Mastering AML compliance in 2026.

Practical AML advice and best practices for conveyancers

OneSearch.

Overview

This guide provides a practical overview of the AML risks conveyancers face today and the steps firms can take to stay compliant in an increasingly demanding regulatory environment.

In this guide, we cover:

- The key AML and KYC obligations conveyancers must meet in 2026
- What's changed in the AML landscape, including increased regulatory scrutiny and evolving risk expectations
- Common areas where firms fall short, based on recent SRA supervisory findings
- Practical steps to strengthen firm wide and client level risk assessments
- The role of technology in improving consistency, auditability, and compliance
- Safe Harbour explained: what it is, when it applies, and how it fits alongside AML requirements

Foreword

Anti-Money Laundering (AML) is more important now than ever.

It’s not just a matter of ticking boxes or avoiding fines from the regulator - it’s about protecting our infrastructure, communities, and, most importantly, the vulnerable who are most impacted by serious crimes like human trafficking, county lines drug dealing, and money muling. These crimes are not victimless. As professionals in the legal sector, you have a duty to ensure you are not helping criminals’ benefit from these crimes by allowing them to launder their dirty money through the services you provide.

With the UK’s latest National Risk Assessment on money laundering and terrorist financing published in July 2025 [1], it’s vital to stay ahead of the ever-evolving risks. Criminals are constantly finding new ways to exploit weaknesses, by staying ahead of these trends and by utilising technology, you protect not only the legal profession, but you will also help safeguard those who need it most. **Together, we can all make a real difference.**

Kayleigh Smale

Kayleigh Smale | Director, Smale Compliance

1 www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2025

Conveyancers in the UK are at the forefront of a rapidly rising wave of money laundering by domestic and international criminals seeking to ‘clean’ illicit money acquired through drugs, people trafficking, fraud, and other serious crimes.

The use of criminal proceeds to buy property and the widespread theft of client money are now placing conveyancing firms and their clients at enormous risk. Conveyancing anti-money laundering (AML) checks remain the primary defence against money laundering in the UK’s property sector.

The SRA has made no bones about its intentions to clamp down further on money laundering prevention in 2026 and beyond. In recent years we have seen record fines issued by the SRA for non-compliance with AML requirements [2] and the first-ever conviction of a Solicitor for alerting someone that they are under investigation (referred to as ‘tipping off’). [3]

2 www.sra.org.uk/consumers/solicitor-check/recent-decisions
3 www.lawgazette.co.uk/news/revealed-fines-mount-up-as-sra-cracks-down-on-aml-breaches/5118978.article

Despite the fact that conveyancers know that non-compliance AML requirements can lead to substantial fines of up to £25,000, being struck off, or even prosecution, many firms are still yet to put the necessary measures in place.

With the SRA's latest report showing a significant increase in supervisory activity, it's clear that expectations continue to rise. Over the most recent reporting period, the SRA carried out 935 proactive AML engagements, reviewing 833 firms across the legal sector. Around one third of those firms were found to be non-compliant, with more than half assessed as only partially compliant. These issues most commonly stemmed from gaps in firm-wide and client risk assessments, weaknesses in AML controls, insufficient training, and limited internal monitoring.

Thankfully, with a determined focus on AML best practices, a robust fit-for purpose AML system, education, and effective internal oversight, full and consistent compliance with the SRA's AML obligations can be achieved. This is why we created this guide to explain everything that you need to know to achieve long-term AML compliance within your conveyancing practice.

Alongside increased enforcement by existing supervisors, the wider AML regulatory landscape is also evolving. The UK government has confirmed plans to reform the supervision of anti money laundering and counter terrorist financing across professional services, with the Financial Conduct Authority (FCA) expected to take on a more central supervisory role in the future. While day to day AML supervision for legal services remains unchanged for now, the direction of travel is clear: firms will be expected to demonstrate stronger, more consistent, and more evidence led AML controls.

