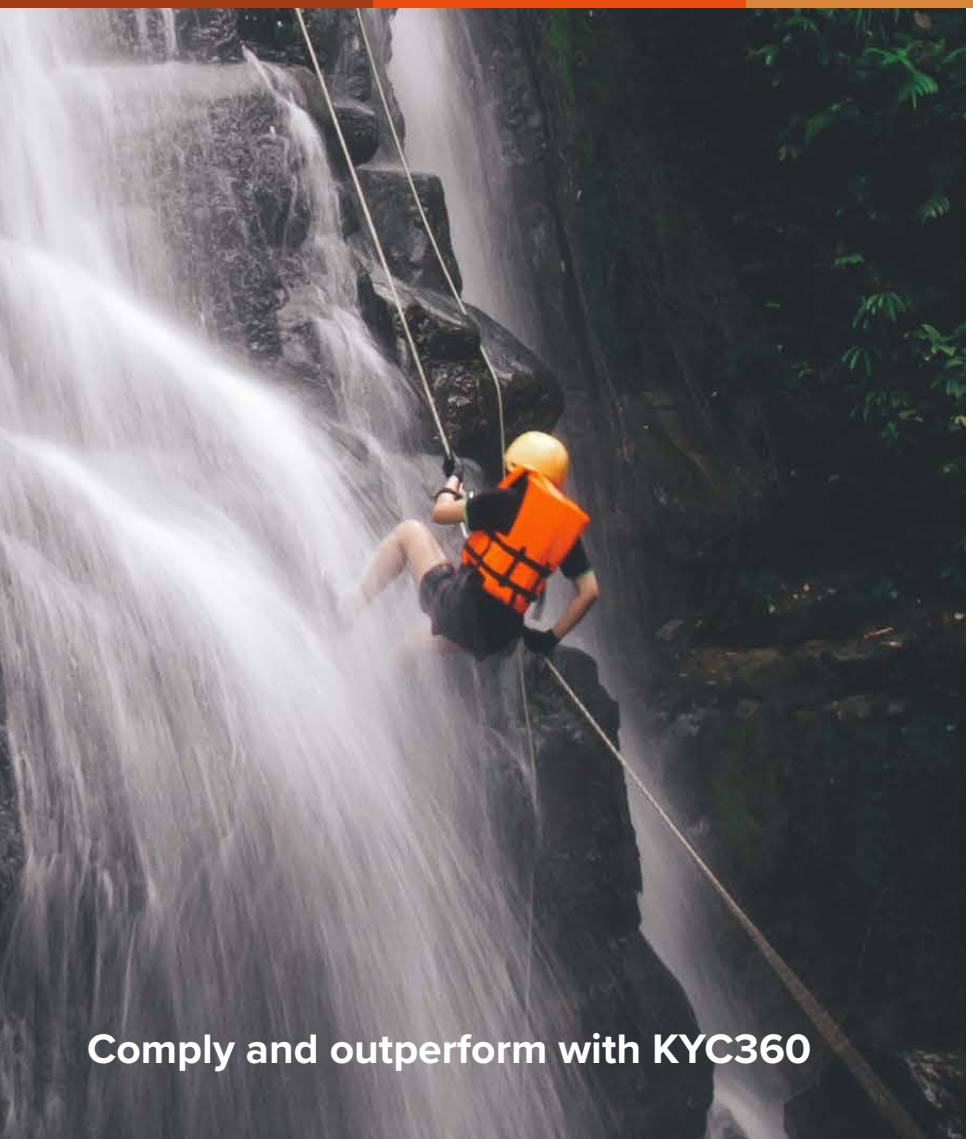
KYC360

AML and KYC Vulnerabilities for

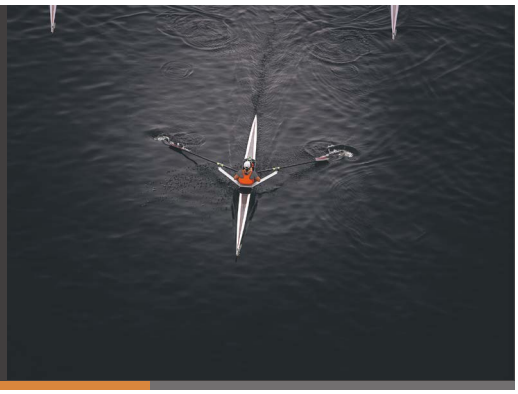
Gaming and Gambling



Comply and outperform with KYC360

KYC360

Spotlight on Gaming and Gambling



Gaming and gambling companies risk getting caught in a pincer movement.

