



HM Revenue
& Customs

Framed

'Framed', our film on GOV.UK, shows how an art business can find itself involved in money laundering, if it doesn't take proper measures to protect itself.

Money laundering means passing illegally obtained money through legitimate businesses or financial systems, to make it appear lawful. Money laundering has a huge impact on local communities, as that money originally comes from other forms of crime, such as drug sales, human trafficking, and modern-day slavery.

Suspicious Activity Reports help the National Crime Agency, and other law enforcement agencies, to find and dismantle criminal networks that try to launder the proceeds of their crime through businesses like yours.

Customer Due Diligence is one of the best ways you can spot suspicious activity. It involves checking who the customer is, considering what they're doing with the transaction, and how they're doing it. The aim isn't to stop customers from being able to buy art; it's to prevent criminal finance, for example from laundering drug money, being used to buy art that the criminals can then sell on or enjoy.

Under the Money Laundering Regulations, art businesses have to train their staff about what to do when they spot something suspicious. This training guide, alongside the film on GOV.UK will help you to do that.

If you're a sole trader

Watch the film and think about the questions below. Then check the potential answers to see if you've missed anything.

Not all the questions will be relevant to you, if you don't employ anyone, but you should come back to them if you change your business model.

If you're an employer

We recommend you use this material to run a training session. We expect it will take around 2 hours, although this will vary based on the size of your teams, and how much time you allow for discussion.

Watch the film as a group or have everyone watch the film before the session. Then put the questions to the group to prompt discussion. You can split your staff into smaller discussion groups if you like.

Discussing your answers at the end of each question can be a good way to share understanding. The potential answers are just some of the things that your teams might say, and you can use them to prompt further discussions.

The discussion questions are split into groups by subject, so you can focus your session on the areas you think are most relevant to your staff. This will also make it easy for you to break up the learning into more than one session, if you need to.

After the session

There's information after each question that may help you with future training and updating your compliance work.

Contact HMRC

You can contact HMRC if your business is covered by the Money Laundering Regulations and you have any questions about money laundering, this training material or you want to make a money laundering disclosure.

Details on how to contact HMRC can be found by going to GOV.UK and searching for 'money laundering enquiries'.

Glossary of Key Terms and Abbreviations

Abbreviation	Term	Description
AML	Anti-Money Laundering	Anti-Money Laundering means the laws, regulations, and procedures that prevent criminals from disguising illegal funds as legitimate income.
AMP	Art Market Participant	<p>An Art Market Participant is a business or individual who either:</p> <ul style="list-style-type: none">• trades or acts as an intermediary in the sale or purchase of works of art valued at €10,000 or more• stores these works in a Freeport <p>By law, Art Market Participants must register with HM Revenue and Customs.</p>
CDD	Customer Due Diligence	The process of verifying a customer's identity and assessing the risk they pose. Businesses must carry out Customer Due Diligence to comply with AML regulations and prevent financial crime.
EDD	Enhanced Due Diligence	The process of conducting deeper scrutiny and ongoing monitoring of high-risk customers to better understand their activities, verify the legitimacy of their funds, and mitigate potential money laundering or terrorist financing risks.
DAML	Defence Against Money Laundering SAR	A request made to the UK's NCA within a SAR when a person suspects that property involved in a transaction is criminal and seeks consent to proceed in order to avoid committing a money laundering offence under POCA.
MLR 2017	The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017	Refers to The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, which set out the UK's anti-money laundering framework.

Abbreviation	Term	Description
NCA	National Crime Agency	A UK law enforcement agency responsible for tackling serious and organised crime, including economic crime.
PCPs	Policies, Controls and Procedures	Internal measures implemented by organisations to mitigate financial crime, money laundering and terrorist financing risks and ensure regulatory compliance.
POCA	Proceeds of Crime Act 2002	Refers to Proceeds of Crime Act 2002, legislation that provides the legal framework for recovering criminal assets and addressing money laundering offences.
RA	Risk Assessment	A systematic process for identifying and evaluating risks associated with financial crime, used to inform mitigation strategies.
SAR	Suspicious Activity Report	A report submitted to the authorities (the NCA) when suspicious financial activity is detected, as required under POCA.
TACT	Terrorism Act 2000	Refers to Terrorism Act 2000, UK legislation that addresses terrorism-related offences, including the financing of terrorism.

