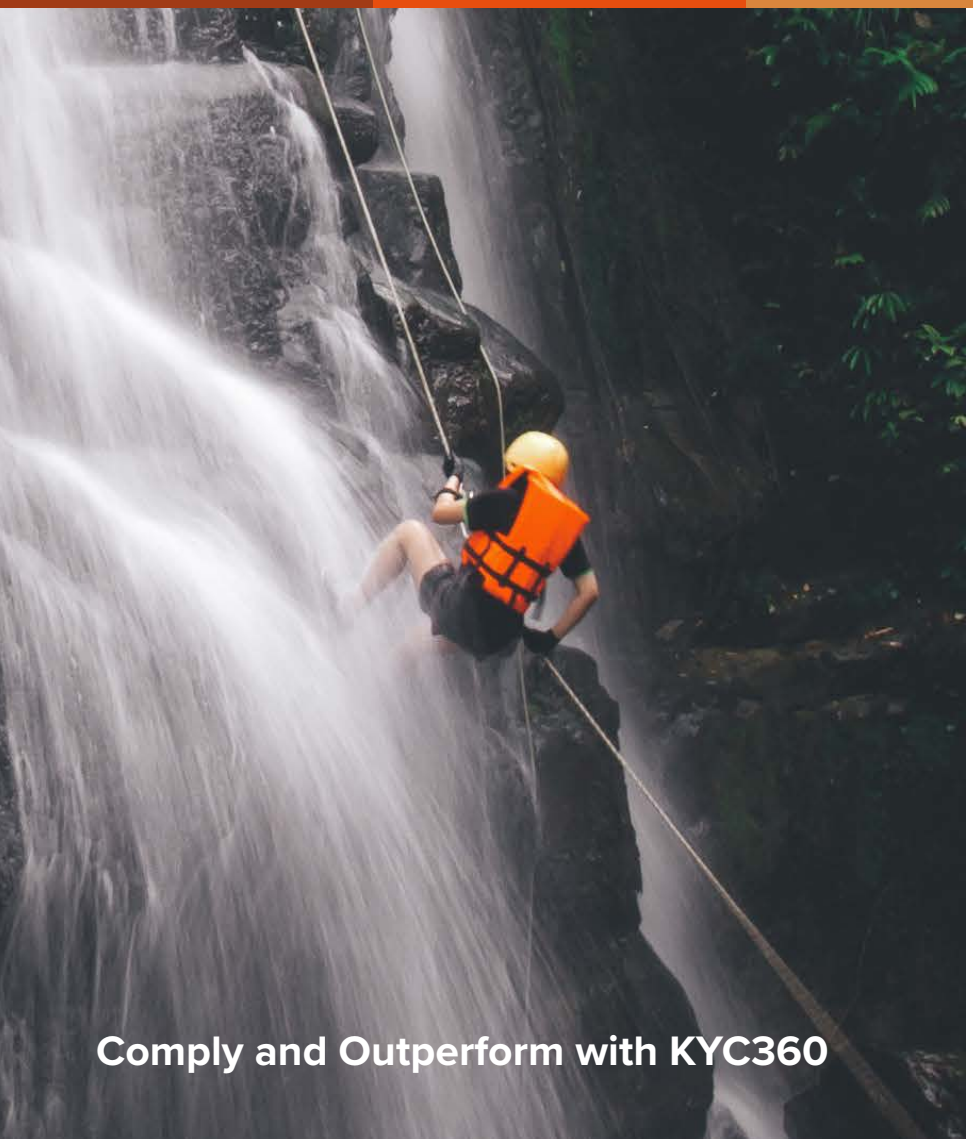
KYC360

AML and KYC Vulnerabilities in

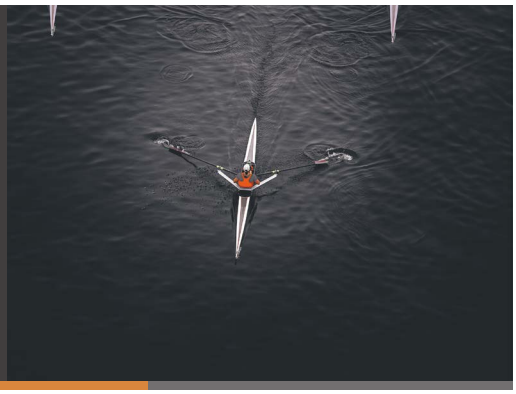
Asset Management



Comply and Outperform with KYC360

KYC360

Spotlight on Asset Management



There was a time when asset managers could afford to take a more relaxed view of money laundering risk than colleagues in other parts of financial services. That time is over. The rapid growth of the asset management industry, the increasing sophistication of financial criminals, and tighter rules on money laundering in sectors such as banking, mean asset managers are increasingly at risk.

