generally not viewed as financial institutions, but rather are entertainment venues they enter and leave as it suits them. Many patrons are not, and never will be, personally known to casino employees. Unlike a traditional financial institution's customers, casino patrons are not required to identify themselves unless they trigger certain regulatory requirements (e.g., filing a CTR), and there may be only a limited amount of publicly available information about many gaming patrons.

Even those patrons who become identified to the casino, because they are frequent visitors or because they require assistance with financial transactions, ordinarily have no reason to disclose to casino employees their business or professional activities. Most are engaging in gaming activity as a form of leisure or entertainment.

Some, for legitimate personal or privacy reasons, may not care to have their gambling activities known. This is especially true for individuals in states that only recently legalized a form of gaming or wagering. In addition, the relatively small number of patrons who may attempt to launder funds through casinos take considerable pains to conceal that purpose from the casino.

To help address money laundering risks, casinos have developed comprehensive risk-based programs to identify patrons whose gaming activity approaches the CTR reporting threshold. That

[4] Financial Crimes Enforcement Network, Anti-Money Laundering and Countering the Financing of Terrorism National Priorities, https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf (June 30, 2021).

BACKGROUND

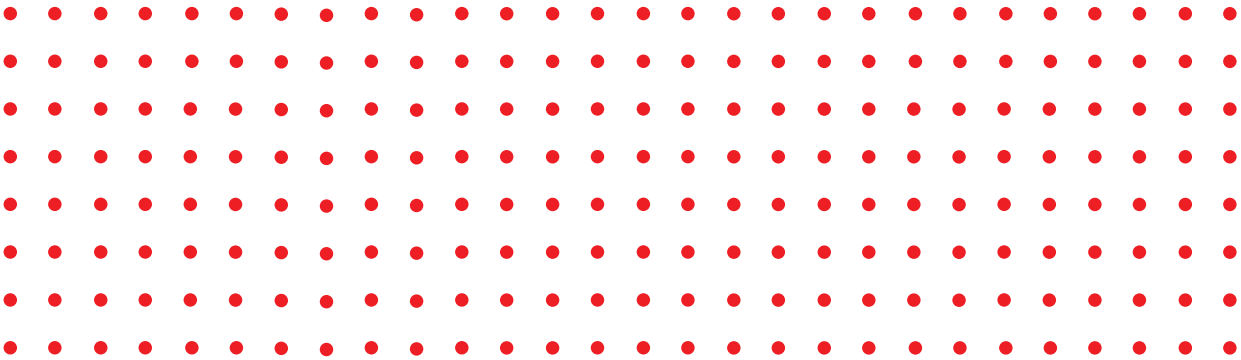
requires the aggregation of currency transactions from several different parts of the casino: the gaming tables, electronic gaming machines, TITO Redemption Units, and casino cage activity, including credit (or marker limit), credit card cash advances and front-money transactions.

To detect and report suspicious activity, casino employees and supervisors must make complex, nuanced judgments based on readily available information about a patron's activities. The process of investigating activity and deciding whether to file a SAR necessarily requires these judgement calls, and in some instances, reasonable minds may disagree over whether a SAR should be filed.

In some situations, suspicions can be confirmed or disproved only with information that is ordinarily unavailable to the casino, or by making inquiries of the patron—for example, concerning the source of the patron's funds. In some situations, patron activity that requires further vetting may only be resolved through candid conversations or obtaining sensitive documents (e.g., tax returns, divorce decrees).

These conversations can be sensitive as they may involve personal matters or complex business dealings. There may also be cultural differences and language barriers. Given these nuances, consideration should be given as to who is best suited to obtain this information and maintain the customer relationship or determine that the relationship should not be retained because it presents unacceptable risk - Front Line Associates, Casino Marketing, leadership from other departments (AML, Finance, Legal, Compliance) or a coordination of efforts.

Casinos should make a risk-based determination about which employees—senior managers or front-line employees—are in the best position to determine whether and how to undertake such an inquiry. For instance, the matter may involve issues that the casino ordinarily would have no business reason to investigate, and some patrons may have little or no incentive to review those issues with the casino. The involvement of senior managers may facilitate the interaction with the patron, as well as signal the importance of the inquiry. The strict confidentiality requirements for SAR filings and care around tipping off, necessitates careful consideration of what information will be disclosed before contact is made.



CASINOS' CULTURE OF COMPLIANCE

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

Casinos should consult with FIN-2014-A007[5], which discusses "Promoting a Culture of Compliance" including the following principles:

- Leadership should be engaged.
- Compliance should not be compromised by revenue interests.
- Information should be shared throughout the organization.
- Leadership should provide adequate human and technological resources.
- The program should be effective and tested by an independent and competent party.
- Leadership and staff should understand how their BSA reports are used.

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.[6] 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 FBI field office and sharing suspicious activity or information).

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 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 and customers.[7]

In its most recent 314(b) fact sheet[8], FinCEN highlights the following benefits of the information sharing program:

While information sharing pursuant to Section 314(b) is voluntary, it can help financial institutions enhance compliance with their anti-money laundering/counter terrorist financing (AML/CFT) requirements, most notably with respect to:

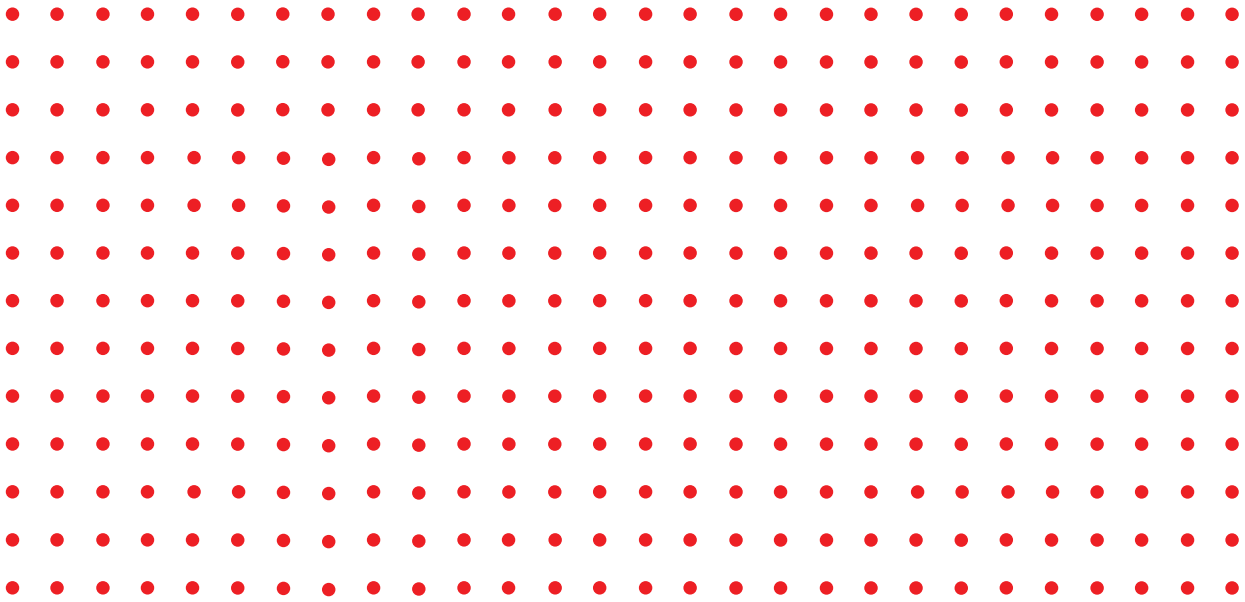
- Gathering additional information on customers or transactions potentially related to money laundering or terrorist financing, including previously unknown accounts, activities, and/or associated entities or individuals.

[5] See also, Financial Crimes Enforcement Network, Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance, FIN-2014-A007 (Aug. 11, 2014), https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2014-a007.
[6] 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. https://www.american-gaming.org/wp-content/uploads/2018/12/AGA-AML-Research-Report-Final-011916.pdf.
[7] Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the 11th Annual Las Vegas Anti-Money Laundering Conference and Expo (August 2018), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-11th-annual-las-vegas-1.
[8] Financial Crimes Enforcement Network, Section 314(b) Fact Sheet (December 2020), https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf

CASINO'S CULTURE OF COMPLIANCE

- Shedding more light upon overall financial trails, especially if they are complex and appear to be layered amongst numerous financial institutions, entities, and jurisdictions.
- Building a more comprehensive and accurate picture of a customer's activities that may involve money laundering or terrorist financing is suspected, allowing for more precise decision-making in due diligence and transaction monitoring.
- Alerting other participating financial institutions to customers of whose suspicious activities they may not have been previously aware.
- Facilitating the filing of more comprehensive SARs than would otherwise be filed in the absence of 314(b) information sharing.
- 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.

There is no more effective way to foster a positive culture than to have the casino's senior leadership and Board of Directors (whether directly or through the Board's Audit or Compliance Committee) engaged in the AML compliance effort, receiving periodic updates on regulatory developments, changes to the program, resources, and audit findings by regulators and by other independent compliance reviews. Senior leadership and the Board should communicate the importance of BSA/AML compliance within the organization, setting the compliance tone from the top.



RISK ASSESSMENT

The Bank Secrecy Act requires casinos to implement risk-based internal controls. Every financial institution is potentially at risk of being used for illegal purposes or accepting funds that were obtained illegally. Casinos should identify and assess their specific money laundering risks and adopt effective measures designed to mitigate those risks. The Risk Assessment and internal controls should be clearly documented as a part of the casino's AML program.

The casino's Risk Assessment should be the first step in building a compliance program.

Risk assessments should be reviewed and approved by senior leadership.
The risk assessment, conducted no less than annually, should be tailored to each specific casino venue and the nature and characteristics of its location, enterprise, products, financial services, and customers.

Many factors may be relevant to the risk assessment for a specific casino, but the risk assessment process begins with asking basic questions:

- First, what are the entry and exit points at the casino for patron funds that may come from illicit sources?
- Second, what casino departments or employees are best positioned to detect the entry and exit of such funds?
- Third, what are characteristics of transactions that may involve illicit funds, or of patrons who are more likely to engage in suspicious activity?
- Fourth, what measures (including automation) are in place to mitigate these risks?
- And finally, how effective are those measures?

In answering these questions, a casino will assess the BSA-related risks present at different parts of its business.

Casinos should also look at relevant enforcement actions, press reports, and legal cases to identify typologies that may be used to exploit their properties and evaluate whether their present compliance structure is sufficient to mitigate risks associated with those typologies.

On an annual basis and as part of its ongoing risk assessment, the casino should review its filed SARs for the previous year to analyze patterns of suspicious activity. The trends then may be reviewed by a casino's AML Committee, if applicable, to determine whether adjustments to the AML program or Risk Assessment are warranted.

