jumio FINTRAIL

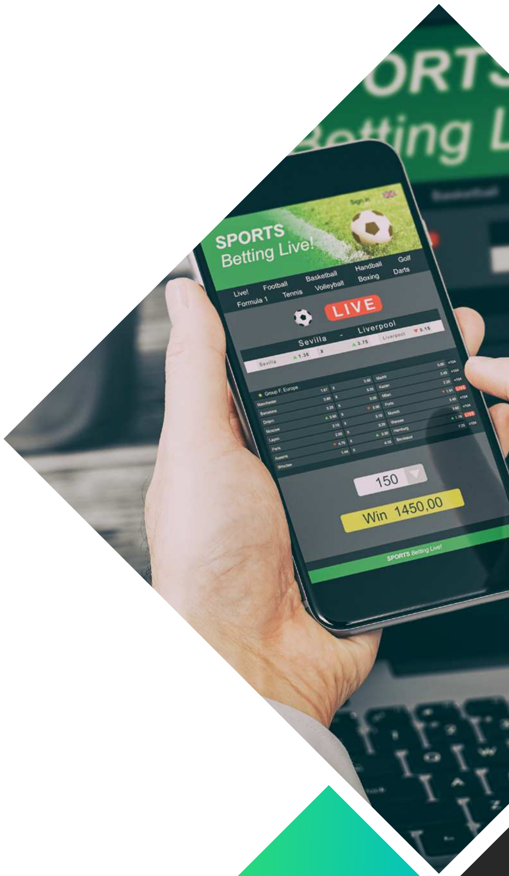
Regulatory Guide to AML Compliance

Trends, Technology and Threats for Online Gambling Operators

APRIL 2023

TABLE OF CONTENTS

INTRODUCTION



The online gaming industry has witnessed massive growth in recent years and shows no sign of abating - the sector is projected to grow to USD 153.6 billion globally by 2030. The increase in activity has been accompanied by increased risk of exploitation by financial criminals and increased scrutiny from regulators. More than ever before, online gaming operators — providers of activities including sports betting, online wager, games of chance (e.g., roulette) and skill-based games (e.g., poker) — must take compliance seriously or risk suffering enormous fines and reputational damage.

Online gaming is a regulated sector for anti-money laundering (AML) and counter-terrorist financing (CTF) in most jurisdictions, and providers have responsibilities in line with banks and other financial institutions. Their obligations include Know Your Customer (KYC) checks, compliance with financial sanctions, reporting suspicious activity, and an increasing focus on non-AML risk factors such as age restrictions and problem gambling.

Regulators are tightening up the legislative framework for online gaming operators and imposing penalties on those who do not comply.

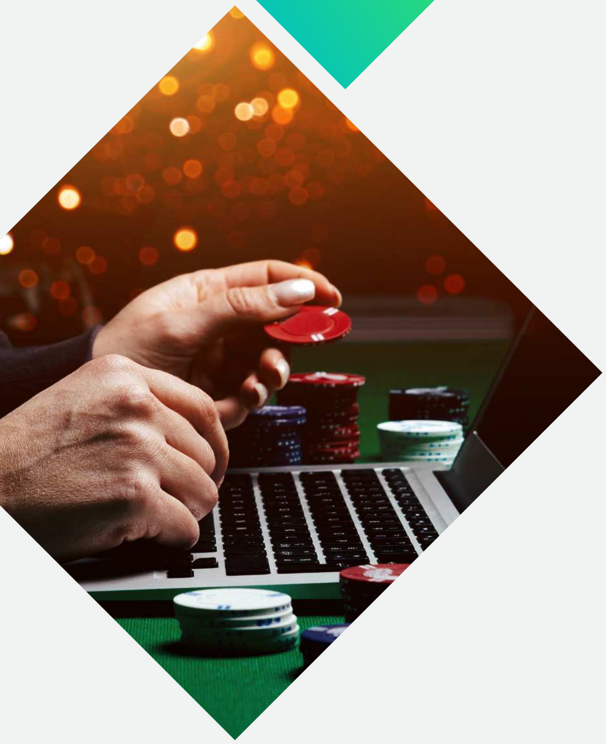
In Europe, the European Gaming and Betting Association recently strengthened its AML efforts with pan-European guidelines that cover customer and business risk assessments, due diligence and record-keeping requirements. The UK's Gaming Commission, one of the strictest gaming regulators in the world, issued new rules on protecting "at-risk customers" in September 2022, to sit alongside existing AML regulations. The Commission also made clear that its rules do not just exist on paper and that implementation will be enforced, stating that "an attitude of the lowest-possible compliance being sufficient" will no longer be tolerated. Indeed, a review of the Commission's website indicates the level of recent enforcement activity, with £20 million in fines issued in August 2022 alone.