The Art Market

Discussion questions:

- What makes the art market so appealing to money launderers?

Answers might include:

- Access to a significant share of the high-value global art market, making it a prime target for illicit financial activity.
- Transactions can offer anonymity – buyers and sellers may use intermediaries or shell companies to hide their identities.
- Art valuations are highly subjective and can be manipulated to suit a particular narrative or financial goal.
- Artworks are portable and can be stored discreetly, making them ideal for hiding or transferring wealth.

Risk Assessments, and Policies, Controls and Procedures

Discussion questions:

- How would you describe Rory's overall approach to complying with The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017)?
- Why didn't Rory carry out much CDD?
- What further checks could Rory have done on Rae?
- What checks did Rory get wrong?
- Could a better risk assessment have helped?
- Does everyone know what your risk assessment says?

Answers might include:

- Rory appeared to take a surface-level approach to compliance with MLR 2017.
- He completed CDD checks on the art-dealer Rae and verified her identity as per MLR 2017. But he trusted her too much as he'd known her for many years and didn't do further checks.
- Rory should have checked if Rae was registered with HMRC as an AMP. He could have gone further and checked if there were any sanctions about her on GOV.UK.
- Rory didn't ask what Rae had been doing in the last few years, what art she'd been involved with buying and selling, or who she'd worked with. He could have searched the internet to verify what she said.
- Rory only had a quick look at the provenance documents and didn't check if the artwork was listed as stolen. He should have made proper checks in line with the POCA regulations. He trusted what Rae said she'd done, rather than checking himself. This put the business at risk of exploitation.
- A better risk assessment might have directed Rory to the risks more clearly, and then he'd have thought more about how to mitigate them.

Detail

If Rory had taken his responsibility under MLR 2017 more seriously:

- the risk assessment would have included more checks on the artwork
- he would have completed more detailed CDD
- he would have seen the risks of this transaction earlier
- he could have made a DAML and protected himself, his business, and his customers from criminal activity.

Businesses must maintain PCPs and Risk Assessments under regulations 18 and 19 of MLR 2017.

Regulation 18 – Risk Assessment

You must:

- identify and assess the risks of money laundering and terrorist financing to which your business is subject
- consider the customer, geographic, product, transaction, and delivery channel risk factors
- keep an up-to-date written record of all steps taken
- give this Risk Assessment to your supervisory authority when asked.

Regulation 19 – Policies, Controls and Procedures

You must establish, maintain, and regularly review AML PCPs to effectively mitigate and manage the risks identified in your Regulation 18 RA. These must include:

- risk management practices
- internal controls
- customer due diligence
- record keeping
- monitoring and compliance
- staff training

Keep written records of these policies and any updates and communicate them internally.

The HMRC Economic Crime Supervision Handbook confirms:

“A requirement for businesses to maintain written risk assessments and policies, controls and procedures” is a core obligation under MLR 2017.

To read the handbook, go to GOV.UK and search ‘Economic Crime Supervision Handbook’.

Customer Due Diligence

Discussion questions:

- Why is it important to carry out appropriate CDD?
- What does our CDD process look like?
- Was Rory’s CDD process effective?
- Do we take CDD seriously?
- What background crimes might be funding an illicit transaction?
- What could Rory have asked to see?

Answers might include:

- To understand who your customer is and assess the nature and purpose of their transactions.
- It plays a key role in detecting and preventing financial crime within your business.
- It safeguards your business's reputation and builds trust with customers and stakeholders.
- To comply with your legal and regulatory obligations.
- A well-documented customer profile makes it easier to spot unusual or suspicious behaviour.
- Rory's business completed basic CDD on its customer, Rae, confirming and checking Rae's identity. But Rory trusted Rae as he had known her for years and did no further checks.
- Rory should have done more here to make sure things had not changed with Rae. For example, a simple internet search could have shown if Rae had a recent criminal conviction, was sanctioned, or was linked to suspicious activity. He should have checked GOV.UK to make sure Rae was registered as an AMP, and that HMRC hadn't placed sanctions on her business.
- As Rory had not had an established business relationship with Rae, he could have decided to carry out his own checks on the seller.
- The CDD on the buyer was effective. The change of address and name match on sanctions were red flags, prompting further checks to see if these issues should stop the sale going through.
- Money laundering is not a victimless crime. The funds that are used in those illicit transactions come from crime, which includes:
 - Selling drugs
 - Human trafficking
 - Modern-day slavery
- Rory could have asked for some of the following:
 - Proof of ID
 - Proof of address
 - Proof of ownership
 - Commercial rationale

Detail

MLR 2017 explicitly requires AMPs to have effective controls in place to manage money laundering and terrorist financing risks.