On the one hand, criminal groups are eyeing the potential opportunities afforded by the industry to launder the proceeds of wrongdoing, particularly as online gambling has boomed.

On the other, regulators, alert to this danger, are increasingly cracking down on companies judged to have fallen short on know your customer (KYC), anti-money laundering (AML) and countering the financing of terrorism (CFT) standards.

The fines continue to mount up. In March 2022, the UK Gambling Commission fined 888 UK Limited £9.4m for a series of money laundering and social responsibility failings. The penalty followed a £2m fine levied just two months earlier against BetVictor relating to similar issues. Action against Genesis Global went even further, resulting in a £3.8m fine and a three-month suspension of its licence to operate. The scale and frequency of these penalties underline exactly what is at stake for companies that fail to stay on top of AML and CFT compliance.

It's also important to note that gambling is one of the few industries beyond financial services to count as part of the regulated sector for the purposes of money laundering legislation. As a result, the potential regulatory sanctions include formal warnings, substantial fines, the possibility of operating licences being suspended or revoked, and the launching of mandatory audit investigations.

Moreover, these direct impacts on gaming and gambling companies come with additional costs. Regulatory sanction can lead to substantial reputational damage and hinder business growth. The costs of correcting compliance deficiencies are often extremely high. There is even the potential for individuals in the company to face legal action, which could result in fines and even prison sentences.

Against this backdrop, it has never been more important for the industry to focus on its AML and CFT responsibilities. Increasingly, the risk of a policy or process failure can threaten the very existence of the business.

KYC360

Where Gambling and Gaming face risks

KYC and AML are powerful complements to each other and important elements for gaming and gambling operations looking to protect themselves against fraud and financial crime. Both involve verifying the identity and legitimacy of individuals and organisations through rigorous checks. In itself, that makes it harder for criminals to operate. In addition, AML checks help to uncover the money trail, understanding where money comes from and how it's spent so that companies can ensure it's not laundered through them.

The Financial Action Task Force (FATF), the inter-governmental body responsible for setting worldwide AML standards, is very clear on its view that the gaming and gambling industry is a high-risk industry. It published its very first major report on the problems posed by the sector more than a decade ago and has updated its guidance at regular intervals ever since.

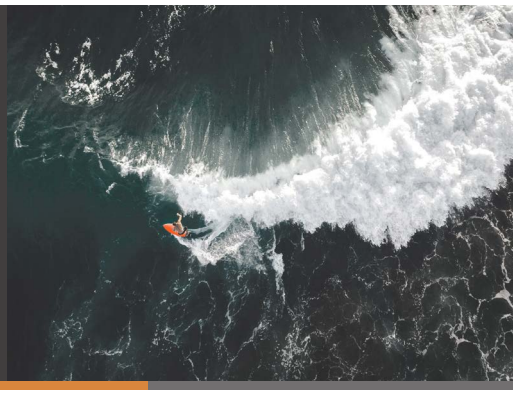
The unpalatable truth for gaming and gambling businesses is that their industry has always been attractive to individuals and groups seeking to legitimise the proceeds of crime. Long before online gaming surged in popularity, live casinos accepted cash payments for chips, which money launderers could then play for a short period before cashing out their money in the form of a legitimate check. Bookmakers and fixed-odds betting terminals afford similar opportunities.

The growth of the online sector has certainly upped the ante, with huge sums now flowing through online casinos, digital sportsbooks and similar services. It is forecasted that the global online gambling industry is expected to be worth $94bn in 2024 which provides ever-increasing opportunities to hide criminal money in plain sight.