Financial regulators are certainly taking more interest in the sector's compliance with anti-money laundering (AML), know your customer (KYC) and combating the financing of terrorism (CFT) legislation.

In 2022, the Dutch financial market regulator AFM fined the asset management business Robeco €2m for failing to make sufficient checks of its clients for money laundering. In another case, DWS Group was fined $25 million by the U.S. SEC for ESG failings and for failing to implement an effective mutual fund AML programme.

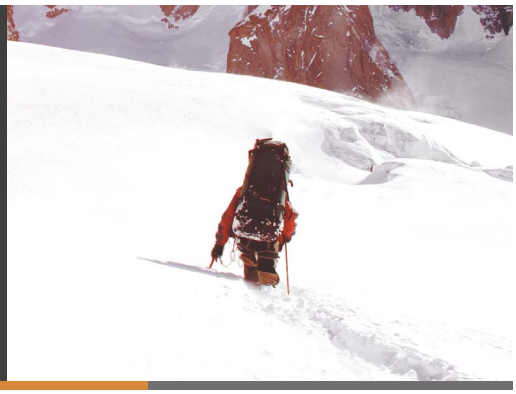
An industry expanding as quickly as the asset management sector is bound to attract attention. Ocorian's 2025 Global Asset Monitor reveals that global assets hit a record $246.8 trillion in 2024 and PWC has forecast the value of global assets under management (AuM) to reach US$171 trillion by 2028. That provides a huge opportunity for criminals to hide their money in plain sight and to seek to legitimise the proceeds of their wrongdoing.

Moreover, asset managers, wealth managers and the networks of partners through which they operate, including intermediaries, often work with complex organisational structures. Their activities frequently cross borders; the offshore finance industry is an important part of the sector and firms regard it as important to maintain client confidentiality. The effect is to create the conditions in which money laundering and financial crime may flourish.

Asset managers that fail to recognise this mounting risk – and to respond – are putting themselves in danger. It is not just the prospect of regulatory penalties that should be of concern, substantial though these can be. The reputational damage from a breach may also be significant. In addition, the regulatory burden of remediation and potentially increased supervision may be substantive. Bear in mind too that directors and senior managers of asset managers falling foul of AML regulation may be personally liable for prosecution and penalty.

KYC360

Where asset managers may be vulnerable to risk



Asset and wealth management has not traditionally been regarded as a high-risk area for money laundering. The nature of asset management activity makes it a less obvious way to launder criminal proceeds than more transactional financial services activities such as banking.

However, perceptions are shifting. In one recent survey, financial crime professionals working in the sector flagged money laundering as one of the most important risks now facing the industry; 80% also felt the risk of financial crime had increased because of shifts made by the investment industry in response to the Covid-19 pandemic. There is concern that asset managers have not invested in AML systems and controls in the same way as higher-risk segments of the financial services sector. This could make them a soft target. In practice, there are a variety of ways in which criminals might seek to launder money through the sector:

- Investment funds may be used for money laundering where a large sum of criminal money is already within the financial system. The nature of such structures means the movement of large sums of capital into or out of a fund may not be seen as unusual or even noteworthy.
- Many jurisdictions allow investments in asset management products to be redeemed to a third party, or allow the investor to re-register their shares in the fund in the name of a third party. That provides a simple way to move the proceeds of criminal activity around while simultaneously giving the money the appearance of legitimacy.
- Wealth managers, in particular, are likely to have dealings with high-net-worth individuals, who may have a preference for operating through offshore trusts or companies; the opacity of these structures may make it more difficult to ensure AML and CFT compliance.
- Research also suggests that politically exposed persons represent a particular risk to wealth management firms, which are therefore vulnerable to failures linked to bribery and corruption.
- Third party relationships may also give rise to financial crime in the asset and wealth management sector. The UK's Financial Conduct Authority (FCA) has warned that many firms do not have adequate systems and controls for assessing bribery and corruption risks in relation to relationships with parties such as agents or introducers.