HMRC's Economic Crime Supervision Handbook reinforces that AMPs must:

- properly risk assess each area of their business activity
- implement tailored PCPs – not generic templates
- show how these PCPs are used to manage and mitigate risks
- maintain records that show ongoing monitoring and compliance with their own PCPs.

AMPs in the UK must follow specific CDD requirements under MLR 2017. You can find guidance on GOV.UK with examples of the key checks an AMP should carry out. Go to GOV.UK and search for the following terms:

- Art Market Participants Guidance for Money Laundering Supervision
- Your Responsibilities Under Money Laundering Supervision

Enhanced Due Diligence

Discussion questions:

- What is the difference between CDD and EDD?
- When is EDD appropriate?
- Do we have any customers that we should carry out EDD on? How do we identify them?
- What does our EDD process look like?

Answers might include:

- CDD is the standard process for identifying customers, and understanding the business relationship or transaction.
- EDD is where there's a higher risk of money laundering. It includes all the same things as CDD, plus extra checks tailored to the increased risks. It might include deeper verification of ID, the source of funds, or purpose of the transaction.
- Our risk assessment tells us how to identify a higher risk of money laundering, and our policies, controls and procedures tell us how to manage it.

Detail

There's more guidance on CDD in **MLR 2017 Regulation 27, Regulation 28 and BAMF guidance** which has been authorised by HMRC. Further guidance on EDD is at **Regulation 33** and in the authorised BAMF guidance.

To view the authorised BAMF guidance, enter the search term 'BAMF AML guidelines' into your search engine.

Regulation 33(5) MLR 2017 sets out EDD measures where there's a high risk of money laundering or terrorist financing. These include:

- seeking additional independent, reliable sources to verify information provided or made available to you
- taking extra measures to better understand the background, ownership and financial situation of the customer, and other parties to the transaction
- taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship
- increasing the monitoring of the business relationship, including greater scrutiny of transactions.

Red Flags and Suspicion

Discussion questions:

- What was the first 'red flag' Rory should have seen that suggested the transaction might be higher risk?
- Have you seen anything suspicious about a customer or transaction, and what did you do about it?
- If Rory felt suspicious, what might he have done?
- Could Rory have recognised the risk earlier?
- How many red flags can you spot?
- What red flags do you see in your own business?
- How can we prioritise recognising red flags while still providing high-quality customer service?
- Why is it important to recognise these risks?

Answers might include:

- Rae unexpectedly calls Rory after years of no contact, proposing a high-value sale.
- Rory acknowledges the long gap in contact – this alone should have raised concerns.
- Rory should have looked into the transaction in more detail.
- Rory could have submitted a Suspicious Activity Report.
- We can see all the following red flags:
 - unexpected contact from an old acquaintance
 - an offer that seems too good to be true – a business in financial difficulty is promised a 30% commission on a high-value art sale
 - an unclear reason for the sale – does Rae's explanation make commercial sense? Has Rory been given enough detail to assess this?
 - Rae's dismissive response to requests for CDD documents – she says "Leave that for now" and tries to change the subject
 - over-reliance on Rae to complete CDD without challenge – she only provides copies of documents, not originals
 - Rae implying that more business will follow if the sale goes through
 - Rae's overly enthusiastic reaction when the sale is completed
 - Rae's phonenumber being disconnected
- We might see:
 - the buyer flagged on a sanctions list
 - the buyer changing the delivery address unexpectedly
 - pressure to complete the sale quickly
 - discrepancies in provenance documents
 - other risks listed on our risk assessment
- It's important to recognise red flags because it can stop us getting fined or prosecuted.
- Recognising the risks means we can prevent criminals from laundering their money, which is from illicit activity, including people trafficking, drug sales, and other organised crime.

