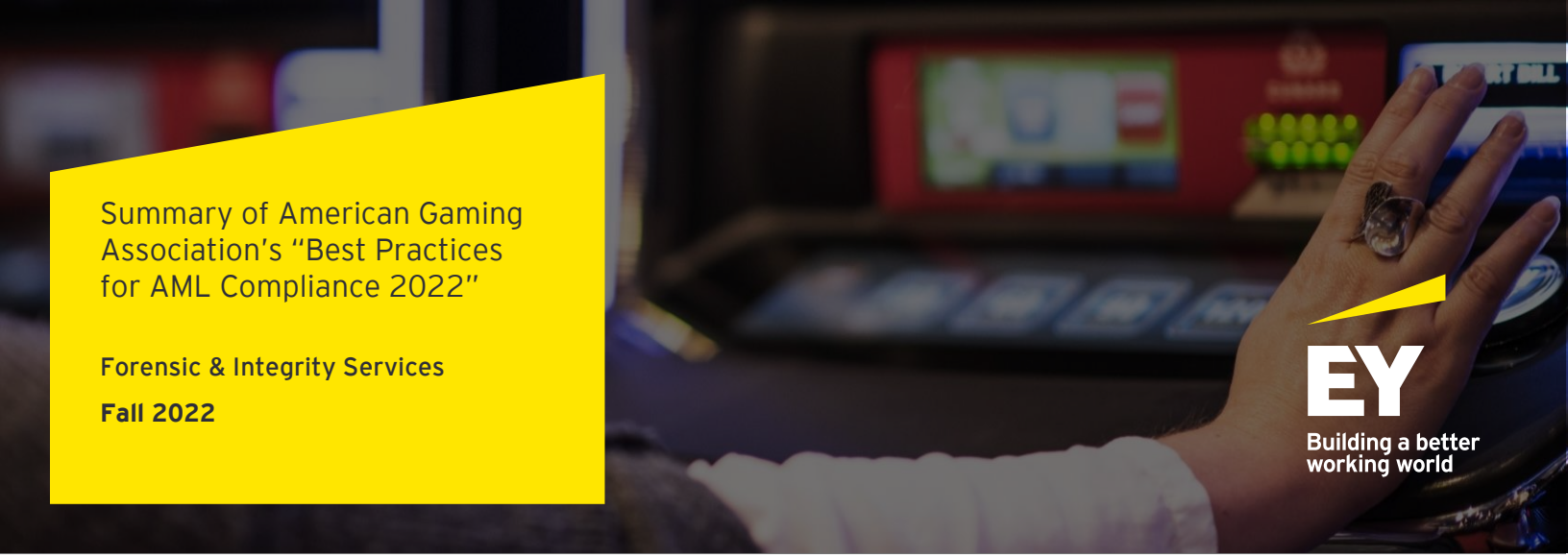

Summary of American Gaming Association's "Best Practices for AML Compliance 2022"

Forensic & Integrity Services

Fall 2022

EY
Building a better working world

Recent updates and digital operation focus

The American Gaming Association (AGA) recently released the third edition of Best Practices for Anti-Money Laundering (AML) Compliance[1], providing an update for the gaming industry that reflects the continued expansion in laws, regulatory environment, and growing sports wagering and iGaming operations across the United States. The AGA has revised and expanded their guidance on AML compliance, including compliance obligations for digital operations, and guidance around the impact of digital payments, cashless wagering and cryptocurrency. The AGA has also highlighted the linkage between money laundering and fraud, citing the 2022 National Money Laundering Risk Assessment (NMLRA)'s seven principles and Financial Crimes Enforcement Network of the U.S. Department of the Treasury (FinCEN)'s national AML/combating the financing of terrorism (CFT) priorities, both of which highlight fraud as a driver of money laundering activity.

The gaming industry has evolved substantially since the last iteration of the AGA's Best Practices publication in December 2019, specifically in the digital space. Updated guidance, risk indicators, compliance obligations and other essential information are broadly incorporated throughout with a focus on the existing and emerging risks pertaining to the digital space, and the corresponding preventative measures. These include:

