King & Spalding
Client Alert

Government Matters

27 AUGUST 2021

For more information, contact:

Robert Dedman
+44 20 7551 7552
rdedman@kslaw.com

Katherine Kirkpatrick
+1 312 764 6918
kkirkpatrick@kslaw.com

Lisa McKinnon-Lower
+44 20 7551 2190
lmckinnon-lower@kslaw.com

King & Spalding International LLP
125 Old Broad Street
London EC2N 1AR

Tel: +44 20 7551 7500

Anti-Money Laundering Implications for the Art Market in the UK

Introduction

The art market is characterised by high-value, portable items that can be bought and exchanged quickly and often confidentially. These features, which make the market inherently vulnerable to many types of crime, including money laundering, have led to increasing scrutiny by regulators and prosecutors.

Whilst the art market has always been subject to the general money laundering offences contained in Proceeds of Crime Act 2002 ("**POCA**"), amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the **"MLRs"**), which came into effect on 10 January 2020, impose additional obligations on Art Market Participants ("**AMPs**"), who now also fall within the scope of the regulations. HM Treasury has produced detailed guidance for AMPs in the wake of the amended MLRs, the most significant areas of that guidance and the legislation underpinning it, are summarised below.

Principal offences under POCA

Money laundering is the process by which criminal property is disguised or 'cleaned' so as to appear legitimate. To borrow an example from HM Treasury's Guidance, imagine an art collector (who has recently been convicted of insider dealing) asks his wife to buy a painting from an auction. Funds are wired to the auction house from an offshore entity owned solely by the art collector. The auction house accepts the funds, releases the painting to the collector's wife and pays the vendor. There is a risk that the auction house has just accepted criminally derived funds and facilitated money laundering.

In the UK there are three principal money laundering offences that apply universally:

a) Concealing, disguising, converting, transferring, or removing criminal property from the UK (section 327 POCA);

b) Entering into or becoming involved in an arrangement which facilitates the acquisition, retention, use, or control of criminal property by or on behalf of another person (section 328 POCA);

c) The acquisition, use, and/or possession of criminal property (section 329 POCA).

Criminal property is defined in section 340(3) POCA as property that constitutes or represents (wholly or in part) the benefit derived from criminal conduct. To commit any of the three principal money laundering offences, the alleged offender must know *or* suspect that the property in question is in fact criminal property. From a risk management perspective, it has always been best practice for anyone involved in a financial transaction to take steps to check and ensure that funds or property received, sent, or handled are not criminal property. Although there is no specific definition of what amounts to a suspicion, and the HM Treasury guidance is also silent on this point, some red flags include:

a) the customer does not have any obvious source of legitimate income comparable to the value of the intended purchase;

b) the funds for the artwork are coming from a third party, or multiple third parties, unconnected to the customer;

c) the funds are coming from a country which is a high risk jurisdiction for money laundering; or

d) the most obvious example, there are grounds for believing that the customer has been or is actually involved in criminal activity.

Secondary money laundering offences under POCA

Additional offences of failure to disclose and tipping off also apply to anyone within the regulated sector, which now includes AMPs. A person commits a failure to disclose offence where he/she knows or suspects that someone is involved in money laundering and fails to disclose that to the money laundering officer (a senior employee designated by the AMP) as practicable after that information comes to light. The money laundering officer then has an obligation to consider that information and ultimately has responsibility for deciding whether that should be disclosed externally to the National Crime Agency, making what is known as a suspicious activity report (**"SAR"**). By making a SAR, an AMP may also have a defence to a principal money laundering offence if the property received was in fact criminal property.

A person commits an offence of tipping off if he or she discloses the existence of an ongoing investigation where that disclosure is likely to prejudice an investigation. In line with s 333A, where an AMP has made a SAR, the AMP should avoid any communication that could prejudice the investigation. That is not to say that all contact must stop as this may well cause the customer to ask questions but an AMP should err on the side of caution when communicating because anything that puts the customer on notice of an investigation will constitute an offence. Delaying the customer or client is often the best option as this avoids inadvertent prejudicial communications and/or the AMP committing a principal offence.

Obligations under the MLRs

In addition to the requirements under POCA, AMPs are now also subject to a range of compliance requirements under the MLRs.

