arcarta

Online AML Training

Art Market Anti-Money Laundering &
Financial Crime Prevention Training

Section 3:

Monitoring, Suspicious Activity, GDPR & Sharing Due Diligence

- Monitoring
- Suspicious Activity
- Data Protection
- Sharing Due Diligence

Monitoring

Effective CDD measures must include ongoing monitoring of the business relationship.

This involves the scrutiny of the transactions that take place during the course of the relationship to ensure that both the transactions and the activity being conducted are consistent with your knowledge of the customer, their business and their risk profile.

This includes, where necessary, exploring the source of the funds being used and ensuring that the documents, data and/or information held are kept up to date.

Particular scrutiny must be applied to ***unusual*** activity and/or transactions, and also to any ***higher risk*** activity.

This ensures money laundering or terrorist financing can be identified and, where possible prevented - or at the very least, reported to the National Crime Agency.

In effect, transaction monitoring is an automated way you can:

- Ensure that a customer's activity is in line with what you would expect it to be.

- Ensure that staff members identify and report any activities considered suspicious or unusual At the least, ensure these activities are identified automatically and then flagged internally for review - therefore enabling a ***four eyes check*** on what you would expect staff to identify.

- Identify suspicious or unusual activity that has been undertaken by ***Straight Through Processing (STP)*** - STP is a transaction that has been executed via an automated system without any human oversight or intervention.

The reports issued from transaction monitoring should be produced:

- In a timely manner.
- Related to a transaction that is relevant (not based on outdated procedures within the company).
- Related to an activity that is considered unusual or suspicious.
- Inline with the identified risks that need controlling or mitigating - this should not be dependant on the number of staff available to review the reports.

For each customer due diligence report, a Nominated Officer, Deputy or other member of staff, must satisfy the obligation under the regulations to write what is known as a ***'Client Risk Assessment'***.

A Client Risk Assessment will record what has been done and why - this is not an optional element but an essential part of your ***Reporting and Record-Keeping*** obligations.

In summary, transaction monitoring should be:

- The automated ears and eyes of a firm.
- Designed to spot unusual activity in automated or straight through processing (STP).
- Supplemental and supportive of the human eye.
- Up to date.
- Driven by risk, not resource.

Ordinarily, it should not be necessary to re-verify the identity of a customer, or *'re-run'* the customer due diligence once this has been satisfactorily completed.

You may choose to do so if:

- You have cause to doubt the authenticity or reliability of the original documents supplied.
- A suspicious activity occurs, that suggests that re-verifying the customer would be prudent.
- The risk profile of the customer changes, leaving the previously undertaken due diligence inadequate.
- A trigger event, such as some adverse media coverage occurs.

Suspicious Activity

Proceeds of Crime Act 2002 (POCA)

POCA created an obligation under UK law, requiring you to report any ***knowledge***, ***suspicion*** or ***reasonable grounds*** where you suspect money laundering or the proceeds of crime exist.

What is knowledge?

Knowledge is, well, knowledge - you can't unknow what you know!

What is suspicion?

Suspicion is personal and subjective and falls short of ***proof***, which is based on firm evidence.

A suspicion must at least have some foundation and not just be based on mere speculation.

What are reasonable grounds?

This involves adequately assessing facts and information that are either presented or available and that would put an honest and reasonable person on enquiry - an objective test.

The reasonable grounds test is a bit like this TV program:

“And our survey said…”

There is not always one easy way to identify suspicion.

You may feel comfortable at first with a proposed transaction or activity and only as time goes by do you begin to feel curious as to what is happening, or recognise that what is happening isn't the '*norm*'.

Alternatively, you may immediately feel curious, or concerned.

There is not a prescribed timeframe for identifying and reporting suspicion, but equally there is no excuse for unnecessary delay!

Unusual Versus Suspicious

It is important to distinguish between ***unusual*** and ***suspicious*** activity. Not all activity is suspicious just because we haven't seen it before.

You may not have seen a white squirrel before, but it certainly isn't suspicious.

The chap on the right however, well yes, he is suspicious!

Intelligent use of appropriate CDD can help you determine the difference.