Detail

Remember, a red flag doesn't have to be a firm or well-defined suspicion. It can just be a sign or a sense that something may be unusual or present a risk.

You should think about whether you or your staff have been trained to recognise red flags.

Your policies, controls and procedures should clearly outline the steps staff should take if something raises their suspicion.

Spotting high-risk indicators in an art transaction is crucial for AML. It allows:

- 1. Prevention of Criminal Activity:** Criminals may use art to disguise the origins of illicit funds. Identifying red flags helps prevent money laundering and financing terrorism.
- 2. Regulatory Compliance:** Art market participants are subject to AML regulations. Failing to identify and act on risks can lead to legal penalties and reputational damage.
- 3. Due Diligence:** Early detection of suspicious activity allows for proper due diligence, reporting, and, if necessary, halting the transaction before it's too late.
- 4. Market Integrity:** Recognising and addressing risks helps maintain trust and transparency in the art market.

You can find more guidance on suspicion here:

- HMRC's Economic Crime Supervision Handbook. Go to GOV.UK and search 'Economic Crime Supervision Handbook'.
- BAMF guidance which has been authorised by HMRC. To view the authorised BAMF guidance, enter the search term 'BAMF AML guidelines' into your search engine.

Suspicious Activity Reports

Discussion questions:

- What is a Suspicious Activity Report?
- When should Rory have submitted a Suspicious Activity Report?
- What would you have done in that situation?
- How might you have monitored the transaction?
- Who would you speak to about your concerns?
- When should Rory have become genuinely suspicious?
- What might Rory have asked to try and work out what was going on?
- What is the process for submitting a SAR in your business?
- When might you have submitted a SAR?
- What can happen if you don't submit a SAR?
- What is a Defence Against Money Laundering SAR?

Answers might include:

- A SAR is a formal report to the NCA about your suspicions relating to a customer or transaction.
- A SAR is a legal requirement under the POCA.
- Rory should have submitted a SAR when he became suspicious. That should have been when Rae was evasive and wouldn't provide the information he needed.

- If Rory had a vague gut feeling, he should have continued to monitor the transaction. More time or information might have led to a firmer suspicion.
- In our business, we speak to the Nominated Officer, we contact them by...
- If concerned, we would speak to the Nominated Officer, a manager, or a colleague.
- Rory could have asked to see the provenance documents earlier.
- Rory could have asked for more details about why the transaction needed to be so quick.
- Not submitting a SAR could be a criminal offence.
- A DAML is a request to the NCA to carry out a transaction, where you are suspicious.

Detail

Your processes should allow the Nominated Officer or the staff member to ask for more information.

You should make sure staff know how they can address feelings of unease with a transaction.

Feeling uneasy is not normally enough to justify making a SAR under **Proceeds of Crime Act 2002 (POCA)**. That feeling needs a knowledge or suspicion or reasonable grounds to suspect the person is involved in money laundering or that the property is criminal property.

There is a low threshold for suspicion in UK law. You don't need proof, but you do need more than just a gut feeling. You need some evidence or factual basis for your suspicion.

When you are considering making a SAR, you shouldn't ignore a gut feeling or feeling of unease, you should explore them to resolve the feeling or establish suspicion.

You can find more guidance about suspicion in HMRC's Economic Crime Supervision Handbook (go to GOV.UK and search 'Economic Crime Supervision Handbook').

Failing to make a SAR can be a criminal offence, depending on your role and what you knew or suspected. If you work in the regulated sector, under **POCA Sections 330, 331 and 332** it is an offence:

- if you know, suspect, or have reasonable grounds to suspect that someone is engaged in money laundering, and you fail to make an internal report to the nominated officer
- or as nominated officer fail to submit a SAR as soon as practically possible.

This could result in 5 years in prison, a fine, or both.

A Defence Against Money Laundering SAR (DAML) is a SAR made to the National Crime Agency (NCA) where a business suspects that property (including money and all forms of real or personal property, see **POCA Section 84**), they intend to deal with may be criminal property, and by dealing with it they risk committing a money laundering offence.