Under the MLRs, AMPs falling within the regulated sector are defined as firms or practitioners who either:

(i) trade or act as an intermediary in the sale or purchase of art, the value of which amounts to 10,000 euros or more; or

(ii) operate a freeport and stores art (the value of which amounts to 10,000 euros or more) in such freeports.

Pursuant to the MLRs, all AMPs must:

a) register with HM Revenue and Customs, the supervisory authority under the MLRs for AMPs. This should have been done by 10 June 2021. Any AMP that has not already done so should register with HMRC as soon as possible;

b) follow a risk based approach to prevent and detect money laundering by assessing the level of money laundering ("**ML**") and terrorist financing ("**TF**") risk to which the AMP is exposed, by virtue of the nature of its business and assessing the level of risk in a particular customer;

c) put in place appropriate anti-money laundering policies and procedures to include:

   i. the risks of ML/TF identified in the risk assessment described at point (b);

   ii. the responsibilities of senior management and all employees in relation to anti-money laundering compliance;

   iii. customer due diligence measures;

   iv. suspicious activity reporting procedures;

   v. internal control procedures, including cash and third-party payment handling;

   vi. use of reliance or outsourcing arrangements; and

   vii. ongoing monitoring activities;

d) nominate a person responsible for anti-money laundering compliance (the designated money laundering officer who will be responsible for any SARs);

e) train staff;

f) report knowledge or suspicions of money laundering or terrorist financing; and

g) keep records as proof of the customer due diligence measures mentioned above.

Customer due diligence ("CDD") measures

Conducting CDD is perhaps one of the more onerous requirements for AMPs, not least because the industry has traditionally placed great value on buyer confidentiality.

1. Required CDD Measures

CDD measures should enable AMPs to form a reasonable belief that they know the true identity of each customer and, where relevant, their beneficial owner. The MLRs require an AMP to identify the customer, verify the identity, and assess the purpose and intended nature of the business relationship or occasional transaction. In meeting their CDD obligations, AMPs should adopt a risk-based approach. This means assessing the risks of ML and TF that their business is subject to by taking into account: (i) information on ML and TF made available by HMRC; and (ii) risk factors relating to an AMP's customers, countries in which they operate, services they provide, their transactions, services and the delivery channels they use.

Who the customer is for the purpose of conducting CDD will vary depending on the AMP's business model. It will, however, always involve identifying the customer and any ultimate beneficial owner of the customer to identify the source of funds and source of wealth, to ensure the funds do not stem from criminal activity.

Where an agent is involved in the transaction, the AMP conducting the transaction must carry out CDD on the agent as well as the ultimate customer and verify that the agent is authorised to act on behalf of the customer. An AMP acting

as a selling agent must carry out CDD on the person on whose behalf they are selling the artwork; however, it is not necessary for the buyer (or agent) to conduct CDD on the ultimate seller.

2. When are AMPs required to conduct CDD?

Under the MLRs, CDD must be conducted by any AMP carrying out a regulated activity where it:

a) establishes a business relationship;

b) carries out an occasional transaction that amounts to a transfer of funds, as defined in Article 3(9) i.e. any transaction at least partially carried out by electronic means and exceeding EUR 1,000;

c) suspects money laundering or terrorist financing; or

d) doubts the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification.

In certain circumstances (usually where there has been a change of circumstance) CDD must also be conducted on existing clients and this would involve conducting the same checks as set out above. The factors to take into account when determining whether CDD is required for existing customers include:

a) any indication that the identity of the customer, or of the customer's beneficial owner, has changed;

b) any transactions which are not reasonably consistent with the relevant person's knowledge of the customer;

c) a change in the purpose or intended nature of the relevant person's relationship with the customer; and

d) any other matter which might affect the relevant person's assessment of the money laundering or terrorist financing risk in relation to the customer.

3. Can AMPs delegate their CDD obligations?

The obligation to carry out CDD cannot be delegated but reliance can be placed on third parties who are subject to the same CDD obligations. In practice, AMPs relying on the CDD conducted by an agent or intermediary should obtain written confirmation as to what checks were conducted to assess whether those checks were sufficient or if further checks should be carried out.