Regulators, independent auditors, and law enforcement officials may also provide important guidance concerning risks that are arising in the financial system generally, and in the gaming industry specifically. The NMLRA is a good resource to identify threats and vulnerabilities.

RISK ASSESSMENT

Casino compliance professionals should also bring to bear their judgment based on experience with casino transactions.

Upon completion of the annual risk assessment, the compliance function should develop formal action items to be completed to reduce any insufficiently mitigated risks.

STATE REGULATORY REQUIREMENTS

States that grant casino licenses typically impose exacting regulation on casino operations, though specific requirements vary from state to state. State regulatory specifications can include the games that can be offered and the rules of each game; the financial services that can be offered and the procedures casinos must follow in providing them. State regulation also extends to the nature of the surveillance and security measures employed at the casino.

RESULTS OF INDEPENDENT AUDIT AND IRS EXAMINATION

Information identified in independent assessments of a casino's AML program should be carefully analyzed and reviewed. Such assessments include evaluations of independent auditors and Internal Revenue Service examinations of the casino's AML compliance program. The casino should undertake corrective actions in response to issues that arise during an examination or audit and revise its AML program accordingly or make a determination that no such action is necessary.

GAMING VOLUME AND CHARACTER

Different gaming venues may have differing risks based on their unique product mix and customer pool. Risks may evolve over time as a venue's business model and/or customer 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 at higher-dollar values. Accordingly, larger gaming venues will likely need more AML/BSA compliance procedures than smaller dollar volume casinos.

Nevertheless, smaller volume casinos must be alert to a patron's departure from ordinary patterns of play and the 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, offering safe 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 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 Compliance 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 make money laundering more likely. For example, if a game allows patrons to bet either side (e.g., baccarat, craps, or roulette), confederated patrons might bet both sides in order 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 sports book on behalf of an unidentified third party, concealing the origin and owner of the funds or betting on both sides of the line.[9] 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 the poker tables may occur between customers, rather than with the casino. Accordingly, the casino may be less likely to detect potential suspicious activity because poker—unlike table games, race and sports book wagers, or electronic games—does not afford the casino the ability 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.

COUNTRY RISK

Some patrons with casino accounts 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 defined by the United States as jurisdictions of concern for narcotics trafficking, human trafficking, money laundering, terrorism, or other forms of illicit finance, or if the foreign nation has been identified as high risk requiring a call to action or as subject to increased monitoring because of deficiencies in its AML regime by the Financial Action Task Force (FATF), or if the foreign nation has been identified by Transparency International or a similar reputable organization as having a high level of public corruption.[10]

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

MONEY BROKERS

Capital flight restrictions (currency controls) in countries such as China and others 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 United States to offer illicit cash brokerage service to Chinese nationals traveling abroad. The broker offers cash in the United States in exchange for a domestic transfer in the customer's home country. Money remitters outside the United States may offer foreign exchange services to avoid currency restrictions and could make payments to casinos by wire on behalf of casino customers.

[9] See FinCEN Correspondence with the American Gaming Association Regarding Sports Betting Conducted on Behalf of Third Parties, https://www.fincen.gov/resources/statutes-regulations/guidance/fincen-correspondence-american-gaming-association-regarding. (Jan. 16, 2015).

[10] For example, see the State Department's annual International Narcotics Control Strategy Report (2022). https://www.state.gov/2022-international-narcotics-control-strategy-report-2/#:~:text=The%202022%20International%20Narcotics%20Control,trade%20in%20Calendar%20Year%202021, and announcements by FinCEN on FATF actions with respect to specific jurisdictions. (March 10, 2022). https://www.fincen.gov/news/news-releases/financial-action-task-force-identifies-jurisdictions-anti-money-laundering-and-1.

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.

POLITICALLY EXPOSED PERSONS

Also known as Senior Foreign Political Figures, Politically Exposed Persons (PEPs) are individuals who have been entrusted with a current or past prominent public function, or 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. A casino may need to conduct open source research to identify PEPs. A casino operator may opt to use a commercial service or third-party provider to identify PEPs. Online operators should perform PEP screening as part of onboarding and periodically thereafter.

PATRON BEHAVIORS

Unusual patterns of patron behavior on the gambling floor may suggest the risk of money laundering. For example, a patron may:

- Increase betting or financial transaction activity significantly without explanation.
- Appear to be coordinating their gaming with another patron or patrons (e.g., passing chips or cash back and forth) in an attempt to evade notice.
- Abruptly change the methods they use for bringing money into or out of the casino.
- Unexpectedly use multiple sources or multiple destinations for funds.
- Request multiple monetary instruments for a jackpot or wager win.
- Wagers on both sides of a transaction in ways that are not explainable as “hedging”
- Makes wagers and almost immediately cashes out.
- Demonstrate no concern for the tax consequences of uncarded play, which may generate large documented “income” that is not offset by losses.

Casinos should also be attentive to the influence and impact of Third-Party Marketing Programs and relationships. To the extent such entities may bring a meaningful number of patrons to a casino property, casinos should undertake review of the marketing entities’ practices and procedures and conduct appropriate due diligence on third party marketers or firms.

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, 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 potential suspicious activity.

Some or all of these behaviors or practices may be entirely legitimate, but casinos should be attentive to the risk that they are not. Many of these considerations are detailed further in later sections of this document.

In addition, the U.S. Department of the Treasury noted in its 2015 National Money Laundering Risk Assessment, that money laundering activity at a casino most often involves exactly the same activities – gambling and spending money – that all casino patrons engage in.[11]

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. The result of the monitoring will be investigated by Compliance to determine whether SARs should be filed.

PATRON CHARACTERISTICS

In some instances, a casino may learn information from any source about a specific patron which warrants further inquiry or examination of the patron's transactions. Examples of such information include formal actions against the patron by law enforcement agencies, public reports of negative information concerning the patron's integrity, source of funds, or evidence that the patron is under investigation by law enforcement. In addition to inquiries from law enforcement and regulators, 314(b) requests from other financial institutions may indicate that a casino should conduct additional due diligence on a specific patron or group of patrons. The results of the review should be documented and maintained in the casino's records.

When such is identified about a patron, casinos may wish to review any previous transactions with the patron that may appear suspicious in light of the newer information and file additional SARs or amend previously filed SARs as warranted if suspected illegal activity was conducted through the casino of the patron had an illegal source of funds for gaming. Casinos may also determine to review such patron's future activity, if any, after a prescribed period of time (e.g., 90 days).

In addition, information about the patron's financial situation may be relevant (to the extent known by the casino), including (as examples) the presence of IRS tax liens or personal bankruptcies in recent years. Casinos should also work to ensure they are consistently evaluating 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 an SAR unless there is a suspicion that the person's source of funds for gaming was illegal activity or the casinos was used for an illegal purpose.

Because all of these criteria are necessarily general, individual casinos have adopted a range of implementation measures and guidelines that aim to detect, block, and report efforts to present illicit funds at casinos.

The following discussion of available compliance techniques should not be viewed as mandatory for every casino. Variations in patron mix, games offered, volume of gaming, location of casino operation and many other factors may render some steps listed below less applicable to a specific casino or may warrant measures in that casino that are not identified in this document. A discussion of risk assessment factors for casinos (FIN-2010-G002) appears at the FinCEN website, www.fincen.gov, along with responses to Frequently Asked Questions.

[11] U.S. Department of the Treasury, National Money Laundering Risk Assessment, https://home.treasury.gov/system/files/246/National-Money-Laundering-Risk-Assessment-06-12-2015.pdf, page 75, (June 2015).

RISK ASSESSMENT

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 Customer Due Diligence (CDD) review, that a customer 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 customers with ties to state-legal marijuana related businesses and whose source of funds for gaming may be from these businesses.

CRYPTOCURRENCY

Cryptocurrencies use blockchain technology as a means of decentralized record-keeping 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. Suggested best practice is to require any virtual currency to be converted to US dollars prior to usage for gaming at a slot machine, table game, sports book, or other gaming area. By requiring virtual currency to be converted to US dollars prior to usage for gaming, it will be subject to the same Currency Transaction Reporting and Suspicious Activity 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 anonymous legal entities to promote money laundering and other illegal activity. 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 United States. FinCEN has taken measures to address this risk. In 2018, FinCEN's Customer Due Diligence or CDD Rule became effective requiring banks and certain other financial institutions (not casinos) to obtain beneficial ownership information on legal entity customers. Under the AMLA, FinCEN is in the process of developing a non-public database with beneficial ownership information on corporations and LLCs organized under state law.

Acceptance of payments for gaming or casino debt from legal entities on behalf of customers or other third party payments poses a money laundering risk for casinos. Casinos may have policies that allow payments from operating businesses that are documented to be related to, or owned by, the customer or from relatives of the customer. Acceptance of payments from other persons, or third party legal entities, including from corporations, partnerships, LLCs, and other similar entities are of a concern and should be generally prohibited. To the extent a casino allows third party payments, the casinos should understand and document the nature of the relationship between the customer and third party.

CASHLESS WAGERING ACCOUNTS (DIGITAL WALLETS)

Cashless Wagering Accounts, sometimes also referred to as Digital Wallets allow for cashless gaming on the Casino Gaming floor. Wagers can be placed with a mobile device with access to the patron's wagering account. A patron's identity is confirmed and each transaction creates a digital record.

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. Cashless Wagering Accounts allow customers to load cash into an account and use those funds for gaming at Slot Machines, Table Games and other locations as determined by the casino operator and the functionality of the Digital Wallet.

Cashless Wagering Accounts may be associated to a customer's Player loyalty account with the casino. Best practice is to only allow accounts to be associated to one user. The casino should take reasonable precautions to assure accounts are not shared by multiple customers. The Customer Service Agreement should require customers to agree that the account is for personal use only.

As transactions conducted are non-cash, Currency Transaction reporting requirements do not apply to gaming transactions conducted using Cashless Wagering Accounts. As such, an operator should implement adequate procedures to review transactions using this payment method for Suspicious Activity. Wagering Account deposits and withdrawals in cash are still subject to CTR requirements when they occur on casino premises.

Funding sources may include online transfers from bank account, credit/debit card, deposit with a cashier within the casino and others. Transforming 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 Cashless Wagering Account should be confirmed to be used for a gaming purpose. A reasonable, risk-based review process should be put in place to detect customers that frequently make deposits and withdrawals without associated gaming activity. Such instances should be considered for SAR filing.

ONLINE GAMING

Online gaming has many of the same risks associated with in-person casino gaming. Online operators may be held by FinCEN to the same reporting requirements for reporting suspicious activity under Title 31/BSA/AML laws depending on forthcoming FinCEN guidance.