A person does not commit an offence if they have received 'appropriate consent' (via a DAML) from the NCA.

Failure to report a suspicious transaction before proceeding with that transaction (and receiving a DAML) can result in criminal liability if the transaction is proven to involve criminal property.

A criminal offence would be committed if the business had reasonable grounds to suspect money laundering earlier in the transaction and failed to submit a DAML.

As the business has completed the transaction without Rory identifying suspicion and completing and obtaining a DAML he could find himself criminally liable.

Submitting a SAR

Discussion questions:

- What information do you need to include in a SAR?
- How can we get more information if we need it?
- What could Rory have submitted in his SAR?
- What happens if something changes?
- How does submitting a SAR change Rory's work? Can he continue with the sale?
- What is "tipping off"?
- What would you do if the NCA gave consent to a DAML? Would you continue with the transaction?
- If the NCA refused consent, how would we manage the customer without tipping them off?

Answers might include:

- You should provide as much relevant information as possible. If you don't know something, just state it's "unknown". This includes:
 - name of the reporter
 - the date of the report
 - details about the subject of your SAR
 - details of any associated subjects, and how they're associated to the main subject
 - details of the property, where it is and what it's worth
 - what you're planning to do
 - why you're suspicious
- the UKFIU (UK Financial Intelligence Unit) glossary code
- if you need DAML consent
- Rory should have included:
 - Rae's name, date of birth, contact details and anything else that could help identify her
 - The reasons for money laundering suspicion, including:
 - Rae contacting Rory for the first time in years
 - Rae's hesitation at providing CDD and procurement documents
 - discrepancies in the documents she provided
 - Rae's phone number being disconnected
 - timeline of events
- Buyers' details
- Seller's details (on whose behalf Rae is operating)
- A description of the suspicious activity, and why it's suspicious
- Reporting officer details
- What the suspected criminal property is, where it is, and its estimated value
- If something changes, just submit a new SAR, including the reference number of the previous one.
- If Rory submitted a DAML, then he shouldn't proceed until he receives consent from the NCA, or after 7 working days.
- "Tipping off" is an offence under the POCA. It's when you tell a customer that you've made a SAR.

Detail

You can find more details in the NCA guidance on SARs Reporting. Go to NationalCrimeAgency.gov.uk and search for 'SARs Reporter Booklet July 2025'.

You should submit as many details as possible about the subject, as this will help to identify them. Aim to be clear and concise, as the NCA receives a lot of SARs. To make it easy to read:

- structure your SAR logically, including all the relevant information
- briefly summarise your suspicion
- give a timeline of events
- keep it clear, concise and simple
- avoid acronyms and jargon
- explain any services or technical aspects of your work that you describe
- break up information into paragraphs.

You should make a second SAR when:

- new details emerge
- more events take place
- you need to correct or clarify the first SAR
- ongoing monitoring reveals more detail about suspected crime

If a staff member has made an internal SAR to the Nominated Officer and later becomes aware of new information, they should make a second internal SAR, linking to the first one.

The Nominated Officer should then decide whether to make a second SAR to the NCA; or, if they decided not to make a SAR to the NCA the first time, whether to make one now.

More guidance on making SARs is in the NCA guidance on SARs Reporting. Go to NationalCrimeAgency.gov.uk and search for 'SARs Reporter Booklet July 2025'.

You may need to report the matter using another route if there are other risks. For example, if someone threatens your staff, or a vulnerable person is at risk of immediate harm you may wish to inform police. If you do, include the Crime Reference Number when you submit your SAR.

You should make sure your Nominated Officer knows how to submit both a SAR and a DAML.

There's an example of an internal SAR in Appendix 1. This type of report provides the necessary information and rationale to support an external SAR to the NCA.

For DAML SARs, where consent is requested from the NCA to proceed with a transaction, no transaction should take place until consent is received.

The NCA will grant or refuse permission to undertake the transaction. The NCA has 7 working days to consider a DAML request. If you don't hear anything from the NCA after 7 working days have passed, you have 'deemed consent' to proceed. Please note, the day a DAML is received by the NCA is day 0.

If the DAML request is refused, the day of refusal marks the start of a 31-calendar day moratorium (suspension) period. During this moratorium period, law enforcement will work to take positive action against the criminal property. The moratorium period can be extended beyond the initial 31 days by the court.

