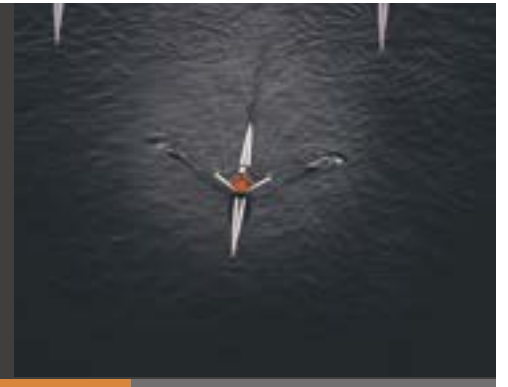


AML and KYC Vulnerabilities

in the Insurance Sector

Comply and Outperform with KYC360

Spotlight on the Insurance Sector



The insurance sector has a money laundering problem. While insurers might assume money launderers are more focused on other parts of the financial services industry – most obviously, banks – the facts tell a very different story. And policymakers in multiple jurisdictions, including the UK, are now taking action accordingly.

Research published by the accounting and consultancy firm PwC lays bare the seriousness of the problem. 46% of insurers had been exposed to fraud or financial crime over the previous 24 months according to its [2022 Global Economic Crime Survey](#).

The regulatory authorities understand this all too well; they are increasingly scrutinising insurers' anti-money laundering (AML) and know your customer (KYC) processes and practices – and handing out stiff penalties where they find failings.

In 2024, [Lombard International Assurance was fined €1.68m](#) by the Luxembourg regulator for serious shortcomings in AML controls. Cardif, the life and casual insurance subsidiary of French bank BNP Paribas, was hit with a €2.5m fine over AML failings in 2021, and in the UK, the global insurance services firm Crawford & Company, also faced enforcement action in 2021 for AML compliance mis-steps.

The problem for the insurance sector is one of perception. As businesses that sell policies, rather than managing a continuous flow of financial transactions, they appear, at first sight, to be a less obvious target for money laundering. But the reality is that huge sums flow into and out of insurance contracts, which are often complex and may involve a significant investment element. The sector is therefore a tempting target for financial criminals.

KYC and AML are powerful complements to each other and important elements for insurance businesses 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 organisations can ensure it's not laundered through them.

Where Insurers may be vulnerable to risk



In practice, a range of insurance products and policy features provide potential opportunities for money laundering. These include:

- / **General insurance.** Individuals who purchase high-value items using the proceeds of crime may insure their possessions and then make fraudulent claims for losses; the reimbursements received from insurers provide a clean source of funding.
- / **Single premium policies.** These provide an opportunity for criminals to move what may be significant sums into the financial services ecosystem.
- / **Annuity contracts.** These insurance plans pay a regular income in return for an upfront cash lump sum. They provide money launderers with an opportunity to exchange a chunk of dirty money for a regular stream of legitimate income.
- / **Cooling-off periods.** Financial regulation requires insurers to offer a refund of premiums paid if the policyholder decides to cancel within a set period following their purchase of insurance. Such refunds effectively provide money launderers with a clean source of funding.
- / **Surrender clauses.** Many insurance policies, including savings plans, offer policyholders the option of early surrender, albeit typically with a financial cost. For money launderers, these clauses provide a means to secure a pay-out of legitimate funds, even though they started the policy with dirty money.
- / **Policy sales.** For many insurance policies, there is now a thriving – and perfectly legitimate – secondary market where the cover can be sold. This enables money launderers to sell their policy for a lump sum that comes from legitimate sources.

- / **Policy loans.** Some insurers are prepared to make loans against the value of life insurance plans with significant value, with the plan treated as collateral during the lending process. This provides money launderers with an easy route to a cash lump sum from a legitimate source – and such loans require less due diligence than traditional lending products.
- / **Collateral.** Insurance plans can also be used as security for more traditional bank loans, another source of clean money. The policy, originally purchased with criminal proceeds, can then be surrendered to repay the advance.
- / **Top-up premiums.** One common tactic employed by money launderers is to set up an insurance policy with a very small initial premium that is unlikely to attract scrutiny, either from the insurer itself or regulators. With a legal policy established, criminals can then make much larger payments through subsequent premiums in order to launder their cash.

Importantly, many of these strategies may be employed through the use of insurance brokers, rather than in direct dealings with the ultimate insurer. Both insurance companies and intermediaries must be on the alert – and have AML processes and practices that mitigate the risks posed by these opportunities for criminals.