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, identification issues etc. Additionally, prior to signing up for an online gaming account, new customers should be subject to identity verification as well compared against the Office of Foreign Asset Control and SDN sanction lists. If a customer 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 to 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 bet operators should establish tools to mitigate such fraud which may include the methods described under "Preventative Steps" section of this document.

BSA/AML COMPLIANCE OFFICER

As required by federal BSA regulations, at least one employee at a casino must be designated as responsible for 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 BSA/AML compliance officer or have another title/duties (for the purposes of this document the employee with the BSA/AML responsibility on property shall be referred to as the BSA/AML compliance officer).

The BSA/AML compliance officer should be well-versed on the casino's products, services, customer 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 compliance officer understand how BSA-required reports are used by law enforcement agencies and act as a liaison (partner) with those agencies. The compliance officer should be the designated point of contact for any AML/BSA related exams, audits, and law enforcement inquiries.

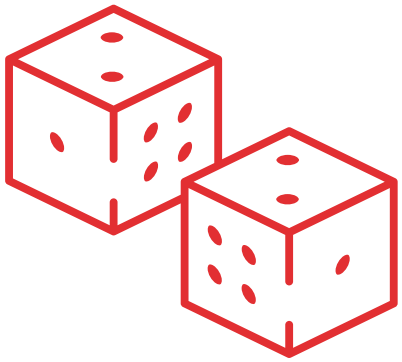
In addition, to ensure that the BSA/AML compliance officer has the necessary independence to execute their responsibilities, they should report to, for example, the General Manager, Chief Legal Officer, Chief Risk Officer, Chief Compliance Officer, or executive of comparable stature. Property-level leadership with oversight of BSA/AML programs should themselves have a direct reporting line to the centralized corporate compliance department, if applicable. All compliance-related reporting lines within the organization should be clearly delineated and identified to employees. The corporate board of directors, or relevant committee, should also receive routine briefings on the BSA/AML program and any material changes.

The BSA/AML compliance officer, along with the AML 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 BSA/AML compliance officer should have sufficient stature in the organization to be a member of, or otherwise be able to regularly brief, senior leadership. The BSA/AML compliance officer should be senior enough to effectively promote the culture of compliance at all levels of the organization.

EMPLOYEE TRAINING

Ongoing training on AML procedures and BSA compliance requirements should be provided to employees who deal with customers or conduct, assist with or review patron transactions that may be subject to the BSA. The extent and intensity of the training should vary according to the responsibilities of the employee but should address CTR and SAR reporting, how those reports are used by government agencies, and the casino's AML Program. Training should be department specific, so that the trainee understands their role in the overall AML program's success and how the particular transactions that they themselves conduct fit in. Trainees should gain an understanding of the types of transactions they will be responsible for, and how they can be exploited in an attempt to launder money. Trainees should be well-equipped to identify red flags, know the procedures, understand confidentiality, and have the tools for reporting such behaviors.

Employees that may encounter a transaction governed by the BSA should receive training before functioning in a capacity alone when newly hired or promoted, and an ongoing annual basis. Training may take place more frequently if changes in the law or circumstances require it. Training should be appropriate for the level of seniority and responsibilities of employees and management.



Consequently, senior level officials/executives should receive different AML training than frontline supervisors and employees. On the job training is also an important component and provides real life context to supplement official training materials.

The responsibilities of more senior personnel may tend to involve more oversight and assessment of risk so AML training should be tailored to these roles. For frontline supervisors and employees, a testing component should be incorporated into the training to ensure comprehension and a signed acknowledgement form agreeing to comply with company BSA/AML policies.

A casino should tailor its training program to employees who would be in a position to observe potentially suspicious activity or directly handle patron transactions, consistent with the risks

Training materials should be updated regularly to reflect regulatory and enforcement developments under the BSA. If such regulatory developments warrant a revision in the casino's compliance practices, relevant personnel should receive information on a timely basis about those developments and any revised casino practice.

EMPLOYEE TRAINING

identified in the risk assessment. At a minimum, training should extend to the following general categories of employees as applicable:

- Those engaged in the operation of casino games (table games, poker, slots, keno and bingo, and race & sports), at least beginning 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 frequent direct contact with patrons, including domestic and international hosts, branch office employees, and special events employees;
- Cage employees;
- Credit & collections employees;
- Surveillance employees;
- Property compliance and AML compliance employees;
- Audit employees, including Internal Audit and Fraud Department employees; and
- Senior gaming management, Board of Directors, Audit Committee or Compliance Committee.

Training on BSA/AML policies and Form 8300 reporting for non-gaming employees (high-end retail, night clubs, convention sales, hotel and food and beverage) may be incorporated into their respective job training, as necessary.

The casino's AML compliance performance, as well as the compliance actions of individual employees, should be a factor in performance reviews of those employees involved with BSA compliance. These factors should be considered in calculating compensation and bonuses, and in determining any negative personnel action, including performance improvement plans through to termination from employment.

PREVENTIVE STEPS

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 business profile and customer base; geographic location; financial services offered; and product offerings.

Some examples of such policies and procedures may include:

- Requiring that "ticket-in/ticket-out" (TITO) redemptions at self-service kiosks be capped at an amount below $3,000 determined by the risk assessment for such transactions at that casino and monitoring to identify TITO redemptions of multiple tickets below $3,000 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.
- Declining to accept cash to purchase a casino check or other monetary instrument or to 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.
- Concern would be heightened with respect to checks or wire transfers which originate from a labor union, charitable/non-profit organization or foundation, law firm (including from a Interest on Lawyer's Trust Account ("IOLTA")), accounting firm, or any type of trust account. A casino may determine to reject and/or reverse such checks and wire transfers and consider filing SARs on the payment.
- Issuing casino checks and wires to a patron only for the amount of his/her winnings (e.g. the remaining funds from a check or wire which already has been accepted).

PREVENTIVE STEPS

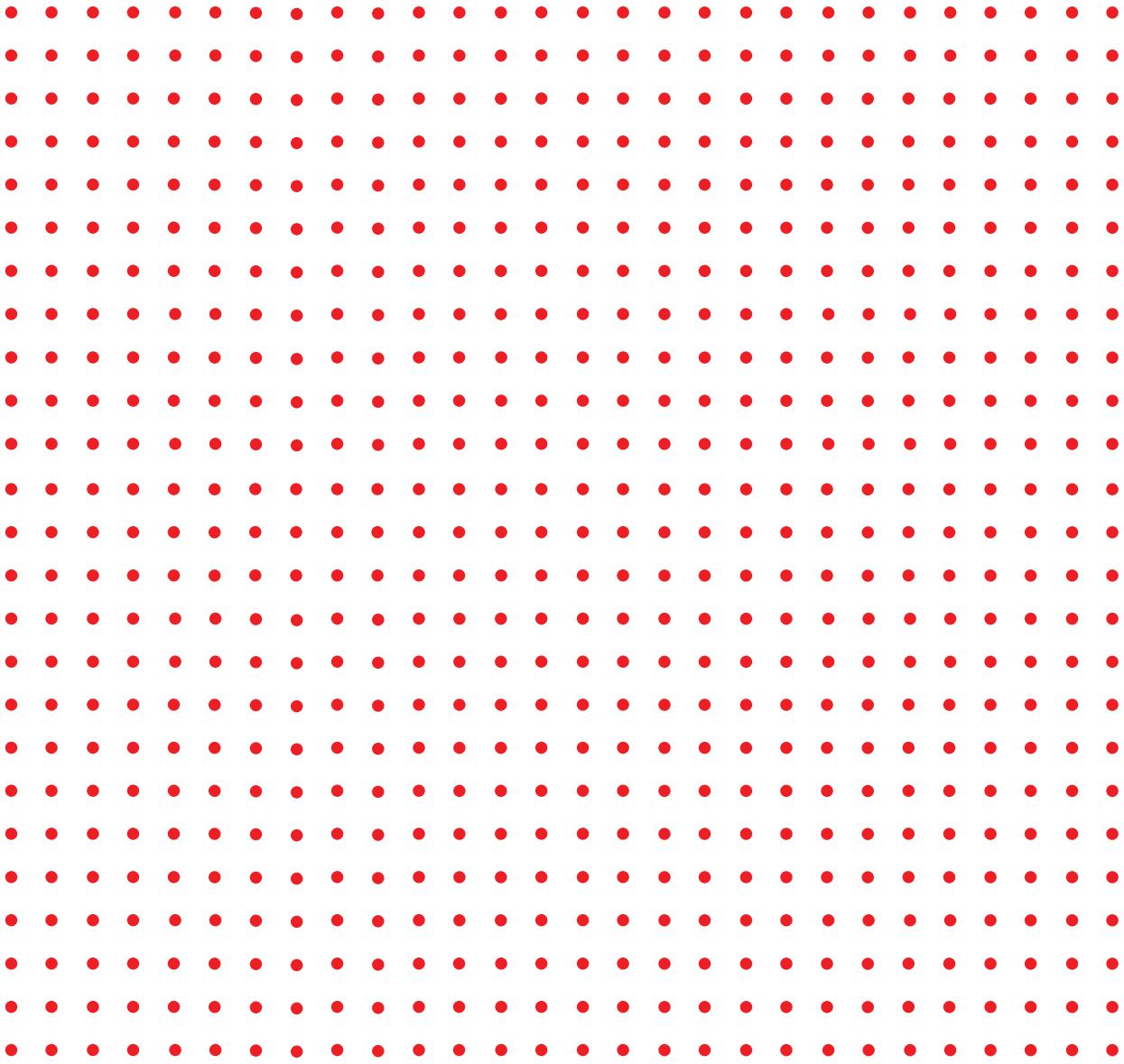
- A check for winnings should be payable only to the patron, and a wire transfer should be made only to the patron's account or, if applicable, to the account from which the originating wire was received. Similarly, if there is a return of front money paid by wire transfer, it should be wired back the 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 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 be considered. In such instances, the patron will be prohibited from further gaming and may be prohibited from the redemption of complimentaries. Senior management should have discretion on such matters if the patron is cooperative, the complimentaries were already earned, and the expectation is that acquisition of verifying identification will be facilitated by maintaining the patron relationship.
- 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.
- Additionally, all traveling marketing executives, prior to travel outside the U.S. 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.

Online operators should consider the following, among other things:

- Requiring that accounts from which patrons deposit and withdraw funds match the name of the accountholder;
- Where possible, return funds by the method paid;
- Analyzing customer activity for evidence of account sharing or attempts at evading/ manipulating geolocation;
- Monitoring customer activity for evidence of deposits and withdrawals without legitimate wagering activity; and

PREVENTIVE STEPS

- Searching player databases for:
  - Multiple players with using similar user names and email addresses
  - A large number of players geolocating at a similar residential location
  - Multiple players using a shared device
  - Analyzing player accounts with multiple payment methods and consecutive deposits.