Key consideration topics	AGA Best practice takeaways
Risks associated with organized, large-scale cyber-enabled crimes, such as identity and credit card theft fraud rings	▸ **Industry guidance:** Large-scale fraud rings have targeted online gaming and sports wagering operations due to the ability to create or takeover multiple accounts quickly to move funds, oftentimes using stolen identities. ▸ **Best practice considerations:** Given the AGA's emphasis on preventative measures, operators should consider establishing preventative tools focused on geolocation. This includes monitoring patron account for device sharing, common IP addresses and indicators of multi-accounting, such as players utilizing the same or similar contact information across accounts.
Risks associated with the types of online fund deposit and withdrawal methods	▸ **Industry guidance:** Offering multiple forms of online fund deposit and withdrawal increases the risks of coordinated efforts to launder money between accounts, using one type of account to deposit funds, and another to withdraw. While online transfers mean that these transactions are cashless and therefore not subject to currency transaction report (CTR) requirements, operators should still evaluate and implement procedures that review transactions at a certain threshold or risk profile. ▸ **Best practice considerations:** Operators should, where possible, return funds to the method paid, implement payment controls around deposits and withdrawals requiring the account information to match that of the patron's account with the operator, and consider analyzing patron accounts with multiple payment methods and consecutive deposits within a short period of time.
Risks related to the acceptance of cryptocurrencies, a blockchain-based technology, as an alternative payment method for online gaming and sports wagering	▸ **Industry guidance:** Accepting cryptocurrencies as a form of payment allows operators to benefit from the decentralized record-keeping properties of cryptocurrency, however, the changing regulatory landscape and overall volatility of the market creates additional risks for digital operators to consider. ▸ **Best practice considerations:** As operators consider expanding their deposit and withdrawal methods to include cryptocurrency, additional steps, such as the conversion of funds into cash, should be implemented. By requiring virtual currency be converted to US dollars prior to deposit or wagering, this will subject the activity to the same CTR requirements, suspicious activity review and monitoring as other cash transactions conducted at the casino.

[1] https://www.americangaming.org/wp-content/uploads/2022/07/AGA-AML-Best-Practices-Guide-2022.pdf

Key consideration topics	AGA Best practice takeaways
Risk associated with customer identity verification in the virtual environment and the benefit of leveraging third-party databases and solutions	▸ **Industry guidance:** Casinos should examine their risk-based approach to identification and verification. ▸ **Best practice considerations:** Some operators allow for accounts to be established in person, while others take a non-documentary approach and require the patron to enter personal identifying information (PII) into their online platform, which is then independently verified through a comparison of information obtained from consumer reporting agencies, public databases or other third-party electronic ID verification services.
Risk that casino employee training programs do not address risks specific to digital operation environments	▸ **Industry guidance:** Trainings should be department-specific and address risk factors that are pertinent to digital operations, as the risks associated to digital gaming are different than traditional brick-and-mortar operations. ▸ **Best practice considerations:** Ongoing training should be provided to employees with customer-facing roles such as customer service, customer experience or other employees who would not traditionally be given training on how to identify suspicious behavior. Specialized training should also be provided to those reviewing patron transactions, such as compliance investigators, and should be refreshed periodically to capture new and growing threats in the digital space. All employees, regardless of their role, should be able to understand their role in the overall AML program and be informed on how to identify and escalate suspicious typologies.

Each operator has a unique risk profile based on their size, geographic footprint, product offerings, wallet options and patron demographic. The online gaming space is constantly evolving as new jurisdictions are becoming accessible on a regular basis, which in turn means operators' risks profiles are constantly evolving and need to be assessed. In addition, operators should be aware of how risks can affect their business as they continue to grow. Ernst & Young LLP (EY) has observed instances of cybercrime involving fraud-related transaction activity where patrons were defrauded of funds through identity theft or other means, and the online platform was subsequently utilized to launder the money. Given the large amounts of funds that money launderers can potentially encounter, bad actors may be drawn to larger casinos or online platforms with higher levels of game play and traffic. Through EY's experience conducting annual AML and Fraud programs assessments, investigations, risk assessments, transaction monitoring tuning services and training to gaming clients, we have observed very distinctive shifts in the volume of fraud, money laundering typologies, account takeover and other schemes with online gaming clients.

With additional jurisdictions approving digital gaming, existing and incoming online gaming and sportsbook operators should be prepared to evaluate the overall adequacy and compliance of their AML programs and leverage the information available from the AGA's most recent publication. This analysis should be performed periodically, addressing any potential gaps across various elements of their AML program against updated regulatory requirements and emerging industry trends.

Ernst & Young LLP contacts

Arpi Lal
Forensics Partner
+1 212 773 3038
arpi.lai@ey.com

Alexander Perry
Forensics Managing Director
+1 212 773 7845
alexander.perry@ey.com

Bob Boyle
Forensics Senior Manager
+1 212 773 1335
bob.boyle@ey.com

Elise Lebourg
Forensics Senior Manager
+214 969 9564
elise.lebourg@ey.com

EY | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

US SCORE No. 17094-221

US.2208-4081461
ED None

ey.com/us/forensics