Even simple strategies can be difficult to detect. For example, money launderers deposit illegal cash in an online betting account, make a few small bets for the sake of appearances, and then transfer what is left to a bank account in what appears to be a legitimate transaction. Criminals breaking down large sums into smaller amounts by opening multiple accounts in this way may be hard to spot; in the meantime, they create a useful paper trail for their cash.

KYC360

Where Gambling and Gaming face risks



It is also important to recognise that the definition of money laundering is broader than is often realised. As well as the conversion of dirty money to clean cash, it includes the disposal of the proceeds of crime.

As a result, when the gaming and gambling industry fails to prevent criminals spending the proceeds of their illegal activity, it may also fall foul of compliance failures. These are also broad-based risks.

The FATF identifies at least nine ways in which gaming and gambling companies may be particularly vulnerable to money laundering:

/ **Proceeds of crime.** Any business accepting payments from retail customers faces the risk that the cash has come from illegal activities, but the volume of customers with which gaming and gambling companies deal increases this vulnerability.

/ **Cash payments.** Live casinos and other physical gaming and gambling environments accept cash payments, providing criminals with a means to legitimise this money.

/ **Transfers between customers.** Many online casinos and gaming sites enable customers to easily move money between themselves.

/ **Improper use of third parties.** Criminals may use third parties to gamble on their behalf to avoid customer due diligence checks.

/ **Casino deposit accounts.** These can be used to deposit and withdraw cash, with the holder engaging in little or no gambling activity.

/ **Pre-paid cards.** Can be purchased with cash and make it difficult for operators to make suitable checks on the holders.

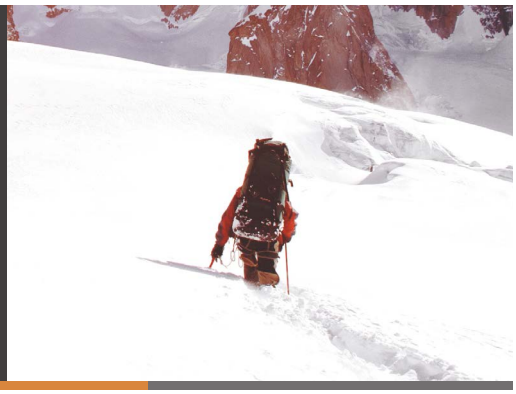
/ **Identity fraud.** A common money laundering tactic is to open gaming accounts with stolen identities; the accounts can then be used with impunity.

/ **Multiple accounts.** Many customers legitimately hold multiple accounts with the same company, which may operate many different web sites or gaming activities. This also provides criminals with an opportunity to break up large sums into smaller amounts.

/ **Multiple operators.** Some gambling platforms support different operators offering their products and services in a single venue. This may make it more difficult to keep track of customers' activities, and spot suspicious behaviour.

KYC360

The regulatory environment for Gaming and Gambling



The duty of gambling providers to report suspicions or knowledge that a customer is using the proceeds of crime to gamble, or using their services to launder money, dates back to the Proceeds of Crime Act 2002. Failure to do so is an offence that carries a maximum penalty of five years imprisonment.

More recently, the UK Government's National Risk Assessment of Money Laundering and Terrorist Financing specifically warned that criminals were targeting gaming and gambling operators.

The Money Laundering Regulations 2017 introduced specific requirements for areas of the industry, including requiring operators to conduct written assessments of their vulnerabilities to money laundering. This assessment should be reviewed annually, or more regularly if an update is required, and be available for inspection.

Other industry-specific regulation requires gaming and gambling operators to:

- Carry out enhanced due diligence on any customer placing bets totalling €2,000 or more in a 24-hour period.
- Screen relevant employees before they are appointed and then on an ongoing basis.
- Appoint a member of the board of directors or senior manager as the officer responsible for regulation compliance.
- Establish an independent audit process to assess the effectiveness of measures introduced to comply with the regulations.
- Appoint an individual in the firm as the nominated officer.
- Inform the Gambling Commission of the identities of the person responsible for compliance with the regulations and the nominated officer within 14 days of their appointments.