While regulations become increasingly stringent and enforcement actions abound, digital gaming operators still typically maintain limited compliance resources. This ebook is a regulatory guide designed to help online gaming companies' compliance teams understand their obligations and how to maximize their resources, focusing on critical threats and opportunities. Through examining global patterns while honing in on key markets in the UK, U.S. and the EU, this guide explores current and future trends to help online gaming operators fortify their operations and remain compliant.

THREAT LANDSCAPE

The Financial Action Task Force (FATF), an intergovernmental financial crime policy-making body, defines all gaming operators as designated non-financial businesses that should be supervised for compliance with AML /CTF requirements. Recently, the European Commission gave online gaming the highest threat level possible for money laundering weaknesses, citing its non-face-to-face nature, vast and complex financial flows and the propensity towards the potential use of cryptocurrencies that may increase customer anonymity. Frauds and scams are also significant risk factors, including the use of stolen credit cards, fake identities and illegal chargebacks. And like brick-and-mortar casinos, online gaming sites have extremely high customer turnover and transaction volumes, making them an attractive target for money launderers and professional fraudsters.

Meeting customers' expectations for quick and frictionless onboarding while verifying and screening players using the right level of controls is a difficult balance to strike. However, there are some helpful features of online gaming that can be exploited in the fight against financial crime. While land-based casinos are cash intensive — a high risk factor for money laundering — online betting operators typically see the depositing and withdrawing of funds through payments using credit cards, online wallets or wire transfers, which means a layer of customer due diligence is already conducted by a financial institution. Moreover, online systems capture a lot of data that can theoretically be analyzed to allow compliance professionals to identify red flags and flag suspicious behavior.



Common money laundering behaviors and red flags:

Cash-in, cash-out

Criminals convert dirty money into an electronic balance and gamble for a short period of time in low-outcome bets. They then cash out all the funds, with the intention of subsequently claiming that the money originated from gambling wins.

Structuring

Criminals divide dirty money into several small betting accounts, purposefully avoiding monitoring and reporting thresholds.

Intentional losses

Funds are deliberately lost to a secret accomplice posing as an opponent in a game such as poker, allowing that person to withdraw the dirty money as winnings.

Excessive deposits

Excessive deposits from various payment processors, bank accounts or prepaid access cards can be indicative of money launderers pooling illicit funds from different sources.

Mutliple IPs

Account holders using multiple IP addresses or devices (a "one-to-many" relationship) can be indicative of several illicit actors controlling an account being used for money laundering. On the flip side, multiple accounts using the same device or IP address (a "many-to-one" relationship) can be indicative of a money launderer or fraudster setting up multiple accounts using different fake identities.

SUITABILITY CHECKS

While AML and CTF responsibilities are clearly critical, online gaming operators must also consider increasingly rigid suitability or responsibility checks. These checks vary by country and include identifying signs of gaming addiction or lack of financial stability, and eligibility in terms of age and location. Gaming regulations are contingent on physical jurisdiction and can even be state- or city-specific. For example, not all U.S. states permit online gaming, so people who reside in some states cannot patronize online gaming sites. Legal age requirements also vary by country, sometimes based on the type of gaming activity, and providers have a responsibility to detect and decline underage players.

As the social risks of gaming addiction garner more attention, problem gaming has become a more important risk for providers to mitigate.

Online gaming is considered more addictive than in-person gaming, given its portability, convenience and temptation to play 24/7 on a computer or mobile device. Additionally, hiding problem gaming is easier online, as all activity can be done privately. Noting this, regulators are increasingly fining operators for social responsibility failures such as giving customers irresponsible deposit caps, not effectively identifying players at risk of harm or not interacting appropriately with individuals suffering extreme losses. In the UK, credit card payments to gaming operators are banned to prevent customers gambling with money they may not have, and firms are obligated to ensure payments from e-wallets are not loaded from a credit card.