Understanding your KYC / AML obligations

Key AML obligations for conveyancers include:

- **A firm wide AML risk assessment**
  Firms must maintain a written firm wide risk assessment under Regulation 18, identifying the money laundering and terrorist financing risks their practice is exposed to and how those risks are mitigated. This should be reviewed regularly and approved by senior management. (sra.org.uk)
- **A documented client and matter risk assessment**
  A written client and matter risk assessment must be completed for every instruction, in line with Regulations 28(12) and (13). This should reflect both the specific risks of the matter and the firm wide risk assessment. (sra.org.uk)
- **Client identification and verification**
  Firms must identify and verify the identity of all clients and, where applicable, ultimate beneficial owners before establishing a business relationship or carrying out a transaction.
- **Source of funds and source of wealth checks**
  Reasonable steps must be taken to understand where funds originate and whether they are consistent with the client's profile and the transaction.
- **Ongoing monitoring**
  AML is not a one off exercise. Firms must keep client information up to date and reassess risk where circumstances change.
- **Training, governance and reporting**
  Staff must receive regular AML training, and firms must appoint a Money Laundering Reporting Officer (MLRO) responsible for reporting suspicious activity to the National Crime Agency.

The problems vs the solutions

In their latest AML report, the SRA highlighted a number of persistent weaknesses across law firms that commonly lead to non compliance with AML and KYC requirements. The 2024–25 findings show that many firms continue to struggle with core obligations such as firm wide risk assessments, client, and matter risk assessments, and maintaining effective AML controls. In the following section, we outline the key issues the SRA identified and explain how they can be addressed in practical, manageable steps.

Risk assessments

Risk assessments are the foundation of effective AML compliance - yet they remain one of the most common areas of failure.

Problem	Solution
Client and matter risk assessments are not completed consistently or in full.	Use workflows that make risk assessments mandatory before a matter can progress, ensuring they are completed every time.
Risk assessments are treated as a tick box exercise, with little consideration of the actual risks involved.	Design risk assessments that require narrative input and justification, encouraging fee earners to actively assess risk rather than select default answers.
Firm wide AML risks are not reflected at client or matter level.	Regularly review risk assessment templates to ensure firm-wide risks are clearly embedded into client and matter-level assessments.
High risk matters proceed without senior oversight.	Apply risk-weighting so that higher-risk clients or matters automatically trigger escalation and senior approval.
Risk assessments are completed once and never revisited.	Build review points into your processes so risk assessments are updated when new information emerges or circumstances change.

Key takeaway: Risk assessments should inform decisions, not just document them.

Identity verification

Incomplete or inconsistent identity checks continue to expose firms to fraud and regulatory action.

Problem	Solution
Identification and verification documents are missing from client files.	Use systems with mandatory document capture and clear audit trails to ensure evidence is always retained.
Only one individual involved in a transaction is verified, with others overlooked.	Apply consistent identity checks to all relevant parties, including beneficial owners and individuals acting on behalf of others.
Due diligence is relaxed for long standing or familiar clients.	Standardise identity verification so checks are applied consistently, regardless of how well a client is known.
Enhanced due diligence is not applied when risk indicators are present.	Define clear triggers for enhanced due diligence and ensure they cannot be bypassed without appropriate authorisation.
Identity checks rely solely on manual review of documents.	Combine document verification with biometric and fraud detection measures to reduce the risk of impersonation or document manipulation.

Key takeaway: Knowing your client is not the same as verifying their identity.

Other AML risks

Even where initial checks are completed, ongoing AML obligations are often overlooked.

Problem	Solution
Source of funds information is incomplete, unclear, or poorly evidenced.	Require clear documentation that explains where funds originate and whether they align with the client's profile and transaction.
Bank statements or financial documents are accepted without scrutiny.	Apply checks that help identify inconsistencies, alterations, or high risk transaction patterns.
Ongoing monitoring is not carried out once a matter is underway.	Implement regular monitoring of client and transaction information to identify changes in risk.
Sanctions and PEP checks are carried out once and not refreshed.	Re screen clients periodically to ensure changes in status are identified promptly.
AML records are scattered or difficult to audit.	Maintain a clear, centralised audit trail showing decisions made, checks completed, and actions taken.