The regulatory environment



The Financial Action Task Force (FATF) is increasingly worried about the insurance sector's exposure to money laundering. The intergovernmental agency set out its risk-based approach to insurance as long ago as 2018.

The principle of this approach is that money laundering risk assessments should reflect the nature, size and complexity of the business: from a simple assessment for less complex insurers and intermediaries to more complex work for larger groups.

In other words, financial regulation and compliance work should be proportionate, in the FATF's view. But the agency's guidance also stresses the importance of senior management taking responsibility for AML policies and processes. And it points to the broader related risks that the sector faces, including the

possibility that money withdrawn from insurance policies could be used to fund terrorism.

The FATF does not set regulatory standards of its own. Rather, its role is to support and inform member states as they implement regulatory regimes, ensuring common standards in international markets. However, while this supports collaboration between different countries and – to some extent, at least – informs a similar regulatory approach, insurers and intermediaries will need a clear understanding of the specific rules that apply in every jurisdiction in which they operate.

/ AML regulation for insurance in the UK

In the UK, insurers may be lulled into a false sense of security by the fact that in most cases, the insurance sector is not subject to the Money Laundering Regulations regime. However, the industry still has very significant responsibilities under the Proceeds of Crime Act to report suspicious activities – which requires insurers to spot them in the first place - and there are penalties for both companies and individuals who do not meet these requirements. Indeed, insurers and intermediaries lacking systems

and controls that will prevent financial crime will be at risk of committing money-laundering offences. Since 2009, the UK's Financial Conduct Authority has taken [enforcement action](#) against four insurance intermediaries for failure to adequately manage corruption risk. The industry therefore cannot afford to ignore AML.

The regulatory environment



/ AML regulation for insurance in the European Union

The European Union's 6th Anti Money Laundering Directive (6AMLD) came into effect across the bloc on 6 December 2020, with parties given until June 2021 to comply with the legislation. The 6AMLD explicitly sets out who is covered by the regulation and, unlike in the UK, insurance companies and insurance intermediaries, are expressly included.

The 6AMLD introduced significant changes to the EU's previous AML regime, setting out 22 new offences that would be treated as money laundering and extending the reach of legislation. It also included provisions for stronger penalties for individuals and corporate entities found guilty of money laundering offences.

/ AML regulation for insurance elsewhere

Most other major jurisdictions have similar regulation in place. In the US, for example, the Bank Secrecy Act sets out a range of in-scope products where there are strict transaction monitoring requirements. For insurers, these include most permanent life insurance policies, annuity contracts and any insurance product that has a cash value or investment features.

The Bank Secrecy Act also requires insurers

to submit suspicious activity reports to the Financial Crimes Enforcement Network in cases where specific red flags are apparent.

In the Asia Pacific region, meanwhile, regulators take a similar view. The Monetary Authority of Singapore is just one regulator in the region to set out specific regulations for AML compliance for the insurance sector.

/ Complying with sanctions

Insurance companies are required to comply with financial sanctions 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.

Insurers will need to have robust sanctions screening policies and practices in place as part of their AML work, in order to identify customers – either new or existing – that are subject to these measures. Where customers are identified, insurers may need to take a series of steps, including blocking transactions and freezing assets, as well as notifying the authorities.

How to comply with AML and KYC regulation



With so many moving parts – and such wide-ranging risk – compliance for the insurance sector requires significant engagement and commitment. It is a battle that will need to be waged on several fronts simultaneously.

/ KYC and CDD checks

Strong know-your-customer (KYC) and customer due diligence (CDD) practices will provide insurers and intermediaries with an important first line of defence against money laundering.

Insurers will need to look at how they are verifying individuals' identities – as well as how they are recording this work.

This will need to include both basic checks – authenticating key personal data and documentation – and screens for individuals where there may be a duty to do more; in particular, politically exposed persons (PEPs) are individuals in positions of influence who may pose a higher risk for bribery and corruption. These PEPs will require enhanced due diligence procedures.

/ Transaction monitoring and reporting

In addition, insurers that do not have robust transaction monitoring processes in place cannot be sure their products and services are not being used for criminal purposes. Given the volume of work that this will entail for most insurers, it is important to have systems that are capable of identifying red flag transactions and sounding an alert.