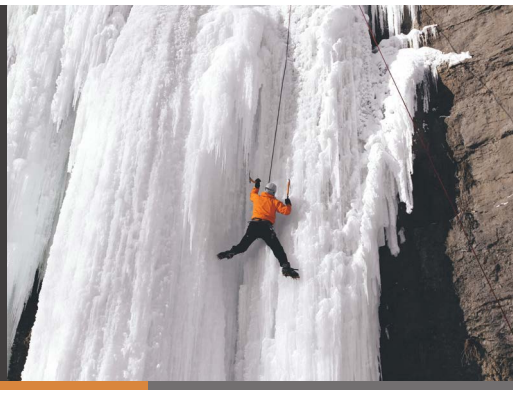
In addition, holders of remote casino operating licenses (online operators) must carry out enhanced customer due diligence; including checks on whether a customer is a Politically Exposed Person (PEP) or a relative or close associate of one.

As the supervisory authority for the UK's gaming and gambling industry, the UK Gambling Commission takes primary responsibility for enforcing money laundering regulation in the sector, though in practice, it may work alongside agencies such as the National Crime Agency.

The Gambling Commission publishes detailed guidance on the approach it takes to regulating both remote and non-remote operators. Its legal framework reflects the FATF's recommendations for a risk-based approach, which gives organisations some flexibility to devise policies, procedures, and controls that are appropriate to their assessment of the money laundering and terrorist financing risks they face.

KYC360

The regulatory environment for Gaming and Gambling



/ The international perspective

Regulators around the world have responded to the FATF's focus on gaming and gambling, by introducing their own frameworks and standards. Operators will need to have a detailed understanding of the legislative environment in each of the jurisdictions where they have operations.

In the European Union, new money laundering measures came into effect in January 2020 under the EU's 5th Money Laundering Directive. Changes that are particularly relevant to the gambling sector include Regulation 19, which requires all operators to have appropriate anti-money laundering measures in place when launching new products or business practices; Regulation 24, which sets out how agents working with casinos should be given training on such issues; and Regulation 28, which details what information is acceptable as a reliable source when a person's identity is being verified.

In the US, in states where gambling is legal, the Financial Crimes Enforcement Network is responsible for policing the money laundering risk in the sector. In addition, FinCEN publishes specific advice for online casinos. Operators in the US will also need to take onboard the requirements of the Interstate Wire Act and The Unlawful Internet Gambling Enforcement Act.

/ Complying with sanctions

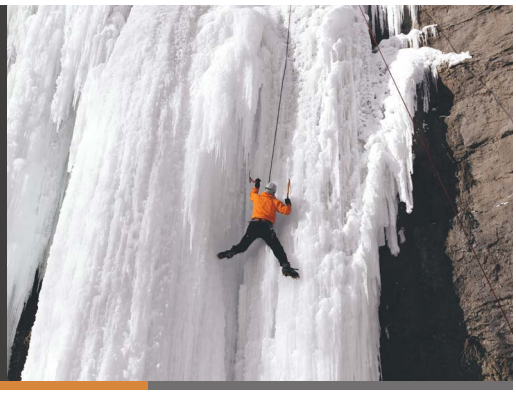
All organisations are required to comply with sanctions and export controls that may be imposed by the UK Government or other jurisdictions on specific individuals or corporate entities. The number of these sanctions currently in force has increased significantly in recent months as the international community has targeted Russia and Russian entities following its illegal invasion of Ukraine.

In February 2022, the Gambling Commission published guidance for the sector, reminding operators of their legal responsibilities under sanctions legislation.

The guidance focuses on Russian sanctions in particular but applies to any sanctions currently in place.

KYC360

How to comply with AML and KYC regulation



With so much focus on the gaming and gambling industry's vulnerability to money laundering, the sector cannot afford to neglect its compliance responsibilities. This will require action across several different areas.

/ Customer due diligence

Knowing your customer (KYC) is a basic requirement for gaming and gambling operators. They must take measures to identify and verify the identities of new customers before accepting their business. In addition, they must assess the extent to which each customer poses a risk from an AML perspective and gauge their response accordingly.