Where social responsibility concerns are apparent, online gaming operators must have controls to detect and intervene. In practice, these factors typically fall under the general umbrella of “compliance” or “risk”, adding to stretched teams already responsible for detecting money laundering and terrorist financing. However, the good news is that many of the same controls that are used to identify and prevent financial crimes can also be harnessed to address operational and social responsibility risks.

TECHNOLOGY

Compliance teams across the gaming sector are stretched thin. Despite limited compliance staff, online gaming operations have extremely high volumes of transactions that must be monitored and assessed. The UK Gaming Commission has stated that many operators have insufficient resources, accounting for their frequent regulatory failings. Making the most of scarce resources is clearly vital.

Coping with these enormous and rapid-fire transactions ideally requires some level of technology and automation to screen intelligently for risk indicators and to optimize resources. Solutions that capture and consolidate player data through all touchpoints provide useful metrics, generate meaningful and insightful alerts and help prioritize compliance operations. This helps streamline processes in line with a risk-based approach that can respond to the demanding pace of regulatory change and encompass additional risk factors such as gaming addiction.

Identification and verification tools, especially those that leverage biometrics, are vital to verifying a customer’s identity and eligibility when onboarding a new customer.

Automated tools can screen client and transaction details against sanctions lists and other official watchlists to ensure prohibited actors aren’t onboarded or allowed to make transactions. Other screening lists help detect politically exposed persons (PEPs) — individuals considered to pose a heightened threat due to their more significant risk of involvement in corruption. Additionally, names can be searched against media databases and other sources to detect negative media findings indicating potential risk. For example, media searches may yield a news article showing that a subject was previously charged with money laundering. Even without an official conviction, this information must be considered, as it will alter the customer’s risk profile. And finally, given the jurisdiction-contingent nature of online gambling regulations, verifying customers’ IP addresses to ensure accurate information on their location is also essential for compliance.

THINGS TO LOOK FOR IN A TECHNOLOGY PROVIDER

- Able to provide low-friction onboarding while confirming customers' identities and conducting age verification and location checks
- Capture of real-time threats and risks, flagging and showcasing relevant information without delay and creating auto-stops
- Consolidation of data and information within one system, removing redundant platforms for increased efficiency
- Effective sanctions screening capabilities to contend with the pace of change of sanctions programs
- Use of updated and comprehensive watchlists for politically exposed persons
- Provision of accurate and explainable customer risk ratings

The role of advanced technologies in gaming compliance has been explicitly recognized by the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN), which highlighted technology's ability to detect and report financial crimes, and the importance of gaming outlets using "all available information and automated data processing systems to aid in ensuring compliance." Having a technology-forward process in place not only assists in preventing crime and detecting risk factors — it also helps online gaming operators justify their program and their approach to regulators.

On a business level, technology can drive operational efficiencies that facilitate scalability and ultimately drive profits. By expediting KYC processes, staff are better prioritized to work on problems that require valuable critical thinking skills. Outsourcing to a provider who can provide these tools is a cost-efficient solution for online gaming operators who are looking to avoid heavy investment into building a custom system that requires an expensive data science team.

KEY JURISDICTIONS – A DEEP DIVE

THE UK

The UK Gaming Commission allows for all forms of online gaming with a license and is notoriously strict in terms of AML and responsibility checks.

Relevant regulations:

- UK Gaming Act
- All online gaming operators are required to comply with certain provisions of:
  - Proceeds of Crime Act 2002
  - Terrorism Act 2000
  - Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
  - Sanctions and Anti-Money Laundering Act 2018

Key regulatory requirements
From the Gaming Commission's Licence Conditions and Codes of Practice:

KYC

A player's identity must be verified before they are permitted to gamble. Information collected should include as a minimum: customer name, address and date of birth. Online gaming operators are expected to take reasonable steps to ensure that they hold accurate customer identity information.

Customer due diligence is mandatory in the following scenarios: when establishing a business relationship, suspecting money laundering or terrorist financing, doubting documents or information obtained to verify identity, carrying out an occasional transaction that amounts to a transfer of funds more than €1,000, any transaction that amounts to €2,000 or more including when it is executed in several seemingly linked operations, or when the risk assessment for a customer has changed.

