Money Laundering Risks for Online Gambling

By Jim Dowling
and Brian Lopez

Introduction

Few would disagree that one of the most transformative inventions of modern times was the Internet. It has permanently changed how we communicate, work and interact with others, and engage in entertainment. Arguably, the second most important invention in modern history was the "smartphone." There it was, in the palm of your hand, capable of accessing almost all the information in the world, the ability to text, talk, and send pictures to anyone, anywhere. It also gave users access to online gambling sites whether they were at home, at work, or in a train, plane, or automobile. Twenty-four hours a day, seven days a week, you could spend five minutes or five hours on your phone gambling online whether through online casinos, poker rooms, or sports betting sites. Among the earliest adapters of the Internet were those involved in online gambling. The growth of the online gambling industry has surpassed some of the wildest expectations of only a few years ago. Some estimates have the current worldwide market for gambling at $2.2 trillion. Putting that into perspective, that is larger than the Gross Domestic Product ("GDP") for all but the top seven countries in the world.[1] The digital transformation that was brought on by the COVID-19 pandemic has only accelerated online and mobile gambling. In the past year, sports betting sites and mobile gambling opportunities have exploded with innovation and offering locations. In 2020, the U.S. online gambling market alone was valued at $1,978 billion[2] and the only limitation might be the threat posed by bad actors trying to launder illicit money.

History of Online Gambling

In order to understand the money laundering threats posed by online gambling, it is important to understand some of the key historical events. In 1949, Nevada became the only state to allow single-game sports wagering. Since sports wagering was limited to just the state of Nevada, it opened up an opportunity for organized crime to offer illegal sports betting throughout the United States. Organized crime syndicates used the Nevada sports books to "set the line" and help balance their books through the use of "layoff guys." In response to the growing threat of organized crime profiting from the illegal sports and numbers operations, Congress passed the Interstate Wire Act in 1961, which prohibited the use of interstate communication for the purpose of gambling.[3] As illegal gambling increased, and in particular illegal sports wagering, Congress further enacted the Professional and Amateur Sports Protection Act ("PASPA") in1992, which outlawed sports gambling in the United States with the exception of Nevada.[4] This law effectively provided Nevada with a monopoly on legal sports betting, but did very little to diminish illegal sports books. The restrictions in online gambling and in particular sports gambling resulted in a proliferation of illegal offshore casinos and sports books.

The widespread use of the Internet marginalized the effects of the Wire Act and made the enforcement of illegal online gambling and sports betting more difficult. Gamblers no longer needed a bookie to place their bets. They could place their bets anywhere in the world as long they had access to the Internet. In 2006, Congress passed the Unlawful Internet Gambling Enforcement Act ("UIGEA"). This law made it illegal for gambling businesses to "knowingly accepting payments in connection with the participation of another person in a bet or wager that involves the use of the Internet and that is unlawful under any federal or state law."[5] UIGEA did allow for exceptions relating to some fantasy sports, as well as some *intrastate* transactions. This legislation forced many online poker sites and payment processors to close. The federal functional regulators, the Office of the Comptroller of the Currency and the Federal Reserve, also stepped in and required their regulated financial institutions to identify and block transactions that might be considered payments for gambling. These federal financial regulators forced banks, credit card companies and other payment processors to develop sophisticated programs to identify and block payments that were in furtherance of illegal gambling. The federal government effectively outsourced their enforcement efforts to the private sector. These financial institutions spent tens of millions of dollars developing sophisticated monitoring systems to identify and block suspected gambling transactions. Illegal online gambling operations quickly adapted to this law and set up shell companies with names and profiles that appeared to be something other than a casino or sports book. Thus began the game of "Whack-A-Mole" between financial institutions and the illegal gambling world.

The UIGEA did have a few high-profile cases. Eleven individuals associated with the largest online poker sites, Absolute Poker, Full Tilt Poker and PokerStars, were charged with money laundering, bank fraud, wire fraud and violations of the UIGEA on April 15, 2011. These online poker sites attempted to "disguise the true nature, source, and ownership" of the gambling payments, and then skimmed funds from player's accounts to pay dividends to company owners. The companies were also charged civilly with money laundering and forfeiture, and several individuals charged in the case were senior executives in these companies. In addition to the criminal charges, law enforcement seized the domain names of these companies, effectively putting them out of business.[6] The cases against all three companies were settled civilly and the assets of the companies were forfeited to the "victims of the fraud," who were the patrons engaging in online poker play.[7]

In 2010, Nevada was the first state to implement mobile gaming. In setting up their mobile gaming program, the Nevada Gaming Control Board made the effort to ensure that everything related to the gaming activity took place within the state of Nevada. The gaming operators, vendors and IT systems all had to be physically located in Nevada. In addition, all gaming operators needed to install geo-fencing software to ensure that before an individual placed a wager, they were physically located in Nevada.