You can't proceed with the transaction until the NCA gives consent.

You also need to guard against 'tipping off'. Tipping off is the disclosure to a customer that a SAR has been made, and the disclosure may prejudice any investigation. Tipping off is an offence under **POCA Section 333(A-E)**.

There's more information in BAMF guidance which has been authorised by HMRC. To view the authorised BAMF guidance, enter the search term 'BAMF AML guidelines' into your search engine.

What Can Happen?

Discussion questions:

- What happened to Rory's business?
- What happened to Rory?
- What happened to Rory's staff member?

Answers might include:

- Increased financial difficulty – the business has not only lost commission from this sale, but also incurred additional costs associated with the sale, having to refund payment and reimburse costs.
- Financial penalty – HMRC may issue a financial penalty for breaches of the MLR 2017.
- Increased regulatory scrutiny – HMRC may consider:
 - the PCPs of the business weak
 - that the business is now at higher risk of being exploited for money laundering
 - the business needs a higher level of supervision, if it's allowed to continue.
- Reputational damage – If HMRC took action against the business, it would publish the details on GOV.UK. Customers may take their business elsewhere.
- Potential removal of registration – HMRC might suspend or cancel the registration of the business, preventing them from trading as an art market participant.
- The person who should have reported it could be prosecuted and face an unlimited fine and up to 5 years in prison.

Detail

HMRC has powers under the MLR 2017 to sanction non-compliance. You can read about it in HMRC's ECS Handbook, by going to GOV.UK and searching for 'ECS handbook'. HMRC can:

- issue financial penalties, either to the business or to an individual who was 'knowingly concerned' - this means they knew and were actively involved in the breach
- Prohibit an individual from managing a supervised business, temporarily or permanently
- Temporarily suspend or permanently cancel the registration of a business, stopping it from trading
- publish a statement on GOV.UK to censure the business publicly
- issue an injunction, meaning the business or person has to do something or stop doing it
- prosecute, under POCA or MLR 2017

If HMRC issues a penalty, prohibits an individual from managing, suspends or cancels the registration, or publishes a statement, it must also publish the details of it on GOV.UK for five years. To see these details, go to GOV.UK and search 'Businesses not complying with money laundering regulations'.

Appendix 1 – Internal SAR (Template)

Part 1: Submitters details

Name	Rory Smith
Date and time of submission	31 July 2025, 2pm
Contact number	0115 111 1111
Contact email	RorySmith@art4sale.co.uk

Part 2: Details of the suspicious party

Name	Rae Clark
Address	1A, Any Street, London, SW1 7AW
Contact number	07111 111 111, RaeClark@Artdealer.co.uk
Additional details	Known to the owner of Art4Sale.

Part 3: Reason for suspicion

On 1 July 2025 at approximately 10:15 AM, I received a telephone contact from an old acquaintance, Rae Clark. Rae is an old friend from university, though we have no contact for approximately 6 years.

Rae is an art dealer. She advised she was acting as an intermediary for a client looking to sell a piece of art. She advised she was interested in selling this via my gallery (Art4Sale).

I met Rae at what she advised was her home (address above) on 3 July 2025. She discussed details of the sale and showed me a digital picture of the art. She offered the gallery 30% commission for completing the sale. She advised the seller was keen for a quick sale, due to bad investments and needing cash quickly. I advised her that we would be required to do customer due diligence checks. She queried this but was not ultimately put off when I advised this would need to be done.

As the transaction continued Rae provided the CDD and provenance documents regarding herself and her client on 8th July 2025. Art4Sale reviewed these and they seemed in order.

The transaction concluded without further incident on 30 July 2025. However following conclusion of the sale, I attempted to contact Rae Clark on 31 July 2025, only to find her phone number had been disconnected. This caused me concern.

Further inspection of the CDD and provenance documents at this point, raised further concern. We have identified a number of inconsistencies in the documents that we had not seen when CDD checks were undertaken.

Raes' behaviour, our inability to now contact her and discrepancies in CDD documents provided have raised our concern this may be a suspicious transaction.

Part 4: Supporting documents

Attachment 1: Copies of the transaction records