Due diligence should follow a risk-based approach. For low risk customers, firms can conduct simplified due diligence. PEPs are considered high risk, and gaming operators must conduct checks to confirm their source of wealth.

SCREENING

Sanctions

Sanctions programs are upheld by HM Treasury's Office of Financial Sanctions Implementation (OFSI). Online gaming operators are required to prevent sanctions breaches and to monitor the risk area closely. They are required to send details of "key events" to the UK Gaming Commission and report any breaches to OFSI.

PEPs

Firms are required to identify both domestic and foreign PEPs and take steps to manage the associated risks.

Adverse media

Adverse media screening is not a regulatory requirement, but the FCA does state that such searches are a part of ongoing monitoring and enhanced due diligence.

ONGOING MONITORING

Transaction monitoring

Firms must conduct ongoing transaction monitoring with either profiling or rules-based monitoring methods. Manual procedures are theoretically permitted, particularly for smaller firms or those processing few transactions. However firms with large transaction volumes are recommended to use more sophisticated automated monitoring systems. Suspicious activity must be reported to the Financial Intelligence Unit either manually or electronically via the FIU's SAR Online System.

Ongoing KYC

Firms must update KYC information and documents on an ongoing basis, although no particular frequencies are suggested.

Ongoing screening

Firms must conduct ongoing sanctions and PEP screening, although no particular frequencies are mandated. Many firms screen customers against sanctions lists on a frequent (e.g., daily) basis but screen against PEP lists and adverse media sources at longer intervals. Firms are advised to consider real-time sanctions screening of transactions.

THE U.S.

Online gaming has a shorter history in the U.S. than elsewhere, only becoming legal nationwide when the Professional and Amateur Sports Protection Act was struck down in 2018. Each individual state can legalize and regulate online gaming on its own terms, as long as activities remain within that state. The general interpretation of federal law is that interstate online gambling is illegal (although there have been challenges) and bets can only be placed with licensed operators by individuals physically located in the relevant state. Each state has a different regulator, with FinCEN being the federal supervisory agency. Online gaming operators are considered financial institutions and are subject to AML program requirements.

Relevant regulations:

- Unlawful Internet Gaming Enforcement Act of 2006
- The Interstate Wire Act
- All online gaming operators are considered financial institutions and required to comply with:
    - The Bank Secrecy Act, reformed by the Anti-Money Laundering Act of 2020 (AMLA 2020)

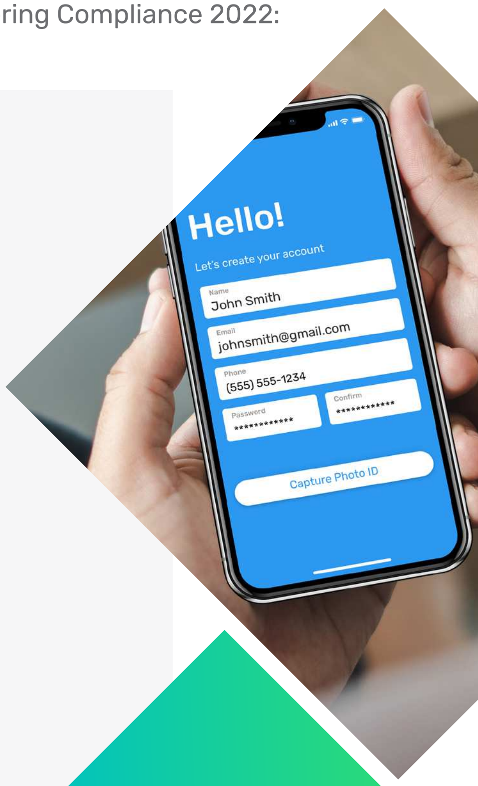
Key regulatory requirements
From the American Gaming Association's Best Practices for Anti-Money Laundering Compliance 2022:

KYC

Players must create an online account with a gaming operator before placing any bets. Accounts can be established either online, using digital identity verification solutions, or in person with a physical document review.

Because online gambling operators are considered financial institutions, standard KYC requirements apply. For U.S. individuals, firms should obtain the name, address, date of birth, and Social Security number. For non-U.S. individuals, firms should also obtain one or more of the following: taxpayer identification number, passport number and country of issuance, alien identification card number, or number and country of issuance of another photographic government-issued document.

Firms should conduct enhanced due diligence where necessary as part of a risk-based approach. This includes foreign PEPs (U.S. public officials are not considered PEPs per U.S. regulations).