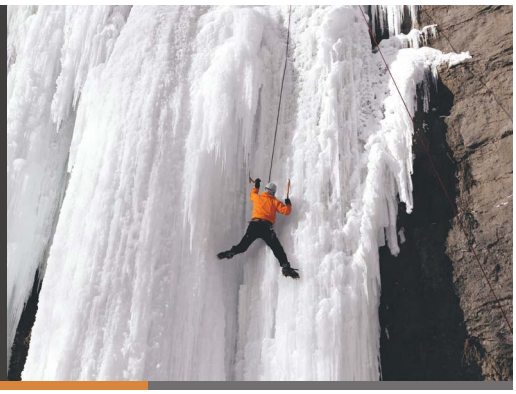
More broadly, the confidentiality that asset managers' clients routinely demand can sometimes translate to a tolerance of secrecy that plays into the hands of those with criminal intentions. Equally, for many investment managers, building very close relationships with their clients is a key element of the business model; the danger is that this level of familiarity may lead to managers allowing basic due diligence procedures to slip.

These are not necessarily new vulnerabilities. As long ago as 2014, the Financial Action Task Force (FATF), the inter-governmental body responsible for setting worldwide AML standards, highlighted how the industry's relationships often "involve the provision of financial services in a managed relationship with clients who are often of high net worth" – where it can be difficult to identify beneficial owners. There is also an increased likelihood of concealment of funds or use of offshore trusts, and banking secrecy.

Nevertheless, the level of risk continues to escalate. As asset management continues to expand and financial criminals find their ability to launder money through other routes under greater pressure, the sector will become an even more attractive target.

KYC360

The regulatory environment



The UK's Proceeds of Crime Act 2002 is the starting point for the UK's AML and CFT legislation and regulation.

The law sets out the primary money laundering offences, and imposes a duty on anyone encountering suspicious activity to report it. Failing to do so is a criminal offence in itself with a maximum penalty of five years' imprisonment.

Building on this framework, the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 introduced specific AML responsibilities for a number of key business sectors regarded as posing the greatest risk for criminal activity. These sectors include all institutions authorised to do business by the FCA (except mortgage brokers and insurance sector firms). Asset managers are therefore directly regulated on AML and CFT by the FCA.

In practice, this regulation means that the FCA will expect asset managers to have internal controls that ensure effective monitoring and management of compliance with AML policies and procedures. These controls will need to be appropriate to the business's size, the products it offers, the parts of the world where it does business and the types of customers that it serves.

Asset managers must also designate a director or senior manager with overall responsibility for AML systems and controls, and appoint a Money Laundering Reporting Officer (MLRO) whose primary focus will be AML activity and compliance with AML obligations.

/ AML regulation for asset management in the European Union

The European Union's (EU) 5th Anti-Money Laundering Directive (5AMLD), which came into force in January 2020, expanded the scope of AML regulation in areas such as customer due diligence, domestic and politically exposed persons, central registrars of beneficial ownership, and AML checks for majority-owned subsidiaries outside the EU. The 6th Anti-Money Laundering Directive (6AMLD), which came into effect in 2021, underlined these provisions, with which all asset management businesses must now comply.

In addition, individual EU member states have introduced further AML provisions on top of these bloc-wide directives. In Luxembourg, an investigation in 2018 warned of a high level risk of money laundering and terrorist financing in the investment fund sector, prompting the Commission de Surveillance du Secteur Financier, the country's financial regulator, to increase the supervision of funds and managers in the country.

In the Netherlands, the Dutch Authority for the Financial Markets now requires investment institutions to draw up transaction profiles for their clients, apply detection rules to identify suspicious transactions, and conduct timely and proper reporting to the Financial Investigative Unit.

KYC360

The regulatory environment

/ AML regulation for asset management in the US

Asset managers and investment advisors that have activities in the US are under greater scrutiny after FinCEN issued a final rule in 2024 that requires certain investment advisors to implement AML/CFT programmes and report suspicious activity related to money laundering and terrorist financing. Compliance is mandated by 1 January 2026. Elsewhere, the SEC requires businesses covered by the Bank Secrecy Act, which includes broker-dealers and other asset management industry firms, to comply with many of FinCEN's AML requirements.

Elsewhere, the SEC requires businesses covered by the Bank Secrecy Act, which includes broker-dealers and other asset management industry firms, to comply with many of FinCEN's AML requirements.

