

# Enhancing iGaming Security Through Smarter ID Verification



# How identity verification can help fight money laundering in iGaming

Money laundering is a global issue and the amount being laundered [is estimated to be somewhere between \\$800 billion–\\$2 trillion](#). New measures against money laundering, for example the 6th Anti-Money Laundering Directive (AMLD6) in the European Union (EU) and generally tougher Know Your Customer ([KYC](#)) requirements, the war on “dirty

money” has led to the development of more creative schemes from fraudsters. One of the largest growing industries, iGaming has always been hit massively by scamsters. Businesses and platforms that fail to implement proper identity verification risk taking regulatory penalties, revocation of gaming licenses, and long-term reputational damage.

## iGaming industry hit by \$184.4 million in AML fines

The iGaming industry has come under increasing regulatory pressure as global authorities issued [\\$184.4 million in anti-money laundering fines in 2024](#). These penalties reflect the heightened focus on enforcing compliance and strengthening KYC standards across the industry. The global online gambling market [was \\$93.26 billion in 2024 and is projected to reach \\$153.21 billion by 2029](#)—indicating a compounded annual growth rate (CAGR) of 10.44% from 2024 to 2029. Regulators are intensifying oversight to reduce financial crime risks to gambling platforms.

### Case study: How a major AML failure triggered regulatory action

In 2023, [William Hill was fined a record £19.2 million by the UK Gambling Commission \(GC\)](#) for widespread AML and safer gambling failures. The bookmaker allowed customers to deposit and lose tens of thousands within minutes, often without verifying identity or checking sources of funds. These failings exposed major gaps in due diligence, risk monitoring, and internal controls—especially around VIP players.

The Commission considered suspending William Hill’s license but settled on a massive fine and strict remedial actions, including independent audits and executive accountability. The case highlighted a broader industry trend of prioritizing revenue over compliance and sent a clear message: Gambling firms must take AML and consumer protection seriously—or face severe consequences.

## How fraudsters use crypto to commit fraud

For businesses operating in gaming, iGaming, or fintech, the adoption of cryptocurrency as a payment method introduces both opportunities and risks.

While crypto attracts new customers and enables faster payments, it also creates vulnerabilities.

The appeal of cryptocurrency to those involved in financial crime can be traced to several key characteristics:

- **Anonymity:** No personal details required to set up wallets.
- **Speed:** Transactions occur in seconds, across jurisdictions.
- **Global reach:** Cross-border transfers face minimal friction.
- **Limited regulation:** Varies widely across countries, leaving loopholes.

The challenge lies in creating processes that don't add unnecessary friction for genuine users, while still ensuring strong defenses against bad actors.

## Navigating cross-border compliance challenges

The iGaming industry faces one of its biggest hurdles in managing compliance across multiple jurisdictions.

Regulatory frameworks differ widely between countries, creating a fragmented environment that complicates AML and KYC operations for global operators.

## Different rules, same risks

While the EU's AML directives aim for harmonization, implementation varies by member state. Some regulators require enhanced due diligence for low-value transactions, while others allow a more flexible, risk-based approach. In Malta and outside the EU, markets like the United Kingdom (UK) and Gibraltar have developed their own AML and licensing requirements—each with distinct reporting standards and audit expectations.

## Key challenges for operators

- **Inconsistent onboarding requirements:** Verification processes and acceptable ID standards differ, increasing operational costs and customer friction.
- **Conflicting data laws:** General Data Protection Regulation's (GDPR) strict privacy rules in Europe often clash with data retention obligations in other regions.
- **Uneven regulatory enforcement:** Ambiguity over what qualifies as "adequate" AML controls makes compliance harder to standardize.
- **Rising compliance costs:** Maintaining regional expertise, localized systems, and multiple reporting lines adds significant expense and complexity.

Global operators must therefore balance regulatory precision with operational efficiency—adapting to local requirements without compromising customer experience or compliance integrity.

## How AML regulations are fighting money laundering

Below we see how key jurisdictions are approaching AML regulations to ensure compliance in the iGaming sector.

### European Union

The EU has developed strict AML rules through directives such as [AMLD4](#) and [AMLD5](#), which impact iGaming and gaming operators. These regulations require platforms to:

- Verify customers' identity
- Conduct risk assessments
- Monitor transactions
- Report suspicious activities

The European Gaming and Betting Association ([EGBA](#)) has issued updated AML guidelines for online gambling operators. These guidelines cover areas like customer due diligence (CDD), risk assessments, and transaction monitoring.

Building on these frameworks, the AMLD6 was officially adopted on 19 June 2024 and came into effect 20 days later. It gives EU Member States three years to implement the new rules. AMLD6 introduces stronger coordination between regulators, expands the definition of money laundering offenses, and increases penalties for non-compliance. It also works alongside the new Anti-Money Laundering Regulation (AMLR), which establishes a single rulebook across the EU and caps cash payments at €10,000 to strengthen financial transparency.

Some EU countries have already adopted AMLD6, with several operators reportedly losing licenses for failing to meet the new standards. To ensure consistent supervision, the EU also established the Anti-Money Laundering Authority ([AMLA](#))—a centralized body based in Frankfurt, set to begin operations in mid-2025. AMLA will oversee high-risk cross-border entities and coordinate national regulators.

AMLA's primary role is to coordinate national authorities to ensure the consistent application of EU anti-money laundering and countering the financing of terrorism (AML/CFT) rules.