SCREENING

Sanctions

Sanctions are administered by the U.S. Treasury's Office of Foreign Assets Control (OFAC), and financial institutions (including online gaming operators) must comply with programs listed on the Treasury website.

PEPs

There is no regulatory requirement for financial institutions to determine whether customers are PEPs, though they may choose to do so to determine a customer's risk profile. However, AMLA 2020 increased penalties for concealing a PEP's source of funds, meaning that firms may wish to have enhanced policies around PEPs.

Adverse media

Adverse media searches are not mandatory but may be appropriate given the risk profile and activities of the regulated firm. Despite this, stricter legislation under AMLA 2020 and the advancement of a risk-based approach suggests that higher-risk circumstances may warrant adverse media screening and may be expected by FinCEN.

ONGOING MONITORING

Transaction monitoring

One of the core requirements for regulated institutions is to conduct ongoing monitoring to identify and report suspicious transactions. Suspicious activity must be reported using the BSA E-Filing System.

Ongoing KYC

Firms are required to maintain and update customer information in line with a risk-based approach and as a result of normal monitoring. However, no specific schedule is mandated.

THE EU

Although there is no EU-wide regulatory framework for online gaming, each member state has its own national regulations and its own regulator. As an exception to Article 26 of the Treaty on the Functioning of the European Union, which upholds the "freedom to provide services to recipients in other EU countries", there is no obligation to recognize authorizations or licenses for gaming services from other EU countries, meaning cross-border activity is not permitted. Additionally, the right to restrict inter-country gambling services to protect public interest objectives including gaming addiction, crime, fraud or protecting minors, is explicitly recognized by the EU's Court of Justice.

The EU's 5th Anti-Money Laundering Directive of 2018 expanded the definition of regulated sectors to bring the online gaming industry within the scope of the directive. This means gaming operators must abide by AML /CTF regulations in the relevant EU state.

Relevant regulations:

All online gaming operators are required to comply with:

- 4th, 5th and 6th Anti-Money Laundering Directives
- Relevant national legislation, e.g., the French Online Gambling Act of 2010 and the German State Treaty on Gambling of 2021

Specific regulatory requirements vary from country to country. However, the European Gaming and Betting Association's AML /CTF Guidelines for the online gambling sector state that customer due diligence should be carried out upon the collection of winnings, the wagering of a stake or both, when carrying out transactions amounting to €2,000 or more, whether the transaction is carried out in a single operation or in several seemingly linked operations.

CONCLUSION

As the online gaming industry grows, more regulatory pressure and enforcement can be expected. While the UK clamps down on social responsibility factors, the less mature U.S. gaming market will likely see more enforcement as the online gaming industry grows and becomes legal in more states. Alongside traditional money laundering and terrorist financing risks, operators must grapple with licensing conditions and social responsibility risks. To keep up with this pace of change in a sustainable way that fosters growth, online gaming operators are increasingly turning to technological solutions that streamline their compliance processes and keep them in step with the industry's ever-changing requirements.

FINTRAIL is a global consultancy passionate about combating financial crime. We've worked with over 100 global leading banks, FinTechs, other financial institutions, RegTechs, startups, venture capital firms and governments to implement industry-leading approaches to combat money laundering and other financial crimes. With significant hands-on experience in the US and UK, we help you prepare, assure, and fortify your controls to meet evolving regulatory requirements. Get in touch here.

Jumio helps organizations to know and trust their customers online. From account opening to ongoing monitoring, the Jumio KYX Platform provides advanced identity proofing, risk signals and compliance solutions that help you accurately establish, maintain and reassert trust.

Leveraging powerful technology including automation, biometrics, AI/machine learning, liveness detection and no-code orchestration with hundreds of data sources, Jumio helps you fight fraud and financial crime, onboard good customers faster and meet regulatory compliance including KYC and AML. Jumio has processed more than 1 billion transactions spanning over 200 countries and territories from real-time web and mobile transactions.

Based in Sunnyvale, California, Jumio operates globally with offices in North America, Latin America, Europe, Asia Pacific and the Middle East and has been the recipient of numerous awards for innovation. Jumio is backed by Centana Growth Partners, Great Hill Partners and Millennium Technology Value Partners. For more information, please visit jumio.com.