In 2011, the state of New Jersey and others challenged the legality of PASPA. Then on May 14, 2018, the U.S. Supreme Court struck down PASPA saying that it was a violation of the 10th Amendment. Subject to individual state approval, this opened the door for online and mobile sports betting as long as all activities were contained within the individual state.

Regulatory Expectations

In August 2019, the FinCEN Director addressed the U.S. Supreme Court decision at a gaming industry conference in Las Vegas.[8] In his prepared remarks, the FinCEN Director stated:

> *"With last year's Supreme Court decision legalizing sports betting, it's important for casinos and card clubs to consider how to integrate sports betting programs into their existing AML [Anti-Money Laundering] programs. Sports betting, and other mobile gaming services run through your casino, are no different than other products and services. FinCEN expects that your casino or card club is monitoring your sports betting programs for potentially suspicious activity. This includes offering sports betting through a mobile app.*

> *Whether or not sports betting is offered on or off-premises, your AML obligations are the same. Not only that, but we also expect your SAR [Suspicious Activity Report] reporting will include cyber-related indicators collected through the use of mobile gaming or betting applications."*

The FinCEN Director went on to warn casinos and sports book operators about using all available information to detect and prevent money laundering.

> *"You must establish and implement procedures for using all available information to detect and report suspicious transactions, or suspicious patterns of transactions, that occur through mobile sports applications.*

The use of all available information also applies to identifying and reporting cyber-attacks. The FinCEN Director reiterated a prior FinCEN advisory requiring all covered financial institutions and casinos to report what FinCEN refers to as a "Cyber Event." FinCEN defines a Cyber Event as "[a]n attempt to compromise or gain unauthorized electronic access to electronic systems, services, resources, or information." The Cyber Event also needs to aggregate to $5,000 or more in a single or multiple events. It is important to remember that the Cyber Event does not need to be successful, but merely needs to be attempted by, at, or through the financial institution. Even though the cyber event may not result in the theft of any money from the casino, if the attack or attempted attack was against an individual player account, casino financial account or an account takeover/identity theft, the attempted attack is reportable on a SAR. Regulators have determined that an attack on any financial account has the potential to exceed $5,000 and is therefore reportable. The filing of a SAR for a Cyber Event does not alleviate the casino's responsibility for reporting such attacks or attempted attacks under other state or federal regulations.

In short, FinCEN expects casinos to have the same robust Bank Secrecy Act/Anti-Money Laundering ("BSA/AML") programs to detect and deter money laundering threats for online and mobile gaming as the traditional brick-and-mortar casinos. On June 30, 2021, FinCEN issued its first government-wide priorities for anti-money laundering and countering the financing of terrorism policy[9] pursuant to Section 5318(h)(4)(A) of the Bank Secrecy Act ("BSA")[10] as amended by Section 6101(b)(2)(C) of the Anti-Money Laundering Act of 2020 (the "AML Act").[11] In the new policy, FinCEN identified eight national priorities for all bank and non-bank financial institutions covered by the BSA, which includes casinos and online gambling establishments, that must be incorporated into existing BSA/AML programs. The eight priorities include (1) corruption; (2) cybercrime, including

relevant cybersecurity and virtual currency considerations; (3) foreign and domestic terrorist financing; (4) fraud; (5) transnational criminal organization activity; (6) drug trafficking organization activity; (7) human trafficking and human smuggling; and (8) proliferation financing. FinCEN will issue further requirements on these priorities within 180 days. Given the new policy, casinos and online gambling establishments should begin to formulate strategies on how to incorporate the AML/CFT Priorities into their risk-based AML programs.