Key takeaway: AML compliance doesn't end once a client is onboarded - it requires continuous oversight.

Manual vs Digital AML checks

It is clear from the problem/solution section above many of the AML compliance risks identified by SRA can be resolved by digitising the money laundering check process. While manual checks may meet the requirements, there is always an ongoing risk that parts of the AML process will be missed or poorly completed. **Here is a comparison of the two approaches:**

Manual AML checks	Digital AML checks
Potential for AML checks to be missed or completed in the wrong order.	Digital AML workflow tools ensure that each step of the process is completed and in the correct order.
It may not be clear when additional checks are required based on risk, geography, and service type.	The workflow, questions answered, and information required dynamically based on risk, geography, and service type.
Requires manual oversight by a human.	Digital AML checks ensure that the quality of information meets the required standard and that risks are automatically detected.
Lack of audit trail.	Digital conveyancing AML systems keep a record of every change, ensuring transparency for auditing purposes.
No automated checks for compliance.	Digital information can be automatically checked for compliance with AML requirements, both for new and existing clients. This includes sanction, fraud, and PEP checks. Digital workflow systems can also alert senior team members of newly identified risks, allowing them to resolve the matter quickly.

What is the Safe Harbour Standard?

'Safe Harbour.' We hear this term thrown around in conveyancing teams a lot, but what does it really mean? And is it something you have to do?

Over the years, property fraud has become quite the headache for conveyancers. Fraudsters have been selling properties they don't own, running off with the cash, and leaving buyers high and dry. The Solicitors Regulation Authority even flagged vendor fraud as an emerging risk in its latest AML Sectoral Risk Assessment.

Naturally, after case law like Dreamvar, lawyers are pretty nervous about getting it wrong. It's the case that changed the liabilities and responsibilities of lawyers and conveyancers when dealing with residential property transactions.

For those who aren't familiar with the specifics of the case of Dreamvar, here's what happened...

A fraudster managed to sell a London property worth around £1 million by impersonating the real seller. After the sale, the fraudster (and the money) disappeared into thin air. Fortunately, the Land Registry caught the fraud when the transfer documents came through, so the title never changed hands.

But poor Dreamvar was left with no property and no cash, so they took legal action against their solicitors, alleging negligence and breach of trust. They also sued the fraudster's solicitor for failing to spot the fraud. Initially, only Dreamvar's solicitor was found liable, which seemed harsh to many, as the fraudster's solicitor hadn't done enough to verify their client's identity under Money Laundering Regulations (MLR).

Guest author:

Kayleigh Smale

Director, Smale Compliance

The case eventually made its way to the Court of Appeal. There, the judge determined that the solicitors representing the fraudulent property seller should also shoulder some responsibility alongside those representing the deceived buyer for any incurred losses.

Following this, the Law Society updated its Conveyancing Protocol.[4] Now, if you're acting for the seller (especially if you're a Conveyancing Quality Scheme (CQS) firm), you need to:

- request details of the bank account for the sale proceeds and
- obtain evidence that the account belongs to the seller, showing that they have had and been using the account for at least 12 months and
- confirm proceeds will only go to that account

This is a great way to ensure the purchase funds are going to the correct person! But let's face it, fraudsters are still out there trying their luck. Take the case of a Vicar in 2021, who came home to find his house gutted and the locks changed. Someone had stolen his identity and sold his home – and this time, the Land Registry approved the title transfer. It took him two years of legal battles to get his house back!

Safe Harbour protects conveyancers who might unknowingly get caught up in a fraudulent transfer, as the Land Registry won't hold them liable. The aim is that, by applying the Safe Harbour standard properly, you'll spot a fraudulent seller right from the start.

So, what is the Safe Harbour Standard?

In March 2021 Land Registry issued 'Practice guide 81: encouraging the use of digital technology in identity verification'[5] which is also known as the 'Safe Harbour' Standard.

The Safe Harbour standard is based on the principles outlined in the Government's Good Practice Guide (GPG45).[6] It includes checking identities using biometrics and cryptography to ensure the person you're dealing with is who they claim to be.