KNOW YOUR CUSTOMER (KYC)

In addition to comply with the BSA reporting and recordkeeping requirements, as part of their AML programs, casinos are expected to maintain risk-based KYC programs with procedures for conducting KYC reviews of certain customers. The reviews generally will consider the customer's gaming activity, history and consider whether the person has a legitimate source of funds to support the level of play and that there is no negative information that supports a suspicion that person's source of funds for gaming may be the proceeds of illegal activity. As discussed below KYC reviews may encompass a casino's largest players and players that present elevated AML risk. KYC reviews may result in possible SAR filing or, in extreme cases, possible consideration of termination of the customer from further business with the casinos and its affiliates. Procedures should include when KYC reviews will be conducted and what reviews will entail on a risk basis customer identification is one of the building blocks for KYC.

PATRON IDENTIFICATION AND VERIFICATION

No front money or marker limit/credit account or safety deposit box agreement will be opened, nor will any transaction involving such services be conducted, unless the patron provides a full name, a permanent address and (for U.S. citizens) a Social Security number (as required by law or regulation). On a risk basis, casinos should obtain additional information depending on the risk presented by the patron and product or service.

For example, in some situations, the casino could consider obtaining additional information, such as occupation, employer, business affiliations, and bank account information. In addition, on a risk basis, casinos should perform an appropriate amount of due diligence to verify information provided by patrons. Procedures should specify when occupation information will be obtained. This requirement does not apply to the establishment or use of player loyalty club accounts.

No transaction(s) known to be reportable under the BSA or AML procedures will be completed or accounts opened unless the individual conducting the transaction(s) provides valid, current, government-issued photo identification, including government-issued Real IDs or digital IDs, and a permanent address.

If the patron asserts that his 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.

Examples of acceptable government-issued photo identification are:

- Driver's License[12]
- Passport
- Alien Registration Card
- State Issued Identification Card (including Real IDs)[13]
- Tribal Identification Card

[12] This does not include "driver authorization" cards or international driver's licenses/permits, which are not an acceptable form of identification.
[13] 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.'

VERIFICATION

DOCUMENTARY REVIEW

Other than a Driver's Authorization Card, for in-person transactions, a casino generally may rely on viewing government-issued identification as verification of a customer'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 customer'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. The reason for using an address other than one on the customer's government-issued ID should be maintained in the casino's records.

If the patron is a U.S. citizen, or a U.S. resident a Social Security number is required for certain transactions including CTRs and taxable events. Patrons may verbally provide a Social Security number. In such cases it is recommended that the patron complete a W-9 to attest to the validity of a verbally provided Social Security number. If the casino knows or has reason to believe that a previous Social Security number 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 a Social Security number when one is required, the casino must not complete any pending reportable transaction with that patron or open an account for that patron. If the patron has exceeded the reporting threshold for a CTR without providing a Social Security number, a casino employee will attempt to acquire that information from publicly available information. Declining to provide a Social Security number may warrant completion of a SAR for the incident, particularly if a pattern has been observed.

> If the patron does not provide proper identification and/or required information, the casino should not engage in transactions with that patron and the patron should be barred from further gaming activity until satisfactory identification and/or the required information is provided. Documentation of the incident should be added to the patron's account in the management information system.

NON-DOCUMENTARY REVIEW[14]

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 the ID is verified by documentary review as described above.

In most cases however, such accounts are established remotely though the internet, so it is not possible to verify identity through the in-person review of physical documentation. In such

[14] Financial Crimes Intelligence Network, Exceptive Relief for Casinos from Certain Customer Identification Verification Requirements, FIN-2021-R001 (Oct. 19,2021). 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.

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 social security number. Some operators may also require the submission of a photo or scan of a government-issued ID and in some circumstances, may require the download of selfie of the patron applying. This information is then independently verified through a comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other 3rd party electronic ID verification services. If the patron's identity cannot be reliably verified, the operator will deny the creation of an online wagering account until such time as sufficient additional documentation is provided that can be reliably verified.

CURRENCY REPORTING

The same patron identification requirements apply to any person(s) who, acting as an agent(s) for another person, performs transactions on behalf of that patron, and to any person who performs transactions in conjunction with that other patron, if the transactions trigger a CTR filing. Casinos should include all readily available patron information on CTRs.

In those circumstances, both the person(s) conducting the reportable currency transactions as well as the person on whose behalf they are acting must provide the identification and required information described above.

If an individual cannot provide the identification and/or required information, that individual will be barred from further gaming activity, and the casino will consider filing a SAR.

For purposes of currency reporting, independent agents that contract with the casino are agents for the patron and not the casino if that designation has been established in the independent agent agreement. Independent agents should acknowledge, in writing, the responsibility of the casino under the BSA and the casino's obligations to report suspicious activity and agree to report to the casino any suspicious activity they become aware of.

SANCTIONS

Although separate from BSA/AML requirements, casinos should check whether patrons and related entities appear on the list of "Specially Designated Nationals" maintained by the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury.[15]

Since it is not practical to perform an OFAC review of every retail casino patron, due diligence may be conducted on a risk basis and should encompass procedures for checking against updates to the OFAC list. Examples of potential high risk customers would be significant players with a residence in a country known to be hostile to the interests of the U.S. Government or sanctioned by the US. Additionally, significant players who are from a country with a high incidence of drug trafficking or terrorist activity should also be screened. Casinos should also consider their SAR reporting obligations and how they intersect with OFAC requirements.

[15] 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.

KNOW YOUR CUSTOMER (KYC)

Online operators should screen customers for sanctions purposes at the time of onboarding as well as at regular intervals thereafter. Furthermore, online operators should leverage advanced geolocation at account opening, deposit and withdrawal and for transaction monitoring to ensure that patrons are not residing in OFAC sanctioned countries or high risk jurisdictions. This will further decrease the risk of proxy betting as well as heighten AML and CFT compliance. A risk based approach to the use of "fuzzy" matching logic should be used to limit the occurrence of false positives.

Some OFAC sanctions programs prohibit transactions with certain foreign jurisdictions or regions and individuals ordinarily resident in those jurisdictions. Casinos should not open accounts for, or conduct transactions with, customers who provide addresses in Iran, Syria, Cuba, North Korea, or the Crimea, Luhansk or Donetsk regions of Ukraine. As with persons on an OFAC list, any funds on account for them or winnings due should not be paid.

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

- Management commitment;
- Risk assessment;
- Internal controls;
- Testing and audit; and
- Training[16] - appropriate employees will be trained on OFAC compliance responsibilities.

ONGOING AND ENHANCED DUE DILIGENCE

The casino's compliance policies should be calibrated to increase scrutiny of customer 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 high-volume patrons, whose activity (in terms of bills-in, marker play, or total play) exceeds a level determined by the risk assessment for that casino or who are otherwise identified as posing a high BSA/AML risk, the casino should review the patron's identity against public records and third-party database(s) to determine whether that person (or related entity):

- Is a Politically Exposed Person ("PEP");
- Is the subject of negative reports concerning possible criminal activity or doubtful business practices; or
- Has a prior criminal history, relevant to AML risk.

For high-volume patrons, high-loss patrons, or transactions identified as possibly posing a high BSA/AML risk, the casino also may need to assess the source of the funds being used by the patron for gaming and whether they may derive from illegal activity or from legitimate sources adequate to support the level of play.

This may require the casino to obtain information concerning the patron's gaming history and financial and business circumstances. In addition

[16] For more information on OFAC compliance, consult the OFAC publication, "A Framework for OFAC Compliance Commitments" (May 2, 2019). https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf.

to querying available databases, leveraging information-sharing arrangements with other financial institutions, or asking the patron, the government's program under Section 314(b) of the USA PATRIOT Act is a critical tool to obtain more information and reach judgments on whether the patron:

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

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, the listing of "Specially Designated Nationals" of the Office of Foreign Assets Control (OFAC), 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.

The COVID-19 Global Pandemic introduced new elements for consideration when assessing the effectiveness of the casino's AML Compliance Program and Risk Assessment. Fraud related to Paycheck Protection Program (PPP) Loans as well as Unemployment Insurance contributed to an overall increase in Suspicious Activity during the pandemic. It is reasonable to expect that similar increases in fraud will follow any additional government release of stimulus or support payments. Casinos should consider whether a customer previously received government funds when conducting KYC due diligence or SAR investigations and whether those funds may have been fraudulently obtained and used for gaming. If detected, such instances should be reviewed for potential SAR filing.

Further due diligence may be warranted if the casino has information indicating that the patron:

- Has financial fiduciary obligations (e.g., trustee, accountant, attorney, nonprofit/charity executive) that may create a risk of misappropriation or other illicit financial activity;
- Is associated with individuals or entities known to be connected with the illicit generation of funds, including unlawful gaming;
- Claims connections with businesses that have no actual operations;
- Proposes transactions with entities of unknown ownership or control;
- Is the subject of substantial tax liens, or has gone through a recent personal bankruptcy proceeding;
- Patron may have ties or be affiliated with a state licensed and regulated marijuana related business;
- Otherwise may present an unacceptable risk of money laundering or violating the casino's AML policies; or
- Is a Politically Exposed Person (PEP).

POTENTIAL SUSPICIOUS ACTIVITY

The BSA requires casinos to file a suspicious activity report (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; or
- Is not the sort in which the particular 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. Casinos should also actively use the 314(b) program to obtain information about patrons which may be used to evaluate potential suspicious activity.

Casinos also should consult with the FinCEN guidance in FIN-2008-G007[17], which discusses "red flags" for suspicious activity at casinos. 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 and BSA violations and other criminal activity involving casinos and their patrons. The list should be updated as needed and included in training Casinos should also 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, including interactive gaming, and all gaming verticals. Casinos should 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.

It is important to maintain a consistent approach to the decision-making around SAR investigations and filing, and to ensure such decisions are aligned with the casino's risk profile. In addition, it is vital to memorialize investigations of suspicious activity, and decisions around filing SARs (including in cases in which the casino decided not to file a SAR). Policies/procedures should include variety of potential suspicious activity examples for team member awareness and included in department specific ongoing training. Compliance should be monitoring industry news for awareness in order to implement risk mitigation measures as needed to minimize exposure.

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

[17] See, Financial Crimes Enforcement Network, Recognizing Suspicious Activity – Red Flags for Casinos and Card Clubs, FIN-2008-G007 (July 31, 2008), https://www.fincen.gov/resources/advisories/fincen-guidance-fin-2008-g007.