Money Laundering Risks

Traditional brick-and-mortar establishments have generally done a good job dealing with their money laundering risks, however, online gambling presents different types of risks that casino operators need to get their arms around. As online gambling has become more prevalent, fraud, and money laundering concerns are top of mind for regulators and the U.S. government. Back in 2013, the U.S. Senate Subcommittee on Consumer Protection, Product Safety, and Insurance held a session to dive deeper into the potential risks associated with online gambling.[12] They addressed a variety of issues including protecting consumers from fraud, underage and problem gambling, and increased opportunities for criminals and terrorists to launder funds. The overall concerns raised were how online gambling provided the benefit of anonymity to a whole host of bad actors. In fact, Chuck Canterbury, the former National President of the Fraternal Order of Police, testified before the subcommittee "organized crime is using offshore online operations to launder their profits. We also know that terrorist organizations are or could be using the same strategies to launder funds." Mr. Canterbury also went on to address the challenges that regulators have regulating a "dynamic, ever-changing technology…"

Real-life examples of the concerns addressed by the U.S. Senate Subcommittee and regulators alike were on full display in China during the first nine months of 2020 when $150 billion was laundered through online gambling platforms.[13] Chinese authorities initiated the "Card Breaking Campaign" to "crack down on illicit bank card transactions and bank card sales to combat telecommunications fraud and cross-border online gambling." Investigators discovered that Chinese nationals from extremely remote locations were recruited to "loan or lease financial credentials to offshore criminal groups." This in turn helped to conceal funds belonging to illegal gamblers. As all forms of gambling are illegal in China, gamblers face obstacles when attempting to deposit funds into an online gambling platform. These illegal gamblers were able to utilize e-commerce platforms along with mobile payment platforms such as WeChat Pay and Alibaba's Alipay to disguise gambling deposits as legitimate online shopping purchases. As mobile payment platforms have become increasingly popular and promoted by China, they have also attracted criminal gambling groups due to the ease of use and the ability to manipulate transactions to conceal identities and illegal activity. Given that the financial credentials are typically coming from young jobless individuals located in remote and rural areas, criminal enterprises have an endless source of recruits, ready and willing to assist for the right price. Cryptocurrencies or Convertible Virtual Currencies such as Tether's USDT, were also used in the scheme.

Chinese authorities have increased their efforts to prevent cryptocurrencies from being used in these schemes through the enforcement of account verification regulations that attempt to ensure the identity of the cryptocurrency account holder. Ultimately, the major challenge facing Chinese authorities is the anonymity factor when utilizing online platforms, which is also a major concern for U.S. regulators.

Here in the U.S., these issues have grown as states begin to allow online gambling. Casinos and other gambling establishments face similar money laundering risks trying to identify their true customer. The requirements for account opening or customer onboarding is still being debated at the state and federal level. As the debate continues, many casinos and other online gambling license holders are struggling to put the right controls and policies in place for online account openings.

Arguably, the most challenging and important aspect of any online or mobile gaming program is to obtain and verify the identification of the patron. Currently, there are several states that do not require a patron to provide their identification for online gaming. Rather, the patron provides limited Personally Identifying Information ("PII") to the casino through a secure portal. Third-party software systems are then used to verify the identity of the person. IRS Examiners and FinCEN currently do not approve of this type of account opening process. However, FinCEN is currently considering whether or not to allow this process for account openings. Whether casinos require patrons to produce identification, or whether third-party software systems are used to validate a patron's identity, compliance personnel must ensure that the identity used has not been stolen as part of an identity theft ring. There have been numerous cases where organized groups have used stolen identity and credit cards to open and fund online accounts only to quickly withdraw the funds leaving the casino or the credit card company with the loss.

Mitigating Money Laundering Risks

In order to mitigate the money laundering risks with online gambling, compliance professionals need to ensure they have a sound anti-money laundering program. A sound risk-based anti-money laundering program starts with having an effective risk assessment. A risk assessment helps compliance professionals understand where potential problem areas and high-risk services exist within their BSA/AML program. Once the pertinent risks are identified and qualified, internal controls[14] can be established to mitigate the identified risks. As an example, to help mitigate the risks of patron anonymity, compliance professionals should establish an anti-money laundering policy around account openings and have detailed step-by-step procedures to capture all required patron information per federal regulations.[15] The procedures should contain a level of detail that can be easily interpreted and executed by anyone who reads them. They should address any potential account opening scenarios one would face and provide steps to follow depending on the information received from the patron. If properly constructed and implemented, the policy and procedures should act as a "mitigating control" to reduce the inherent risk presented in the risk assessment.