4. Are AMPs ever required to do more than standard CDD?

All AMPs must assess whether there are any particular ‘red flags’ relating to a particular customer and thus whether enhanced due diligence is necessary. Examples of situations that may warrant enhanced due diligence include where the buyer is a politically exposed person (“**PEP**”), or where either of the parties to a transaction are established in a high risk third country. The list of high-risk countries is set out in schedule 3ZA of the MLRs. This list can be updated relatively regularly, and additions can take effect in a matter of days, so AMPs should take care to ensure that they stay up to date with the most current version of the list.

Pursuant to UK and EU sanction regimes, AMPs are also obligated to ensure that they are not dealing or transacting with any sanctioned person. The UK government publishes regularly updated sanctions lists which provide details of those designated under the sanctions regulations and are accessible via the UK Government website (https://www.gov.uk/government/publications/the-uk-sanctions-list).

Implications of breaching the MLRs:

Failure by an AMP to comply with the MLRs and the additional obligations imposed on the regulated section under POCA and the Terrorism Act may have serious ramifications and senior management may be personally liable. Breaches may incur a maximum sentence of up to two years' imprisonment, a fine, or both.

However, there are far wider-reaching ramifications that may have an even greater impact on AMPs. For example, where an AMP inadvertently receives, handles, or otherwise deals with criminal property, that property could also be liable to seizure, forfeiture, or could be the subject to a freezing order. Not only could this lead to collateral reputational costs and legal fees, the AMP may ultimately lose the value of the seized/forfeited assets if it transpires that those assets were originally derived from the proceeds of crime.

In circumstances where an AMP failed to conduct appropriate CDD and therefore receives funds from a customer that are the proceeds of crime, the NCA or other enforcement authority may apply to freeze the AMP account holding those funds. Freezing an account results not only in the suspected criminal funds being frozen, but also any other funds held in that account (even if they come from a legitimate source). This is likely to be extremely disruptive to the AMP's business. Money laundering concerns could also result in banks withdrawing their services from the AMP entirely – a process known as "de-risking". A firm that has had banking services withdrawn by one bank may find it difficult to obtain services from other banks in the future.

AML regimes in the EU and the US

EU

Although no longer a member of the EU, the UK Government's intention in amending the MLRs was to give effect to the 5th EU Money Laundering Directive which required all EU Member States to transpose appropriate national legislation by the 10th of January 2020. Consequently, as of that date, similar provisions to those adopted by the UK under the MLRs will apply across all EU Member States.

US

Following various warnings on the risks associated with the art industry and money laundering, on 1 January 2021, Congress enacted the Anti-Money Laundering Act of 2020 as part of the National Defense Authorization Act for Fiscal Year 2021. This major development in the US anti-money laundering regime expanded the definition of *"financial institution"* in the Bank Secrecy Act – which governs how companies prevent money laundering – to include *"a person engaged in the trade of antiquities, including an advisor, consultant, or any other person who engages as a business in the solicitation or the sale of antiquities".*

Despite there being as yet no decision on who would qualify as a *"persons engaged in the trade of antiquities"* (a decision is due by 27 December 2021), those who do end up being covered by the regulations will face obligations in the US akin to those found in the MLRs. For example, businesses will be obliged to develop, implement, and maintain an effective anti-money laundering program and a monitoring system to identify transactions that may indicate criminal activity. Businesses that fail to comply with these obligations can be subject to civil or criminal penalties regardless of whether there is any evidence of money laundering itself.

Do's and Don'ts if you fall within the Regulations:

✓ DO urgently take steps to register with HMRC, if you had not already done so by the 10 June 2021 deadline;

✓ DO ensure that you have an AML policy in place as set out above;

- ✓ DO appoint an AML officer (sometimes known as a Money Laundering Reporting Officer, or MLRO), who will be in charge of making reports to the National Crime Agency ("**NCA**");
- ✓ DO train staff about the risks of money laundering, and the key warning signs (such as requests to pay large sums in cash or in instalments);
- ✓ DO undertake internal risk assessment to assess the level of ML and TF risk to which you are exposed and to identify mitigation strategies to overcome any identified risks;
- ✓ DO undertake stringent CDD to ensure you are not handling, receiving, or in any way dealing with criminal property;
- ✓ DO keep accurate and up-to-date records of client due diligence;
- ✗ DON'T tell someone if you suspect that they could be attempting to launder money, but immediately make a report to the AML officer; and
- ✗ DON'T conceal any suspicions you may have as to money laundering by a customer, but report any suspicious behaviour to the AML officer as soon as possible.