Where a transaction does raise concerns, insurers may be required to file a suspicious activity report (SAR) or a suspicious transaction report (STR) to the relevant regulatory authority.

It is difficult to compile an exhaustive list of the type of activity that might give rise to such a report. But examples of red flags could include clients seeking to pay for policies with cash, seeking to pay via third parties, paying for cover and then seeking a refund for no obvious reason, or making claims very soon after a policy has been purchased.

Insurers may also receive requests to substitute beneficiaries during the life of a contract or be asked to send funds to third parties following termination, despite there being no apparent link between the nominated recipient and the original policyholder.

How to comply with AML and KYC regulation



/ Sanctions checks

Insurers and insurance intermediaries will also need to have a sanctions compliance policy in place. This should be risk-based – that is, focused on sanctions lists on the basis of the risks represented by their customers and the jurisdictions in which they operate – but the policy will also need to be fluid. Their own exposures may change over time and, more broadly, the sanctions environment may evolve very quickly, as the Russia-Ukraine situation has illustrated. Where insurers' AML practices do flag up

a customer potentially subject to sanctions, there must be a clear process in place for confirming the customer's identity and their inclusion on the sanctions list. Insurers should also have back-up processes in place that mitigate against mistakes made by employees, or deliberate attempts to evade their screening processes.

/ The role of technology

Manual approaches to AML and KYC compliance are increasingly impractical. The workload is simply too large, exposing insurers and intermediaries 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 and KYC processes provides insurers with 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 insurers 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. The ability to provide this narrative will become increasingly important as regulators scrutinise the insurance sector's exposure to money laundering issues ever-more closely.

Streamline Compliance, Elevate Customer Experience

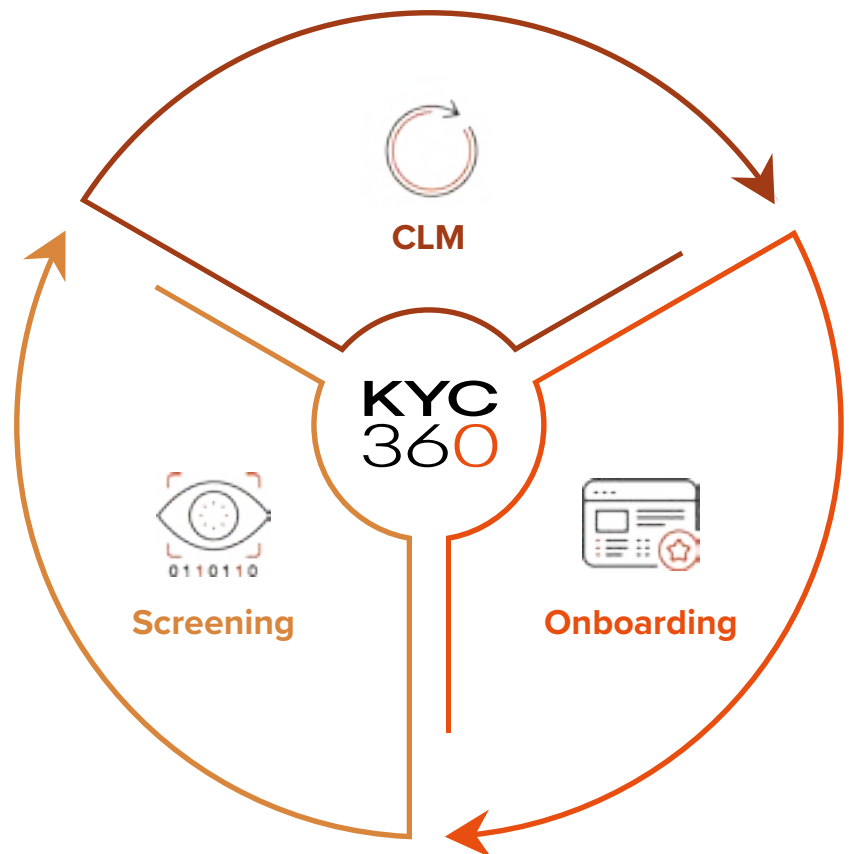
The KYC360 platform is an end-to-end solution offering slicker business processes with a streamlined, automated approach to Know Your Customer (KYC) compliance. This enables our customers to outperform commercially through operational efficiency gains whilst delivering improved customer experience and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



Contact

[/ sales@kyc360.com](mailto:sales@kyc360.com)

[/ www.kyc360.com](http://www.kyc360.com)