Casinos are one of the few financial institutions where regulators do not require a more comprehensive onboarding process. Banks, online banks, money service businesses, and even cryptocurrency companies require

customers to provide background information during the account opening process. In addition to the required name, address, and Social Security number, other financial institutions require customers to provide occupation information, expected transaction levels, and frequency of use. If casinos were to include these additional onboarding questions, which typically take less than a minute to answer, they could potentially save millions of dollars in compliance costs and reduce the number of SARs to be filed.

The next critical piece to mitigate potential money laundering risks is an effective training program. Per federal regulations, financial institutions including casinos are required to train personnel in the identification of "unusual or suspicious transactions" as well as the reporting of these transactions.[16] This would also include training on account opening procedures and the awareness of potential red flags. Training is a critical component as it helps front line employees (referred to as "front of the house") understand what to look for, how to identify, and how to report "unusual or suspicious transactions."

Behind the scenes, employees and compliance professionals (referred to as "back of the house") also need to be trained in how to identify suspicious activity. Federal regulations require back of the house personnel to be able to identify potentially suspicious activity "after the fact" and require them to use "all available information"[17] as well as any "automated data processing systems".[18] This is where the use of data analytics is essential. Since online gambling provides criminals additional opportunities to launder or disguise illegally derived funds, the transactional data generated through online gambling must be used to detect potentially suspicious patterns of activity. Since this type of gaming activity occurs online, compliance professionals must leverage data analytics to identify indicators and patterns of potential suspicious activity. At a minimum, compliance professionals should be looking for indicators of structuring cash transactions to avoid CTRs, minimal gaming activity, and unusual or increased betting patterns. As an example, if a patron's betting limits range between $7,000 and $12,000 per week suddenly jump to $25,000 to $30,000, compliance personnel should investigate this anomaly to determine if the increase is suspicious or not. Was the sudden increase related to messenger betting or even an account takeover (ATO)? Is this new level of betting commensurate with the patron's perceived standard of living ("Source of Funds")? Effective controls and data analytics need to be in place to mitigate the potential risks and to identify this type of suspicious activity.

Lastly, a compliant anti-money laundering program needs to have an individual appointed to "assure day-to-day compliance",[19] such as a compliance officer, as well as "internal and/or external independent testing" of the BSA/AML program .[20]

Benefits of an effective anti-money laundering program

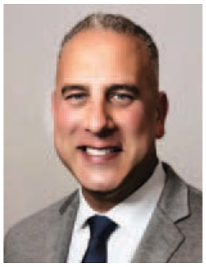
While there are potential money laundering risks associated with offering online gambling, there are also a plethora of potential benefits. First, as gaming activity occurs online and funds need to be deposited into a patron's account prior to any betting, the money laundering risks associated with cash transactions are greatly reduced as opposed to brick-and-mortar casinos. Patrons can choose to deposit cash into their online account; however, these deposits need to take place in person by interacting with casino personnel, thus mitigating potential money laundering risks. The same is true for cash withdrawals from online gaming accounts. With strong controls in place to accept cash deposits or cash withdrawals, the risk of patrons trying to evade cash reporting requirements is greatly reduced. For online gaming, depositing or withdrawing funds via ACH or wire from other regulated financial institutions such as banks, payment platforms such as PayPal, or credit cards, can be much more attractive and easier to use from a patron's perspective as these mechanisms can expedite the gaming experience. The end result is fewer CTRs that need to be filed and better tracking of a patron's funds and gambling activity.

Additionally, the reporting of potentially suspicious activity can also be greatly enhanced utilizing online gambling data. These online gambling systems can be customized to capture and report relevant information in a way that is most beneficial for compliance. Traditional information systems at brick-and-mortar casinos often present challenges for compliance personnel attempting to gather and extract relevant data to identify suspicious activity. These traditional systems, such as table games and slot rating systems, often have set structures and reporting capabilities that are predefined. In contrast, online gambling systems tend to be newer and can be developed and customized to capture pertinent information that makes it easier for compliance personnel to identify potential red flags and file more accurate SARs. The importance of having accurate and reliable information to conduct data analytics to identify suspicious activity and SAR reporting cannot be understated. Good data provides compliance personnel with the ability to do more with less by leveraging technology and providing a perspective to online gambling activity that otherwise may go unnoticed.