Risk-based customer due diligence considers factors such as who the customer is, what they do, where they live and do business, and the nature of the product or service they require. More basic checks are acceptable for those customers assessed as low risk, but operators must have a policy in place in order to make that assessment.

/ Enhanced customer due diligence

Those customers assessed as higher risk will be subject to enhanced diligence requirements. These will include a requirement for new accounts to be signed off by a senior manager, and then enhanced monitoring of the customer's activities on an ongoing basis.

/ PEP screening

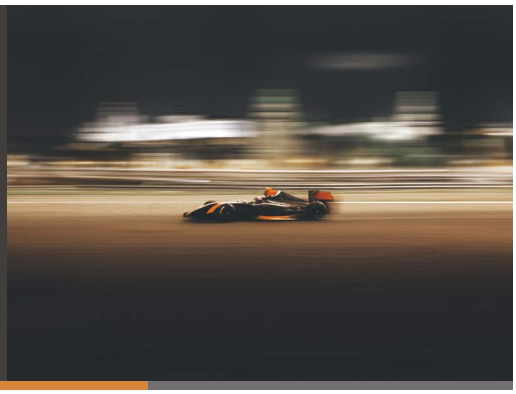
Politically exposed persons (PEPs) are individuals (and their close associates) who may be more susceptible to being involved in bribery or corruption because they hold a prominent position or influence.

For customers identified as PEPs, enhanced AML checks will be necessary, so these individuals must be identified, typically at the onboarding process, but also on an ongoing basis.

There is no global definition of a PEP, but the Financial Action Task Force has issued guidelines on how to identify such individuals; these have largely been accepted into legislation in the UK and the EU.

KYC360

How to comply with AML and KYC regulation



/ Sanctions screening

New customers may be subject to specific sanctions and export controls themselves or have links to individuals and countries that have been targeted. Operators therefore need to monitor the sanctions lists published by governments and other international organisations in order to ensure they are not in breach of these sanctions. The UK Government publishes and updates the UK Sanctions List online, with other jurisdictions following similar practices.

/ Transaction monitoring and reporting

Without robust transaction monitoring processes, gaming and gambling operators cannot be confident their services are not being used for criminal purposes. It is therefore important to have systems capable of identifying red flag transactions and sounding an alert. And where a transaction does raise concerns, operators will typically be required to file a suspicious activity report (SAR) to the National Crime Agency.

In practice, it is difficult to define precisely what constitutes suspicious activity, but regulators deliberately set out broad guidance. The Gambling Commission warns:

> "Operators and employees working in remote and non-remote casinos are required to submit a SAR in respect of information that comes to them in the course of their business if they know, or suspect or have reasonable grounds for knowing or suspecting, that a person is engaged in, or attempting, money laundering or terrorist financing."

/ The role of technology

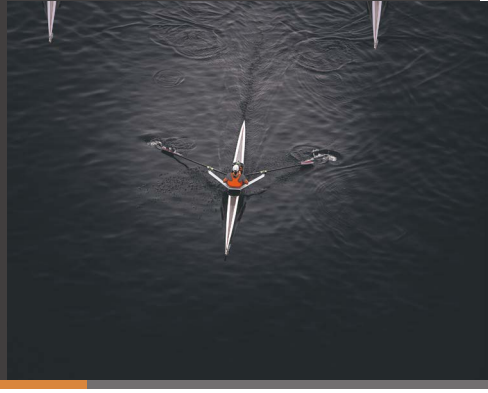
Manual solutions to AML and CFT compliance are increasingly impractical. The workload is simply too large, exposing gaming and gambling operators to regulatory sanction and reputational damage in the event that staff make mistakes or overlook problem cases.
For this reason, technologies that harness tools such as automation and machine learning are increasingly important to AML compliance.

Automating AML processes provides comfort that activities such as screening and monitoring are taking place quickly and accurately, reducing the risk of a compliance failure.
There is also an opportunity to leverage external data sources in order to strengthen compliance even further.