POTENTIAL SUSPICIOUS ACTIVITY

GAMING FLOOR ACTIVITY

- Minimal gaming despite large financial transactions with the casino;
- Structuring of transactions to stay at or slightly below the $10,000.00 reporting threshold for CTRs;
- Placing currency in a slot machine, then cashing out after minimal or no play and redeeming the ticket in ticket out (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 pass 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 identity and/or evade reporting requirements;
- A patron leaves the casino floor with a significant amount of chips in his possession 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 with a safe-deposit box connected to the poker room accesses that safe-deposit box with a frequency that is disproportionately high when compared to the time and frequency of his or her poker play.
- A patron identified as loan shark is observed approaching patron(s).
- Patron is observed requesting large amounts of cash from ATM but has no gaming activity; or
- Patrons who visit the casino with a group (that may arranged by an independent agent registered with state regulatory agencies) need to be identified so that available funds for each patron are accurately reflected in the patron management system and the play of each patron is recorded as warranted.

RACE AND SPORTS BOOK ACTIVITY

- Inquiring with race and sports book 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 aggregate, would have exceeded the thresholds on one ticket;
- Behavior that may be indicative of coordinated betting (or betting on both sides of a game or an event) among related parties for purposes of laundering the funds;

POTENTIAL SUSPICIOUS ACTIVITY

- Indications of insufficient wealth or income to support betting patterns;
- Significant changes in wagering patterns or unusual spike in play that is 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 but in 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, if fraud or identity theft is discovered;
- Unusual wagering activity that appears to lack any legitimate economic purpose;
- Significant changes in wagering patterns or unusual spike 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 geo-location data, such as traveling between jurisdictions in a relatively short period of time or multiple attempts to anonymize the geolocation; and/or
- Deposit(s) to a gaming account 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/non-profit 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 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;

POTENTIAL SUSPICIOUS ACTIVITY

- A patron deposits large sums of cash into a front money account but the 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 to 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 which the casino has a basis for suspecting to be the proceeds of illegal activity;
- A patron requests cash advance from credit card that has been identified as possibly fraudulent;
- Patron uses multiple credit cards to request cash advances.
- Patron is observed requesting large amounts of cash from ATM but has no gaming activity;
- A patron presents funds in any form that derive from a foreign jurisdiction declared by the United States 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;[18]
- 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 related to gaming; or
- 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;
- Patron is the owner of a business, the nature of which has been profiled by the Federal Trade Commission as high risk for fraud schemes;
- Patron is an owner, employee or is otherwise associated with a marijuana related business;
- A patron raises his or her financial transactions to levels well above the ordinary levels for that patron with no reasonable explanation; or
- 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.[19]

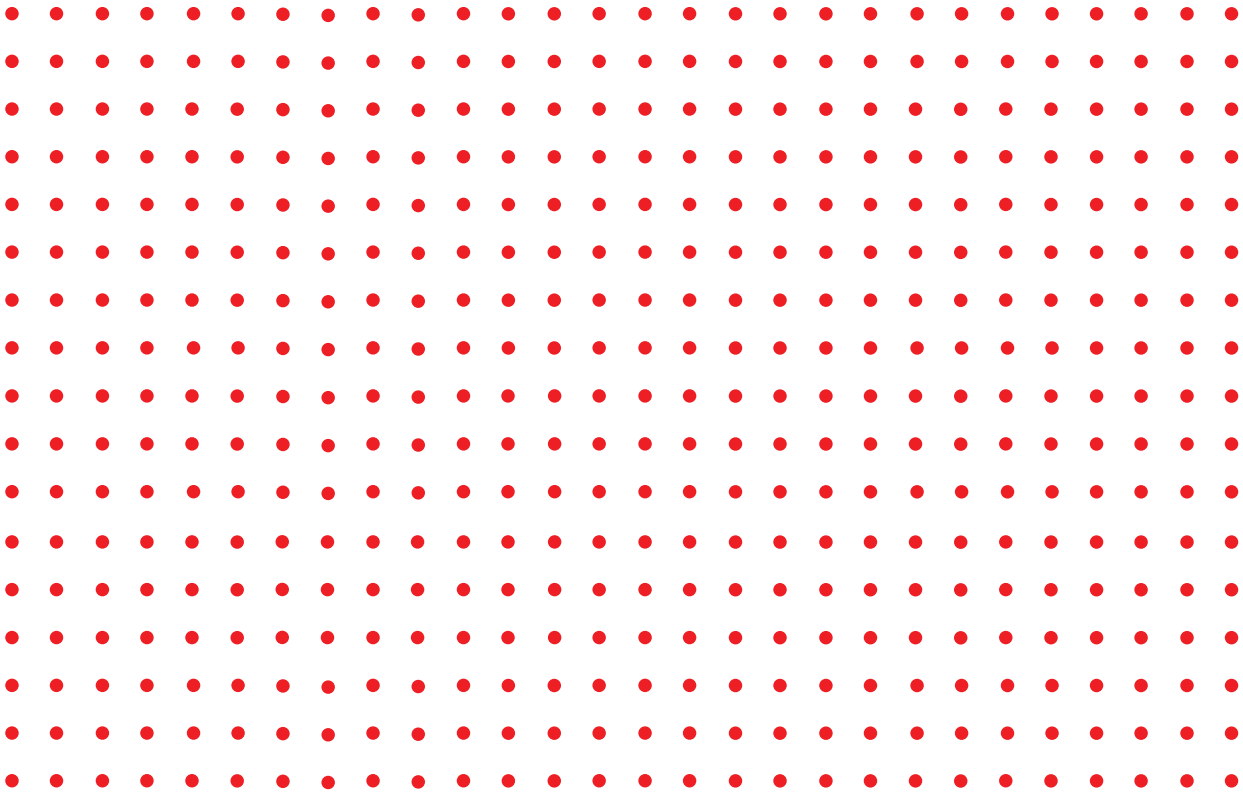
This list is by no means exhaustive; other patron activities may trigger BSA/AML concerns due to the circumstances in which they arise. Each casino should develop its own scenarios tailored to its business.

[18] For example, see the State Department's annual International Narcotics Control Strategy Report (2022) https://www.state.gov/2022-international-narcotics-control-strategy-report-2/#:~:text=The%202022%20International%20Narcotics%20Control,trade%20in%20Calendar%20Year%202021. and announcements by FinCEN on FATF actions with respect to specific jurisdictions (March 10, 2022), https://www.fincen.gov/news/news-releases/financial-action-task-force-identifies-jurisdictions-anti-money-laundering-and-1.

[19] Please see, Financial Crimes enforcement Network, Advisory to Financial Institutions on Cyber – Events and Cyber – Enabled Crime , FIN-2016-A005, (October 25, 2016), https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf.

POTENTIAL SUSPICIOUS ACTIVITY

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 customer to circumvent internal policies or ordinary practices, or an employee's violation of casino policies and procedures.



TRANSACTION MONITORING

Transaction monitoring provides comprehensive and consistent risk-based monitoring of customer transactions, activity, and behavior, enabling the casino to better detect and report suspected money laundering activity. Transaction monitoring scenarios can be developed based on the company risk profile, with specific thresholds related to gaming activity that will generate suspicious activity alerts when those thresholds are triggered. On a regular basis, a dedicated compliance team will complete a review of those transactions alerted at or above thresholds, reviewing all customer information available. In doing so, the compliance team may request additional customer data held by relevant casino departments and functions to facilitate a proper investigation. The sharing of information between these departments and functions is integral to performing accurate investigative analysis on potential suspicious activity

As warranted by the nature of the investigation, the compliance team may utilize third-party databases (e.g. Lexis Nexis, WorldCheck, etc.) to gather and review additional information, such as the patron's professional/work experience, source of funds, business connections, criminal history, etc. This information will assist in performing the investigation and understanding the patron's behavior/transactions. It will also assist in determining an appropriate course of action (i.e. disposition), such as requesting the source of funds, filing a SAR, and/or terminating the relationship, among other dispositions.

Transaction monitoring scenarios and circumstances warranting such review may include the following:

BRICK AND MORTAR TRANSACTION MONITORING

- 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 withdraw (of the same or similar amount);
- Patrons with large cash-out transactions (in the aggregate) with little or no CTR "out" filings;
- Patron 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 with cash transactions, such as deposits or withdrawals, including aggregated transactions, that are just below the CTR reporting threshold;
- Patron using a wagering kiosk 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 (TITO), in a short period of time, at the same (or adjacent) redemption kiosk not associated to a player's card account;

- Checks or wire transfers received for the benefit of the 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 date;
- 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 extended period of times; or
- Patrons that pass winning tickets to others to cash out.

Compliance personnel can take additional measures to identify potential suspicious activity, such as reviewing relevant daily audit summaries, logs and reports, such as marker summaries, front-money/safekeeping summaries, multiple transaction logs (MTLs), negotiable instrument logs (NILs), check logs and wire reports to identify potential suspicious activity. 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 data should also be considered, if available.

ONLINE TRANSACTION MONITORING

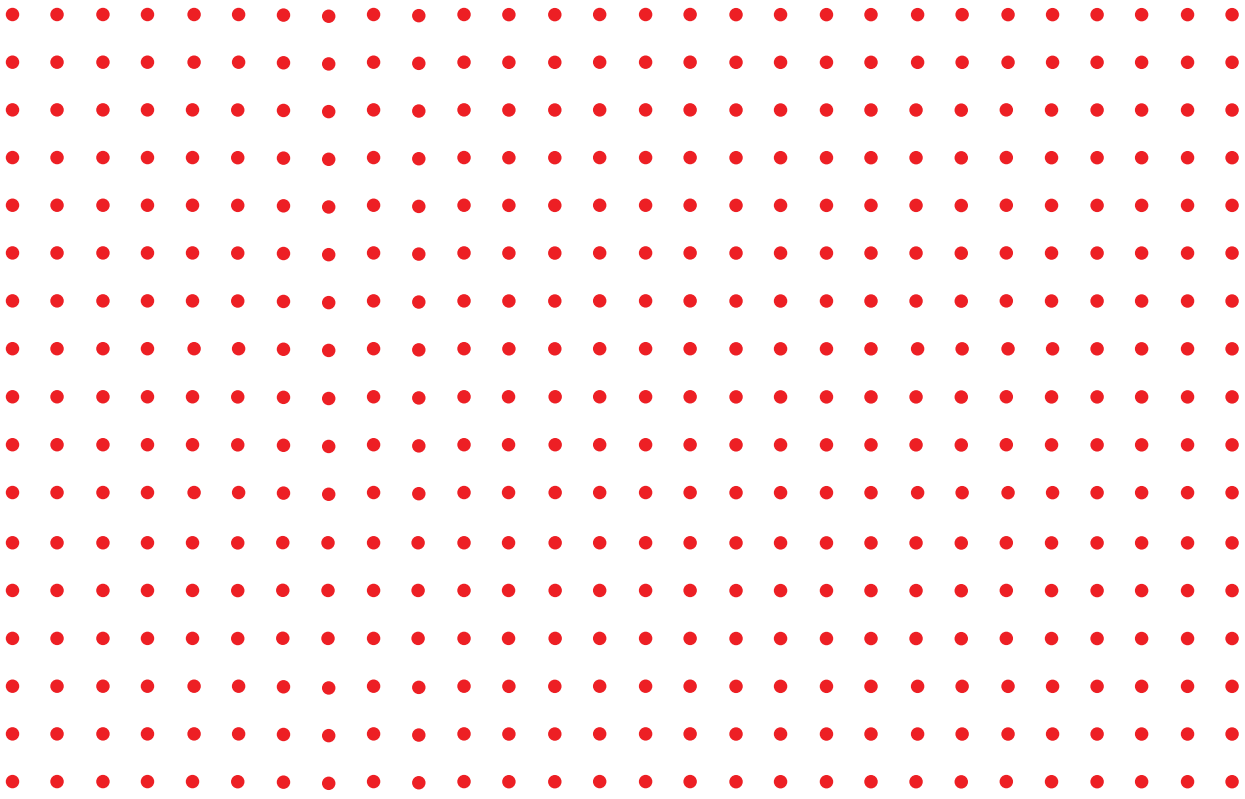
As the gaming industry expands from traditional brick and mortar casinos into the online space with interactive slots, table games, peer-to-peer games and sports wagering, mitigating the risk of money laundering is also expanding. To keep pace with these activities, compliance personnel have broadened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