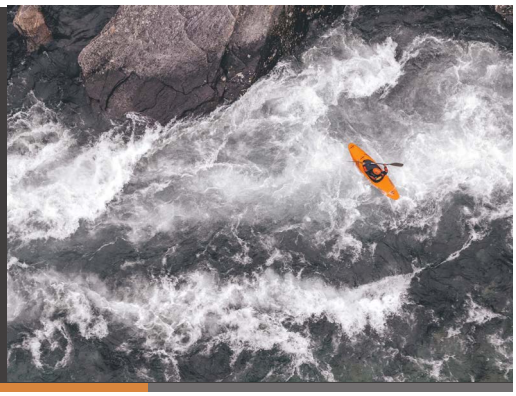
/ Complying with sanctions

All organisations – including asset and wealth managers – 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 has increased significantly in recent months as the international community has targeted Russia and Russian entities following its illegal invasion of Ukraine. In this regard, as well as identifying potential sanctions breaches in the context of its customer base, asset managers will need to review any exposures they have to Russian assets.

KYC360

How to comply with AML and KYC with regulation



The asset management sector faces a number of practical challenges as it seeks to meet its AML compliance duties.

In the UK, as noted above, the FCA takes primary responsibility for regulating asset managers' activities in a money laundering context, including their compliance with the 2017 Money Laundering Regulations. The regulator sets out the details of its requirements and expectations in Chapter 3 of the FCA Handbook. This chapter covers a broad set of duties.

The specificity of these will vary from firm to firm – and by exact nature of business – but could include:

- Equipping relationship managers to become first-line risk managers and to prevent them becoming too close to clients.
- Ensuring sufficient due diligence, particularly on source of funds and wealth.
- Establishing what is normal activity when clients have multiple business interests or sources of income.
- Maintaining oversight of controls and processes conducted by third parties such as platforms, administrators and distributors.
- Managing the risks from the use of third parties such as agents and introducers.
- Recruiting and retaining personnel who understand both financial crime risk and asset management.
- Conducting and updating granular financial crime risk assessments.

Customer due diligence

Asset managers must carry out due diligence on all customers and beneficial owners. The requirement is to "know your customer" – to make identity checks to verify that the customer is who they say they are. In practice, asset managers may take a risk-based approach; more basic checks will be acceptable for customers assessed as low-risk, but there must be a policy in place to make that assessment.

Customer due diligence duties do not end after the first checks are completed; relationships must be monitored on a continuing basis.

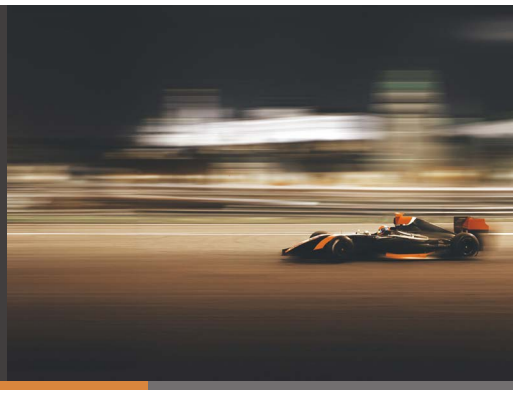
Enhanced customer due diligence

Customers who are assessed as higher risk must be subjected to enhanced due diligence requirements. Examples include situations where the customer is from a high-risk country identified by the UK Treasury, the EU or the FATF; where the customer or transaction is identified as posing a high risk of money laundering or terrorist financing.

In these cases, asset managers will be required to do more to verify the identity of the customer, and to scrutinise the source of their wealth. That might include asking for additional evidence of identity, including corroboration from independent sources, seeking expert validation of identity, and making extra financial checks. It might include asking for additional evidence of identity, including corroboration from independent sources, seeking expert validation of identity, and making extra financial checks.

KYC360

How to comply with AML and KYC with regulation



/ PEP screening

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

Where a customer is identified as a PEP, asset managers must make enhanced AML checks.

In such cases, a senior manager at the company must give their approval before a business relationship is established with the customer. In addition, there is a requirement to conduct enhanced ongoing monitoring of continuing business relationships. The FCA publishes guidance on how to identify and treat PEPs, their family members and their associates.

/ Beneficial owners

Beneficial owners are individuals who ultimately own or control the customer, or on whose behalf a transaction or activity takes place. For example, asset managers may often find their direct relationship is with a beneficial owner operating on behalf of the ultimate investor or wealth owner.

Identifying the involvement of a beneficial owner is part of normal customer due diligence checks. In such cases, asset managers must take reasonable steps to identify the beneficial owner's identity.

/ Sanctions screening

New investors may be subject to specific sanctions and export controls themselves, or have links to individuals and countries that have been targeted. Existing customers may become subject to sanctions over time. Asset managers therefore need to make checks related to this issue, bearing in mind that sanctions may be in force from both individual countries, such as the UK, and supra-national bodies such as the EU.

In the UK, the Office of Financial Sanctions Implementation offers extensive advice on sanctions and related issues. The EU publishes similar advice.