Another advantage of using such tools is that they automatically create an audit trail, providing gaming and gambling operators with a means through which to account for their actions to regulators and other stakeholders.

KYC360

Streamline Compliance, Elevate Customer Experience



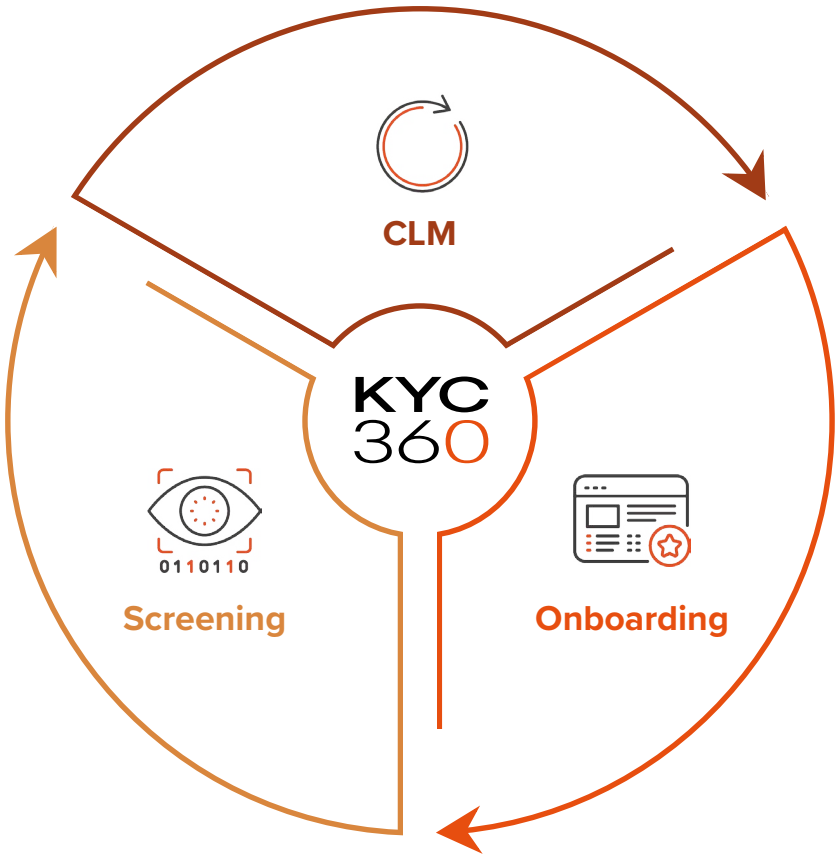
The KYC360 platform is an end-to-end solution offering slicker business processes with a streamlined, automated approach to Know Your Customer (KYC) compliance. This enables our customers to outperform commercially through operational efficiency gains whilst delivering improved customer experience and KYC data quality.

Consolidate your system stack and data vendor relationships with one platform to cover all Onboarding, Screening, Perpetual KYC (pKYC) and CLM tasks, with market-leading data sources pre-integrated under a single license agreement. Live risk scoring and automated data collection enables a shift from periodic to event-driven review, while providing a single actionable picture of real-time risk with all documents and data in one place.

Architected for rapid deployment and ROI, the KYC360 no-code SaaS platform is flexible, fully configurable and modular so that you option and pay only for the functionality you need. Whether automating identity verification and background checks or monitoring risk in real-time, KYC360 adapts to your compliance needs, scaling as your business grows.

/ Key benefits:

- Flexible
- Configurable
- No-code
- Integrated with the world's leading data suppliers allowing you to choose those that are right for your business
- Comprehensive API enabling fully headless integration of all platform features where required
- Pre-built integrations with core business systems
- Full EU data residency
- Azure and AWS hosting



LSEG RISK INTELLIGENCE / DOW JONES / Chartis RiskTech Quadrant® Category Leader KYC Solutions, 2024 / Chartis Financial Crime and Compliance 50 2025 KYC360 Winner / Chartis RiskTech100 2024

/ Full cycle Onboarding, Screening and CLM at the speed of business

KYC360

Contact

/ sales@kyc360.com

/ www.kyc360.com