4 www.lawsociety.org.uk/topics/property/conveyancing-protocol
5 www.gov.uk/government/publications/encouraging-the-use-of-digital-technology-in-identity-verification-pg81/practice-guide-81-encouraging-the-use-of-digital-technology-in-identity-verification
6 www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

The guidance sets out 4 requirements that must be met in order for the checks to meet the Safe Harbour Standard. 1-3 apply to all conveyancers, requirement 4 applies to conveyancers acting for the seller.

Requirement 1 – Obtain evidence

You need to make sure the person you are acting for is who they say they are.

The documents required to meet this requirement are:

- Biometric passports
- EU/EEA ID cards with biometrics
- UK biometric residence permits

Requirement 2 – Check the evidence

You can't just glance at the ID and hope for the best. You need an identity check provider to verify the document is legitimate and hasn't expired.

The identity check provider's system must read the chip within the evidence using NFC by providing any required cryptographic keys and then:

- check the digital signature is correct for the organisation that issued the evidence
- check the signing key belongs to the organisation and has not been revoked
- extract the biometric information needed for requirement 3

Requirement 3 – Match the evidence to the identity

You must check that the person who has provided the evidence matches the photo in the evidence. This is done using biometrics, where an identity check provider performs a 'liveness check' to compare the individual's biometrics with the info stored on the chip.

Requirement 4 – Obtain evidence to make sure the person who owns the property is the same person you are acting for (seller's solicitor only)

You need two pieces of evidence to show the person has a connection to the property. This could be anything from utility bills to a mortgage statement — just make sure it's not a screenshot.

Why use Safe Harbour?

Besides protecting you from claims in case a fraudster slips through, the Safe Harbour Standard encourages using technology as part of the process. Technology can help lower fraud risk and costs and make a more streamlined process for both conveyancers and their clients.

Some Safe Harbour myths...

Safe Harbour is compulsory for all property transactions

Not true! The Land Registry won't force you to use Safe Harbour. Firms can still rely on other methods to identify and verify clients, but Safe Harbour gives you that extra shield of protection if a fraudster manages to slip through the net.

Safe Harbour is the same as NFC

NFC checks are part of it, but there's more to the Safe Harbour Standard — like verifying the person's identity and connection to the property.

If we use the Safe Harbour Standard there are no risks of Money Laundering.

Sorry, but no. Safe Harbour and the MLR might overlap, but they're not the same. However, using Safe Harbour as part of your client ID checks is a great way to strengthen your compliance with the MLR.

One last thing to consider...

Safe Harbour and the MLR might overlap, but they're not the same. However, using Safe Harbour as part of your client ID checks is a great way to strengthen your compliance with the MLRs.

Your guide to AML language

Anyone who has worked in the area of KYC and AML will know that regulators and authorities often use acronyms and terms, the meaning of which are not always immediately obvious to the untrained eye. Understanding these terms is crucial for everyone working in the conveyancing sector.

Here are some common terms used in AML and their meanings:

Money laundering

Money laundering is the process of disguising the origins of illegally obtained money, typically by means of transfers involving foreign banks or legitimate businesses.

Know Your Customer (KYC)

Know Your Customer (KYC) is a standard set of processes and procedures used by financial institutions to verify the identity of their customers, with the aim of preventing fraud, identity theft, and money laundering.

Customer Due Diligence (CDD)

Customer due diligence (CDD) involves checking the identity of clients client with a view to making sure they are who they say they are.

Ultimate Beneficial Owner (UBO)

A UBO is a person or persons who ultimately owns or controls a legal entity and stands to benefit from its activities. Identifying beneficial owners is crucial to understanding the real individuals behind conveyancing transactions.

Suspicious Activity Report (SAR)

A SAR is a report filed by persons in the regulated sector when they know, suspect or have reasonable grounds for knowing or suspecting that a person is engaged in, or attempting, money laundering or terrorist financing.

Transaction monitoring

Transaction monitoring involves reviewing and analysing transactions in real time to identify any unusual or suspicious patterns that may suggest money laundering.