Circumstances warranting review in the online gaming space (including the use of digital wallets):

- Online cash or digital wallet deposits with minimal or no play followed by a withdrawal request(s);
- Cash deposits and withdrawals from the patron's online account or digital wallet at a casino cage that appear to be circumventing 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;
- Account holder using multiple devices (UUID) or IP addresses;
- Multiple user accounts using the same device (UUID) or IP address, if fraud or identity theft is suspected;

TRANSACTION MONITORING

- Geolocation reports identifying individuals who have violated multiple anti-fraud checks like running fake GPS apps along with having mock location settings enabled or 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 REPORT
REVIEW PROCEDURES

A suspicious activity report (SAR) review or investigation —consists of examining all available information to determine whether a SAR should be filed for the reported incident(s) or not. The reviews may be prompted by direct observations by employees, system alerts, by after-the-fact data analysis performed through back-of-house procedures, or by other means (e.g., incoming law enforcement inquiry, 314(b) requests, or public negative news).

On an annual basis and as part of its ongoing risk a suspicious activity report (SAR) review or investigation – consists of examining all available information to determine whether a SAR should be filed for the reported incident(s) or not. The reviews may be prompted by direct observations by employees, system alerts, by after-the-fact data analysis performed through back-of-house procedures, or by other means (e.g., incoming law enforcement inquiry, 314(b) requests, or public negative news).

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

- Internal Notification: Casinos should incorporate a clear, easy to understand, and prompt internal notification process. This should include the reporting individual providing all available information about the transaction(s) or action(s) (e.g., patron name, Social Security number, player's card number, 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, is crucial in ensuring all information is captured surrounding the activity of the activity.
  - Each department involved should be providing their account of the suspicious activity to allow the individual responsible for further investigation to have a complete picture.
  - Casinos should refrain from naming these internal notifications 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.

SUSPICIOUS ACTIVITY REPORT REVIEW PROCEDURES

- Investigation: The BSA/AML Officer and/or staff should begin their investigation promptly upon receipt of the internal notification. Casinos should have a documented procedure for how potential suspicious activity is investigated. Investigations should include reviewing the following resources where applicable:
  - Player Records (retail and interactive)
  - Player Credit History
  - Prior CTR/SAR Filings
  - Incident Report History (surveillance/security)
  - Internet Searches
  - Employee Statements/Interactions
  - Hotel records (where applicable)
  - Technical Information i.e. geolocation, IP information, etc.
  - If the casino participates in voluntary information sharing under Section 314(b) of the USA PATRIOT Act, it may contact officials at other participating casinos or banks or other financial institutions for additional information concerning a patron's business connections and other relevant matters.
- The purpose of the investigation is to gather a complete profile of the individual(s) to understand any possible logical purpose of the transaction(s)/action(s); potential patterns; or that there is in fact suspicious activity occurring.
  - Regardless of final determination of filing a SAR or not, all investigation materials should be retained for a period of at least 5 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 BSA Officer/ designee or SAR Committee will determine if the information warrants a SAR being filed or not. 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 a determination to 'not file' is made, the reasoning for not filing must be documented and retained. In either event, the designated individual will make a record of the determination and the date the determination was made to file or not file.
- 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 patrons 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 initial detection of potential suspicious activity. Casinos should establish what they consider to be the trigger for starting the clock and apply this consistently.

SUSPICIOUS ACTIVITY REPORT REVIEW PROCEDURES

- Completing/Filing a SAR: The individual responsible for completing the SAR form should ensure that the form is completed correctly and thoroughly utilizing all available information. 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.
  - Refrain from using the SAR subject's name within the filing title of the report to avoid potential disclosure of the individuals identity.
  - A secondary review of the drafted SAR is recommended for completeness prior to filing
- Continuing Activity Reporting: Once a SAR is filed, the individual(s) and the reported activity enter a 90-day review period where casinos should be monitoring the individual(s) for continued activity of the same suspicious activity. If the activity is continued, a Continuing Activity Report should be filed, following the same procedures for the initial reporting.
  - The determination of filing a new SAR or a Continuing SAR lies in the activity of the individual(s). If the same suspicious activity is repeated within the 90-day review, it would be filed as a Continuing SAR. If the individual(s) are involved in a different type of suspicious activity, it would be considered a new filing (with reference to the other SAR within the narrative).
  - 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 continues, this timeframe will result in three SARS filed over a year.

When multiple SARs are filed for a patron's activities, casino management should consider whether the casino wishes to continue its relationship with that patron and document those decisions. If there is an indication that the customer has an illegal source of funds for gaming or is using the casino for an illegal purpose, the 90 day review process generally would not apply and the matter should be escalated for a decision whether to restrict or terminate the customer. In appropriate cases, as in the case of ongoing suspected illegal activity that requires immediate attention, the casino should reach out to the appropriate law enforcement agency in addition to filing the SAR.

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 whether or not a SAR was filed only can be shared with federal, state or local law enforcement and generally with a casino's gaming regulators. Best practice is to require that all SAR requests to be in writing.

SUSPICIOUS ACTIVITY REPORT REVIEW PROCEDURES

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, shall 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 any such request and the response thereto.

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. Conversely however, a casino is not permitted to share a SAR with other government agencies or authorities that may have general oversight, but that do not have express BSA oversight authority. 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.

SHARING SUSPICIOUS ACTIVITY REPORTS

According to FinCEN Guidance[20], 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 United States of either the casino itself or a parent or U.S. affiliate of the casino. SAR information on whether SARs were or were not filed cannot be shared with non-U.S. affiliates of casinos.

In order to assist law enforcement and safeguard the confidential and sensitive information contained in and that support SARs, the casino 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 by the BSA.

[20] See Financial Crimes Enforcement Network, Sharing Suspicious Activity Reports with U.S. Parents and Affiliates of Casinos, FIN-2017-G001 (Jan. 4, 2017), https://www.fincen.gov/sites/default/files/2017-01/FinCEN%20Guidance%20Jan%204_508%20FINAL.pdf.

RESTRICTING / TERMINATING
PATRON RELATIONSHIPS

Based on the result of KYC due diligence reviews of high-volume patrons or of certain events identified by the risk assessment for that casino (e.g., the filing of one or multiple SARs for a patron, negative news, or the receipt of a law enforcement request for information concerning a patron), information received pursuant to a 314(b) request, or the filing of multiple SARs on the same individual, the casino may consider whether to terminate or restrict its relationship with a patron.

Law enforcement may utilize a specific request to "keep open" accounts and/or request casinos to maintain customer relations as part of their efforts to identify and combat money laundering, terrorist financing, and other illicit financial activities.

Law enforcement[21] "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.

While casinos generally will endeavor to accommodate keep open requests, casinos are not obligated to agree to do so. The decision to maintain customer relationships, keep open accounts, and/or terminate either, is ultimately up to the casino. 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 casino agrees to "keep open" the account/customer relationship as requested from law enforcement, including requirements for risk based monitoring and SAR filings as well as confidentiality.

- While multiple SAR filings on the same patron is one factor as to whether a relationship should be terminated or not, other factors such as the severity of the conduct must 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, but decisions on restrictions or terminations may be made where the activity is suspected and not confirmed depending on the facts and circumstance. The

[21] See Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation,Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency, Answers to Frequently Asked Questions Regarding Suspicious Activity Reporting and Other Anti Money Laundering Considerations, (Jan, 19, 2021), https://www.fincen.gov/sites/default/files/2021-01/Joint%20SAR%20FAQs%20Final%20508.pdf.

RESTRICTING / TERMINATING PATRON RELATIONSHIPS

greater the likelihood of known criminal activity, the greater the risk to the casino if relationship is not terminated. The assessment process should be documented in policy/procedures for performance consistency along with list of factors that would require the assessment to occur.

To the extent a casino has a BSA/AML exclusion policy, the casino may consider accounting for the following topics:

- Multiple SAR filings on the same patron;
- Severity of alleged criminal activity (e.g., terrorist financing);
- Suspicious versus known criminal activity;
- Use of "all available information";
- Risk to casino if patron is not excluded; and
- Clearly identifies authority to exclude (i.e., BSA Officer and/or Committee).