A key aspect of AMLA's mandate is to [harmonize supervision across the EU](#), addressing the challenges posed by fragmented national approaches. This includes enhancing cooperation among financial intelligence units and ensuring that all obliged entities adhere to a unified set of standards



## United Kingdom

[The UK Gambling Commission \(GC\) released updated guidance on AML and terrorist financing risks](#), highlighting emerging threats in online gambling. Operators were warned about the use of AI tools to bypass due diligence, fraudulent accounts created using personal details acquired from third parties, and vulnerabilities in open-loop payment systems.

## United States

The US iGaming market is highly fragmented, with regulation and AML compliance enforced primarily at the state level. [Operators must navigate a patchwork of state laws and verification standards](#)—creating significant operational and AML challenges when scaling across multiple states.

Separately, the National Council of Legislators from Gaming States ([NCLGS](#)) and related stakeholders are pushing for a model “golden standard” framework that would make it easier for states to adopt consistent legal and AML rules.

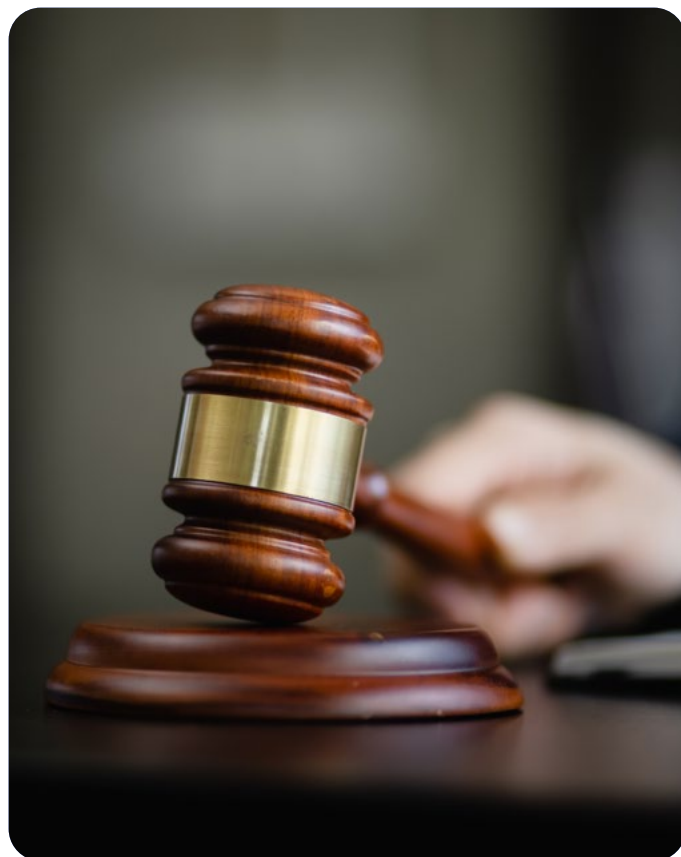
## Asia-Pacific

In the APAC region, AML regulations in iGaming vary widely. Singapore and Hong Kong maintain some of the strictest frameworks, permitting only government-licensed betting and lotteries, all under stringent AML oversight.

Elsewhere, [countries like the Philippines, Australia, and Japan](#) have begun tightening their rules to curb illegal offshore platforms.

## Latin America

Across LATAM, markets such as [Brazil, Mexico, Colombia, and Argentina](#) are rapidly reforming their [gambling laws](#) to align with Financial Action Task Force (FATF) recommendations. Governments are introducing licensing frameworks, KYC obligations, and real-time reporting systems to combat money laundering. Despite fragmented adoption, the trend is toward regional cooperation and standardization to ensure AML compliance in both retail and online gaming.



## Best practices to strengthen KYC and AML compliance

While the risks and penalties for non-compliance are significant, proactive measures can help operators build stronger defenses against financial crime. A structured, risk-based approach to compliance not only protects revenue but also enhances player trust and operational resilience.

### Conduct regular AML and KYC audits

Periodic internal and third-party audits help identify weaknesses in verification, reporting, and transaction monitoring processes. These reviews ensure that controls remain effective and aligned with the latest regulatory standards.

### Adopt risk-based customer segmentation

Not all players pose the same level of risk. Operators should classify customers based on risk factors such as location, transaction size, and source of funds. This allows for enhanced due diligence where it matters most, without burdening low-risk users.

### Leverage AI and automation for identity verification

AI-driven tools can analyze user behavior, document authenticity, and transactional anomalies in real time. Automation reduces manual errors, accelerates onboarding, and improves detection of fraudulent activity or identity theft.

### Ensure continuous staff training

Compliance teams and customer support staff must stay up to date with emerging threats, typologies, and regulatory changes. Regular workshops and certifications reinforce a culture of compliance and accountability across the organization.

### Implement ongoing monitoring and reporting

Continuous monitoring of player activity helps detect suspicious behavior early—before it escalates into a reportable offense. Integrating alerts and analytics into the compliance workflow ensures faster escalation and better traceability.

By combining technology, training, and tailored risk assessment, iGaming operators can reduce exposure to regulatory penalties while maintaining a seamless and secure user experience.

## An all-in-one identification and compliance platform

The challenge lies in creating a pleasant user experience while also adhering to both federal and local KYC and AML regulations.

At G2RS, we bring together leading data and verification providers, giving businesses a unified platform to strengthen KYC workflows. From online ID verification and Electronic Identification (eID) solutions to Politically Exposed Person (PEP) and sanctions screening, our solutions help businesses fight financial crime while protecting customers.

[Contact us](#) to learn how you can protect your business with our robust IDV solutions.