Risk-based approach

A risk-based approach is a proactive strategy used by regulated businesses whereby resources are allocated based on the level of risk associated with a particular customer or transaction. Higher-risk customers receive more scrutiny and monitoring.

Politically Exposed Person (PEP)

An individual entrusted with prominent public functions in the UK or abroad. PEPs, along with their close family members and known associates, require enhanced due diligence (EDD). Under updated FCA guidance, domestic PEPs are generally considered lower risk, and some roles, such as non executive civil service board members, no longer fall within the PEP definition.

Source of funds

The source of funds refers to the ultimate origin of the money used in a particular conveyancing transaction. Verifying the legitimate source of funds is a key element of AML procedures.

Safe Harbour

In 2021, HM Land Registry presented new guidance for a higher standard of identity verification. This encouraged the use of both biometric and cryptographic technology checks, which would offer a greater level of fraud prevention.

If solicitors and conveyancers chose to adhere to these new guidelines, HMLR will consider them to have 'taken reasonable steps' to verify customer identities, and they would have reached Safe Harbour. This means that HMLR would not seek recourse against the conveyancer should the identity of their client confirmed later in the process to be inaccurate.

Passive liveness

Passive liveness refers to the method of identity verification that assesses the ‘liveness’ of a person without requiring active participation from the individual. Liveness detection is crucial in biometric systems to ensure that biometric data (such as fingerprints) is from a live person and not a static image or a recorded video.

Ongoing monitoring

Ongoing monitoring refers to the process of regularly reviewing and updating customer information, transactions, and business relationships to identify and assess any changes in risk factors. The goal is to ensure that a financial institution or business remains vigilant against potential money laundering activities.

Digital Verification Services (DVS) Trust Framework

The UK government has published the Digital Verification Services (DVS) Trust Framework, which sets out the rules and requirements organisations must meet to provide secure and trustworthy digital identity and attribute verification services. Formerly known as the Digital Identity and Attributes Trust Framework, it became a statutory framework in December 2025 under the Data (Use and Access) Act 2025.

Introducing **OneSearch AML**

OneSearch AML is a cutting-edge, online, digital, automated AML and KYC platform widely used across the conveyancing sector in the UK. It has been designed from the ground up to overcome all of the risks and challenges identified by the SRA's recent report and outlined above.

With OneSearch AML, you can relax in the knowledge that your conveyancing firm is compliant with its AML and KYC obligations at all times.

OneSearch AML:

- Automatically verifies the identity and addresses of your clients using a simple automated workflow through a mobile app or online portal.
- Combines ID verification and real-time facial recognition technology to spot masks, impersonations, or fakes with easy-to-use anti-spoofing liveness tests.
- Uses biometric scanning, NFC technology, secure encryption, and cloud-based storage to ensure that ID checks are safe, accurate, and effortless.
- Works for both commercial and residential conveyancing.
- Integrates seamlessly into your existing conveyancing system. This removes the need for a completely new system and simply enhances what you already use.

- Carries out a range of checks seamlessly and automatically, ensuring that you know everything you need to know about your clients, including:
  - UK National Identity Register checks
  - UK Deceased Persons Database checks
  - UK NCOA (Alert Flag) Database checks
  - International Sanctions (Enhanced) checks
  - International PEP (Enhanced) Database checks, and
  - International Passport Machine Readable Zone (MRZ) and UK Driving Licence Algorithm checks.
- Provides ongoing monitoring of AML and KYC data, ensuring that any changes, developments, or updates to customer profiles are carried out automatically over a 12-month period.

Safe, accurate, and effortless conveyancing ID verification with **OneSearch AML**.

To learn more about OneSearch AML,
visit: **info.onesearch.direct/onesearch-aml**

Alternatively, speak to one of our Service Introduction Team on 01782 433 270 or email **intro@onesearchdirect.co.uk**

With thanks to Kayleigh Smale for their contributions to this guide. To discover how Smale Compliance can assist your firm, please visit www.smalecompliance.com

This guide was first published in March 2025 and has been updated to reflect the latest developments for 2026.

OneSearch.