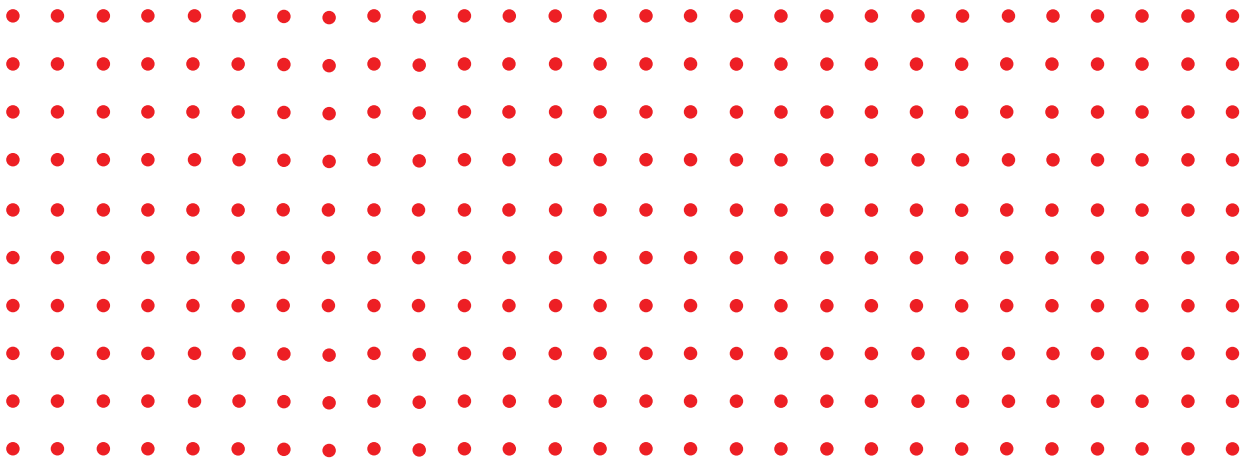
If a committee is used to make exclusion determinations, it should not include anyone with a direct conflict (e.g., Player Development management).

Committee process should be documented in policy/procedures to address the following:

- Composition of the committee;
- How decisions are determined;
- Any process by which the decision can be reviewed or overruled;
- Maintaining the committee review, decision and all supporting documentation per organizational record retention program.

The 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 or the casino's compliance policies. Examples:

- Significant concerns that a patron's source of funds used for gaming stems from illegal activity
- Patron(s) using the casino to facilitate illegal activity.



AUDIT PROCEDURES

The BSA regulations require periodic independent testing of the casino's overall program, as well as specific functions, by qualified independent auditors. Internal auditors who perform the testing should not have any operational responsibilities. Surveillance is typically an integral component of the casino's AML program so their performance of the required audit could be viewed as a potential conflict of interest. Additionally, a regulatory examination of the casino's AML program by governmental authorities does not qualify as independent testing under the BSA.

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

- Customer due diligence;
- Transaction monitoring;
- Required reporting and recordkeeping;
- Training; and
- The AML Officer function.

Independent auditors of BSA/AML compliance may be either external or internal to the casino, depending on the casino's corporate structure and practices. A financial institution's leadership should ensure that the party testing the program (whether internal or external) is independent, qualified, unbiased and does not have conflicting business interests that may influence the outcome of the compliance program test. Safeguarding the integrity and independence of the compliance program testing enables an institution to locate and take appropriate corrective actions to address BSA/AML deficiencies.[22]

The scope and frequency of the testing should be commensurate with the money laundering and terrorist financing risks posed by the products and services provided by the casino.[23] The casino may conduct independent testing over periodic intervals (for example, every 12-18 months) and/or when there are significant changes in the casino's risk profile, systems, compliance staff, or processes. More frequent independent testing may be appropriate when errors or deficiencies in some aspect of the AML program have been identified or to verify or validate mitigating or remedial actions.[24]

[22] Financial Crimes Enforcement Network, FIN-2014-A007 Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance, FIN-2014-A007, (Aug. 11, 2014), p. 4.
[23] 31 C.F.R. § 1021.210(b)(2)(ii)
[24] FFIEC BSA/AML Examination Manual

AUDIT PROCEDURES

If the casino utilizes an internal audit function, that function must be independent from AML compliance, in order to ensure the independence of the internal audit function. Casinos also may consider a reporting process to communicate to the Board of Directors the results of AML independent testing.

The independent auditors should report their findings directly to senior management officials who have the authority to remediate the audit findings and ensure corrective action is taken.

Examinations by the Internal Revenue Service or other governmental authorities will analyze the casino's AML program to ensure that it provides for testing and evaluation for effectiveness by persons independent of the compliance officer.[25]

For each audit finding that raises concerns about the casino's AML program, as well as findings by independent auditors, Internal Revenue Service examiners, or other governmental authorities, the casino should undertake corrective action or make a specific documented determination that no such action is necessary.[26]

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, will review currency transactions by using all relevant records, including but not limited to Multiple Transaction Logs (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.

A detailed audit program should be maintained to document all audit procedures performed by independent auditors.

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; and
- CTRs were electronically filed within 15 days of the transaction date.

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

The Monetary / Negotiable Instrument Log (MIL/NIL) will also be reviewed by independent auditors for proper completion and for retention for at least five years.

A system query should identify those patrons, if any, that completed transaction(s) in currency involving either cash in or cash out more than a 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 onto the multiple transaction log for reporting when required by law.

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

[25] IRS Bank Secrecy Act Examiner Responsibilities 4.26.6.5.1.2 Evaluation of AML Program (3)(d)
[26] Financial Crimes Enforcement Network, Casino or Card Club Compliance Program Assessment, FIN-2010-G003 (June 30, 2010), https://www.fincen.gov/resources/statutes-regulations/guidance/casino-or-card-club-compliance-program-assessment.

AUDIT PROCEDURES

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 test function will establish testing parameters for both SAR and no-SAR decisions. This review will consider the completeness of investigation processes and documentation, timeliness of the review, record retention and safeguards from disclosure.[27] In instances where SARs were filed, the independent auditors will test the completeness of SAR fields and narrative and timeliness of the filing.

This review should also test the casino's monitoring systems and how the system(s) fits into the casino's overall suspicious activity monitoring and reporting process and test the monitoring systems programming methodology and algorithms to ensure the scenarios are detecting potentially suspicious activity.

The independent auditors will test information flow across the casino, including but not limited to the fraud/security and host functions, as well as test whether information regarding employee misconduct is appropriately communicated to the group responsible for SAR decisions.

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, customers, entities, geographic locations volume of transactions, and adequacy of staffing.

[27] See Financial Crimes Enforcement Network, SAR Confidentiality Reminder for Internal and External Counsel of Financial Institutions, FIN-2012-A002 (Mar. 2, 2012). 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, 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 (7)(c).

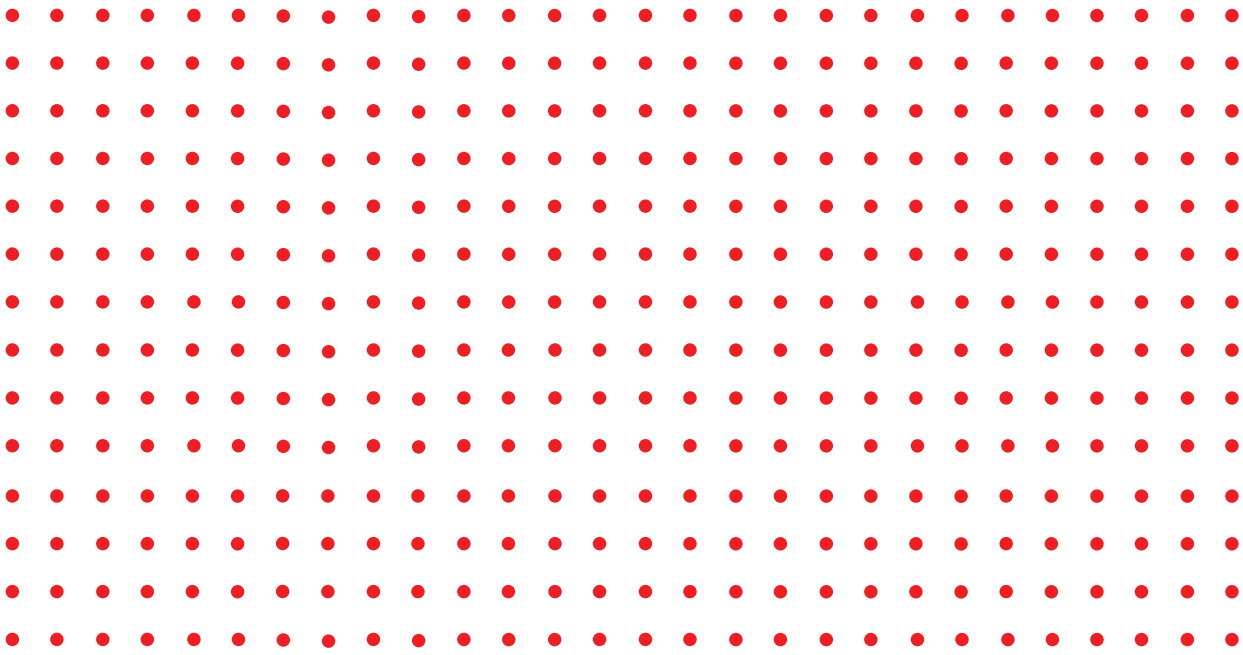
RECORD-KEEPING AND RETENTION

Casinos must have procedures to maintain and retain the specific transactional and customer 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 the SAR decision making;
- Training and testing materials and records of who was trained and when;
- Patron KYC due diligence records, including:
  - A record of those specific procedures performed to analyze a patron's gaming patterns and financial transactions;
  - Any due diligence report created;
  - Any risk determination; and
  - 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 programs, reports of testing and actions taken in response.

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



CONCLUSION

These practices reflect the continuing efforts of AGA member casino operators 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 re-evaluation.

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 or illicit financing threats.

GLOSSARY

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 such records 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 marker/credit, front-money and other gambling-related transactions, and where currency and chips are often kept. Safe-deposit boxes are often available at the cage. A large casino may have more than one cage location.

Casino: A casino is a land-based or interactive entertainment venue 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.

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), which is a negotiable instrument signed by the patron and made out to the benefit of the casino by the patron. 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 specific FinCEN guidance forbidding the use of digital IDs for AML purposes, casinos should include in their written AML program whether or not they will accept digital IDs.

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 to determine this location.

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 smart phone that can be used in digital channels).

Interest On Lawyer's Trust Account: 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.

GLOSSARY

IP (Internet Protocol) 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 and made payable to the casino 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.

Monetary/Negotiable Instrument Log: 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 above $3,000.