KYC360

How to comply with AML and KYC with regulation

/ Suspicious activity reports

The Proceeds of Crime Act requires the reporting of suspicious activity to the National Crime Agency. This will require asset managers to maintain systems capable of identifying activity that gives rise to suspicion.

Inevitably, the definition of suspicion is subjective. However, the broad guidance is that businesses should be concerned if they have any suspicion that the funds involved in a transaction are the proceeds of crime. There is no requirement to know what sort of crime has been committed, but one or more warning signs of money laundering which can't be explained by the customer will be relevant.

/ The role of technology

Manual approaches to AML and KYC compliance are increasingly impractical. The workload is simply too onerous, putting asset managers at risk of 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.

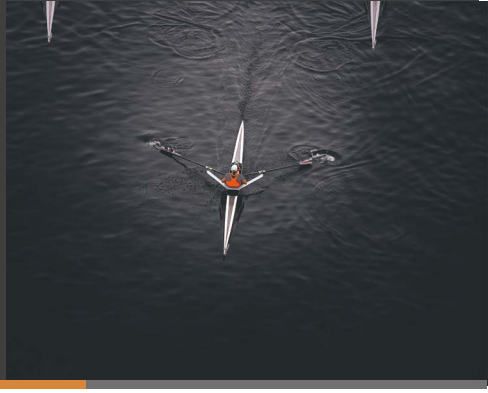
Automating AML and KYC processes provides comfort that activities such as screening and monitoring can take place quickly and accurately, reducing the risk of a compliance failure. There is also an opportunity to leverage external data sources in order to strengthen compliance even further.

Another advantage of using such tools is they automatically create an audit trail, providing the business with a means through which to account for their actions to regulators and other stakeholders. Together, AML and KYC are necessary requirements to effectively manage the end-to-end customer lifecycle.

Manual solutions to AML and CFT compliance are increasingly impractical

KYC360

Streamline Compliance, Elevate Customer Experience



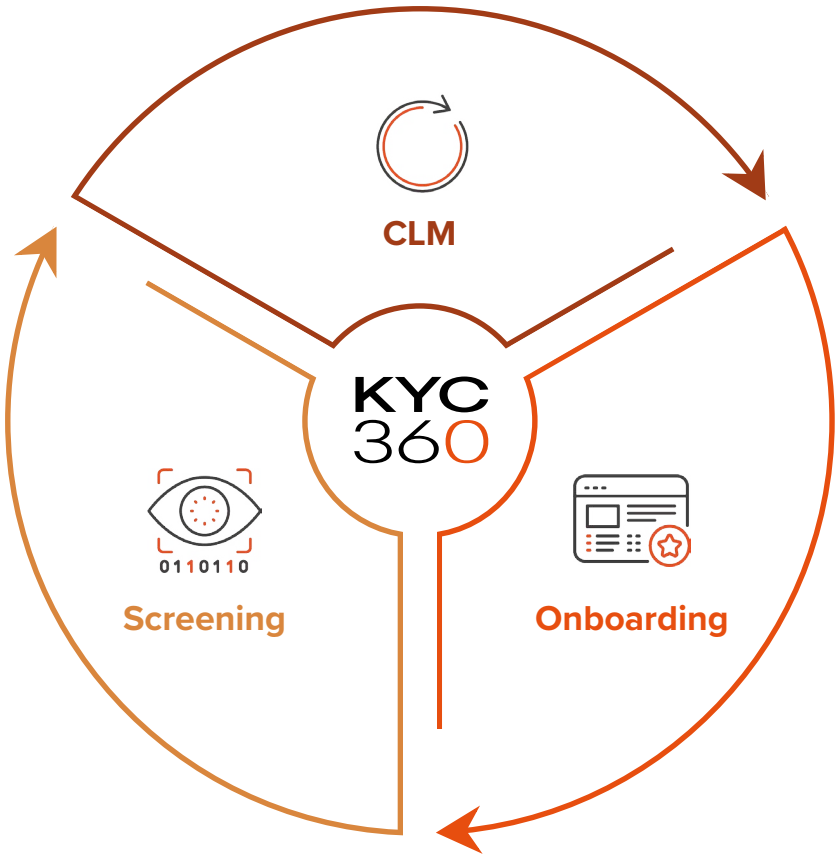
The KYC360 platform is an end-to-end solution offering slicker business processes with a streamlined, automated approach to Know Your Customer (KYC) compliance. This enables our customers to outperform commercially through operational efficiency gains whilst delivering improved customer experience and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