There are also potential benefits from a marketing standpoint. Obtaining accurate information on patrons as well as their betting patterns provides invaluable insights for marketing departments looking to increase their customer base. At traditional brick-and-mortar casinos, marketing departments utilize player ratings as a way to identify "attractive" patrons. However, player ratings are essentially estimating betting activity and are only as good as the individual or system entering and capturing the information. As an example, table games rating information is typically generated by observing the patron's gaming activity for only a few moments at a time, then extrapolating and estimating that information to generate a patron's profile. In contrast, online gambling data can provide a much more accurate patron profile as the information is based on actual wagering activity that has taken place rather than estimates. This gives marketing departments more accurate information to identify desirable patrons and ultimately make marketing efforts much more effective.

As technology progresses and the online gambling experience is enhanced, the market will continue to grow resulting in revenue generation for casinos that has not been seen before. The best way to protect this revenue and allow your business to grow is to have an effective AML program in place, a program that shields your casino from regulatory fines and enforcement actions.

Jim Dowling is the Managing Director with the Dowling Advisory Group and has more than 30 years' experience in the areas of anti-money laundering (AML), fraud and risk management. His career includes extensive experience as a Special Agent with the IRS Criminal Division, "Big Four" accounting and regulatory compliance. Jim also served as the Anti-Money Laundering Advisor to the Executive Office of the President, White House Drug Policy Office and he served on FinCEN's Bank Secrecy Act Advisory Group. Jim was also an adjunct professor at the USC Marshall School of Business where he taught forensic accounting in the master's program and is on the ACAMS Board of Directors for the Southern California chapter. Jim can be reached at Jim@DowlingAdvisory.com.



Brian Lopez is a Director with the Dowling Advisory Group where he specializes in the use of data to help all types of financial institutions in preventing money laundering and the funding of terrorism. Brian has worked with some of the largest casinos in the world, assisting with the independent testing of BSA/AML programs, remediation related look backs, data flows and BSA/AML laundering system validations. Brian also regularly presents, writes, and instructs on the topic of forensic data analysis. He graduated from the University of Washington with a bachelor's degree in Industrial Engineering and obtained his Master's in Business Administration from the UCLA Anderson School of Management. Brian is a Certified Fraud Examiner and a Certified IDEA Data Analyst. He can be reached via email at Brian@DowlingAdvisory.com.

[1] https://www.mordorintelligence.com/industry-reports/united-states-online-gambling-market; https://www.thebalance.com/gdp-by-country-3-ways-to-compare-3306012.

[2] https://www.mordorintelligence.com/industry-reports/united-states-online-gambling-market.

[3] 18 U.S.C. § 1084.

[4] The Professional and Amateur Sports Protection Act of 1992 (Pub. ... 102–559), also known as PASPA or the Bradley Act, is a judicially-overturned law that was meant to define the legal status of sports betting throughout the United States. This act effectively outlawed sports betting nationwide, excluding a few states.

[5] https://www.ots.treas.gov/_files/422372.pdf.

[6] https://www.reuters.com/article/us-poker-fraud-arrest/full-tilt-poker-ceo-surrenders-to-u-s-on-gambling-fraud-idUSBRE86200S20120703.

[7] https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-compensation-program-absolute-poker-victim.

[8] https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-12th-annual-las-vegas-anti.

[9] https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf.

[10] Section 6003(1) of the AML Act of 2020, Division F of the National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283 (January 1, 2021), defines the BSA as comprising Section 21 of the Federal Deposit Insurance Act (12 U.S.C. 1829b), Chapter 2 of Title I of Pub. L. 91-508 (12 U.S.C. 1951 et seq.), and Subchapter II of Chapter 53 of Title 31, United States Code.

[11] The AML Act was enacted as Division F, §§ 6001-6511, of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283 (2021).

[12] https://www.govinfo.gov/content/pkg/CHRG-113shrg82840/html/CHRG-113shrg82840.htm.

[13] https://asia.nikkei.com/Spotlight/Caixin/How-illegal-online-gambling-launders-150bn-from-China.

[14] *See* 31 C.F.R. §1021.210(b)(2)(i).

[15] *See* 31 C.F.R. § 1021.410(a).

[16] 31 C.F.R. § 1021.210(b)(2)(iii).

[17] 31 C.F.R. § 1021.210(b)(2)(v).

[18] 31 C.F.R. § 1021.210(b)(v)(C)(iv).

[19] 31 C.F.R. § 1021.210(b)(2)(iv).

[20] 31 C.F.R. § 1021.210(b)(2)(ii).