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

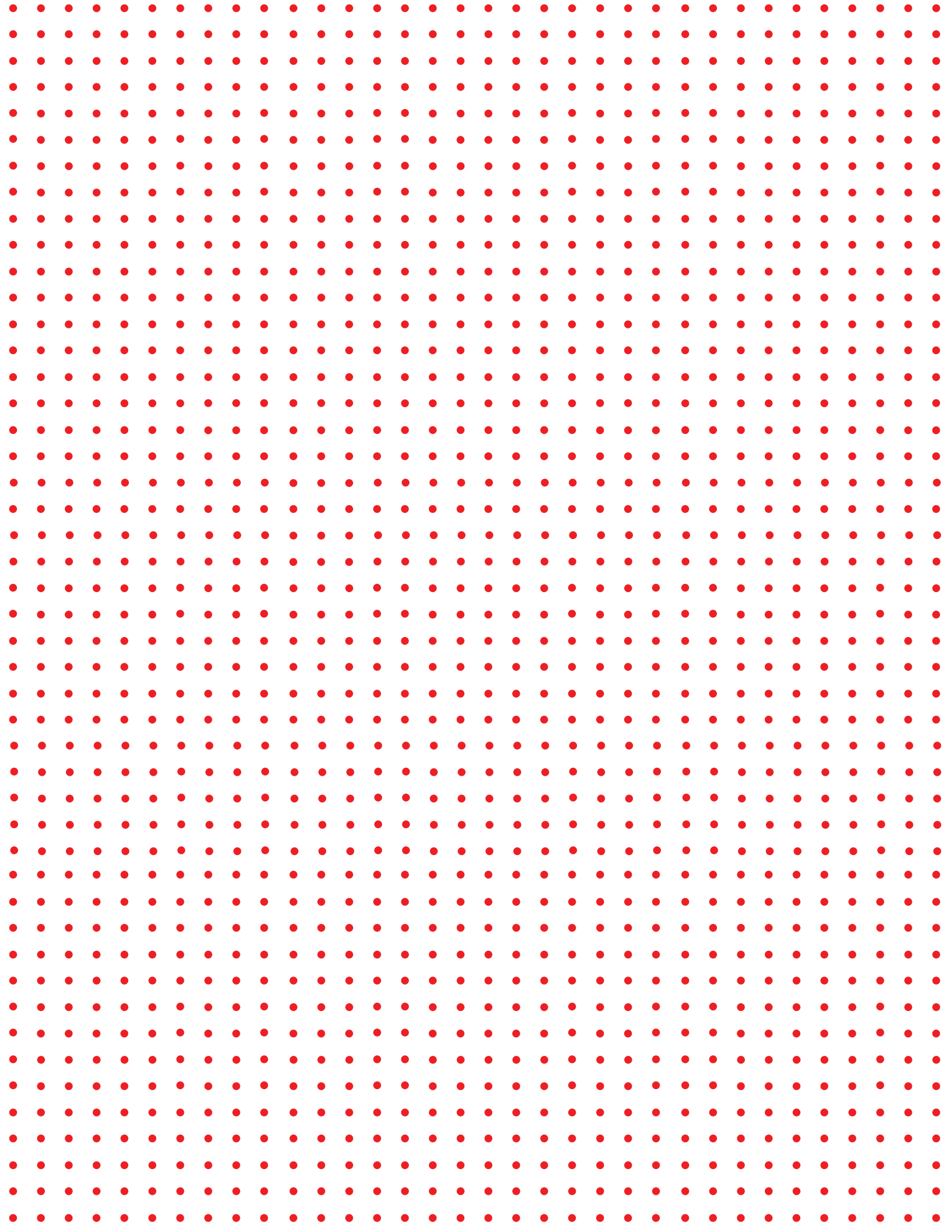
Risk Assessment: The formal process of examining a casino's mix of gambling activity, patrons, and overall economic environment in order to identify those activities and levels of play or other transaction that pose a risk of money laundering to be addressed by the casino's AML compliance procedures.

Safekeeping: Guest 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.

Ticket In/Ticket Out ("TITO"): A system for slot machine play through the use of 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 his play, balances on the ticket can be redeemed for cash at a kiosk or the casino cage, or used for further play at the casino that issued the ticket.

Sports Wagering: With the repeal of PASPA in May 2018, sports wagering is permissible in most U.S. states. A casino may offer sports wagering over the counter, via a sportsbook kiosk, via an internet browser and/or a mobile app. If offered via a mobile app, the patron will have a separate wagering account apart from any casino wagering account for slots, table games, keno, etc., 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.



ABOUT THE AGA

The American Gaming Association 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.

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 compliance 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 bank or corporation on his or her behalf, do you have a policy for inquiring into the identity of the beneficial owners of the bank or corporation involved?
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 (PEP's), 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 United States and in foreign locations?

B. Risk Assessment

11. Do you have a risk-based assessment of your customer base and their transactions?
12. 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 customer's country of origin?
    d. The gambling patterns or financial transactions favored by a customer?
    e. Third-party information about a customer, including negative information regarding the patron's integrity?
    f. Whether a customer has sources of wealth or income commensurate with his or her gaming activity?
    g. Whether a customer has provided verifiable identification information?
    h. Whether a customer has financial fiduciary obligations (e.g., trustee, accountant, attorney, nonprofit/charity executive)?
    i. Whether a customer is associated with individuals or entities known to be connected with the illicit generation of funds or legalized marijuana-related activity?
    j. Whether a customer claims connections with businesses that have no apparent operations?

APPENDIX A: ANTI-MONEY LAUNDERING PROGRAM QUESTIONNAIRE

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

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

C. Know Your Customer and Due Diligence

14. Have you implemented processes for securing identification for those customers whose transactions fall within the AML program?
15. Do you have a requirement to collect information regarding a customer's business activities and connections?
    a. If so, under what circumstances does that requirement apply, and
    b. What steps should be taken in that effort?
16. Do you have a process to review and update customer information relating to high risk relationships and activities?
17. Do you complete a risk-based assessment to understand the normal and expected transactions of customers?

D. Reportable Transactions

18. Do you have policies or practices for the identification and reporting of transactions that must be reported?
19. For currency reporting purposes, do you have procedures to identify multiple transactions that have been structured to avoid such reporting?
20. Do you screen customers and transactions against lists of persons, entities or countries issued by the Office of Foreign Asset Control or other government authorities?

E. Transaction Monitoring

21. 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 customers, and the like?
22. In order to identify AML concerns, do you review daily audit summaries, logs and reports such as Marker Summaries, Front-Money/ Safekeeping Summaries, multiple transaction logs, Monetary Instrument logs, check, logs, and wire reports?

F. Preventive Measures

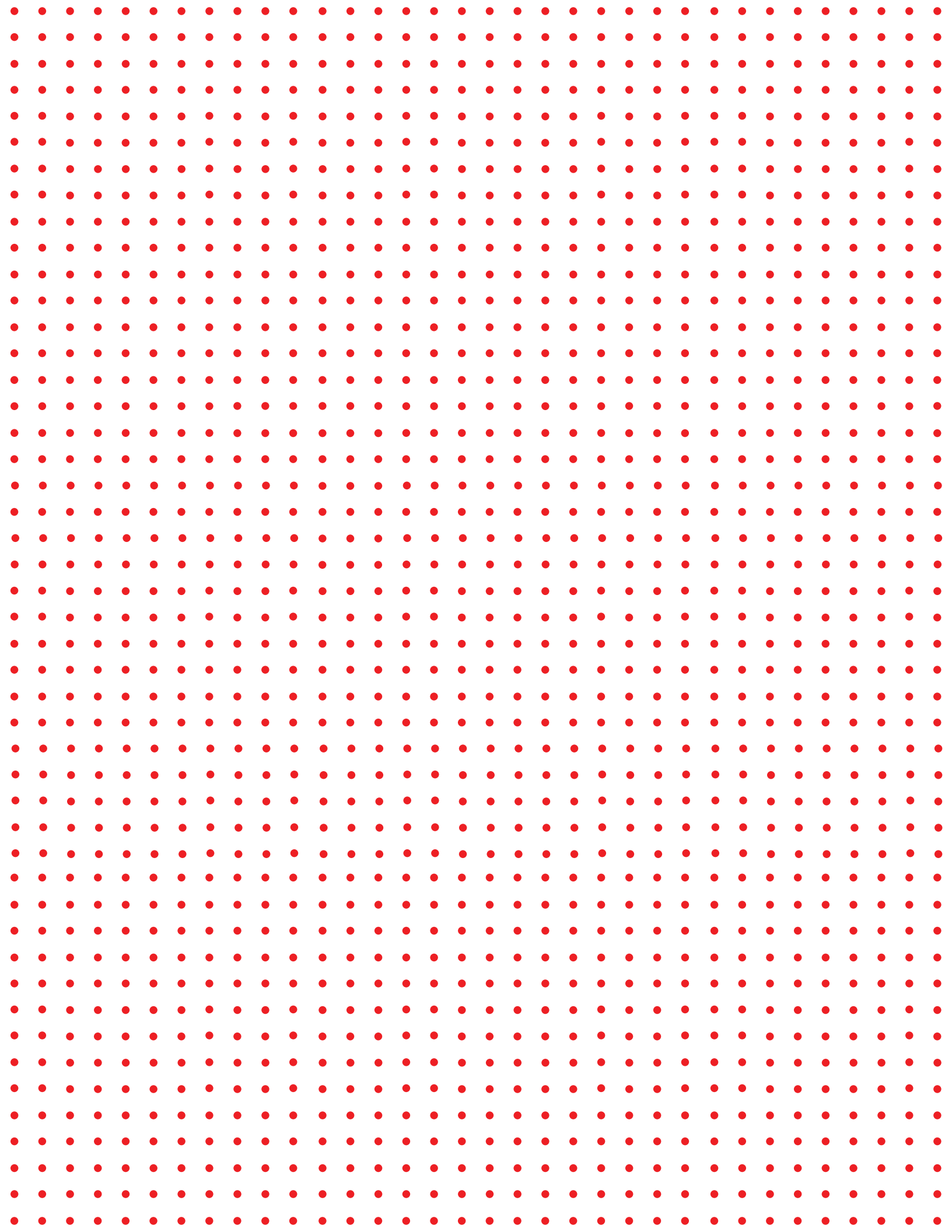
23. Do you cap "ticket-in/ticket-out" (TITO) redemptions at slot machine kiosks?
24. Do you cap the level of cash-for-cash exchanges?
25. Do you accept currency to purchase a casino check, other monetary instrument, or wire transfer?
26. Will you issue casino checks or wires to a patron for an amount greater than his or her winnings? Under what circumstances?
27. Do you issue checks for winnings only in the name of the customer?
28. Do you require supervisor review of checks or wires made payable to a customer's business or other account, or another individual?
29. 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 customer?
30. Do you allow cash play at poker tables?
31. Do you accept virtual currency?

APPENDIX A: ANTI-MONEY LAUNDERING PROGRAM QUESTIONNAIRE

32. Do you protect customer information to prevent social engineering, software vulnerability exploits, and network attacks?

G. Employee Training

33. Is your compliance officer at each gaming venue educated on the requirements of the AML program, including suspicious activity reporting and currency transaction reporting, and the requirements of state and federal regulators for AML compliance?
34. 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 currency transaction report?
    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 suspicious activity reports?
    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?
35. Do you retain records of training sessions including attendance records and the training materials used?
36. Do you update relevant employees on changes in AML law, policies or practices?
37. Do you provide training on the red flags of human trafficking, as well as financial red flags associated with human smuggling?




AMERICAN
GAMING
ASSOCIATION