The more we know about someone or something, the more we can tell whether it is genuine.

In the same way the more provenance you have on a painting allows you to tell if it is genuine or not, or whether the person trying to sell it to you is a fake too!

Sometimes unusual can be the start of the new usual.

Maybe a dealer you know has always dealt in traditional landscape artwork, and is now selling a piece by Damien Hirst.

This doesn’t necessarily mean the piece or the dealer is a fake, it may just be that the dealer is diversifying.

Maybe there is a greater call for modern art now, so the dealer is having to change their business model and in the future you will see them dealing more and more in modern art.

Internal Suspicious Activity Reporting

Holding up to date and accurate CDD information and reports allows you to determine a normal, expected pattern of activity for a customer.

When you know what normal and expected activity should look like, you are more readily able to identify what abnormal and unexpected activity looks like.

Often, abnormal or unexpected behaviour can lead to suspicion.

Remember!

The legal requirement is for ***YOU*** to report ***YOUR*** suspicion to your Money Laundering Reporting Officer (M.L.R.O.) or Nominated Officer (N.O.) – ***NOT*** a colleague.

Once reported to the M.L.R.O. or N.O. or once you become aware that the N.O. is investigating – you must ***NOT*** discuss the matter with anyone but the M.L.R.O. or N.O.

When your M.L.R.O. or N.O. upholds your concerns or suspicion, the matter will be reported to the National Crime Agency (NCA).

When making a report to the NCA, three considerations present themselves:

- Defence Against Money Laundering (DAML)/Consent
- Tipping Off
- Managing Customer Expectations

Defence Against Money Laundering (DAML)/Consent

Has the transaction taken place yet? If not, then you cannot process it if you are suspicious.

An application for a ***Defence Against Money Laundering (DAML)*** - or a ‘consent application’ in its more common form - will need to be made.

If granted, this defence will allow you to proceed with the transaction without being accused of being complicit in the offence of money laundering, or for assisting a money launderer.

The NCA have 7 working days to reply to a DAML request.

This period starts on the first working day after the DAML request is received by the NCA.

If a defence cannot be granted, a further 31 calendar days are available to law enforcement to take action.

Tipping Off

Once an internal investigation into suspicious activity is underway, or an external investigation by the NCA or other law enforcement agency, it is imperative that you do not talk about the situation to anyone other than your MLRO/NO.

If the customer was to find out that they had been reported, and they are genuinely involved in criminal activity, any alert that they receive in relation to the enquiries being made about them, could lead them to take actions that could thwart or prejudice the investigation.

Important!

Making someone aware that they are under investigation or taking any action that could prejudice an investigation could result in you facing criminal charges leading to a fine or imprisonment for up to 2 years.

Managing Customer Expectations

Due to the time that the law allows the NCA to process a DAML request, quite often it is difficult to manage the customer's expectations during this time.

After all, whether they are criminals or not, they just want to see their transaction processed.

Any situation such as this should be managed under the guidance and advice of your MLRO or NO.

Money Laundering Penalties

Money Laundering is a serious matter and as such carries equally serious penalties upon conviction.

- **Money laundering:**
  Up to 14 years in prison and/or an unlimited fine.
- **Failure to report:**
  Up to 5 years in prison and/or an unlimited fine.
- **Tipping off/Prejudicing an investigation:**
  Up to 2 years in prison and/or an unlimited fine.

Data Protection Considerations

The **General Data Protection Regulation (GDPR)** came into force in May 2018.

It is a ***regulation*** – this means it's directly applicable to all EU Member States without the need for additional national implementing legislation.

The UK also introduced a revised **Data Protection Act** in May 2018 to allow for compliance with the same principles as GDPR post Brexit.

GDPR/Data Protection Act 2018 is designed to:

- Harmonise data protection law across the EU.
- Transform the way in which personal data is collected, shared and processed globally.

The GDPR/DPA 2018 has high level principles:

- To provide greater rights for data subjects.
- To enhance the definition of personal data.
- To require firms to ensure exacting clarity when processing data.
- To expect firms to provide data subjects with fair processing notices.
- Firms must declare the legal basis under which they intend to process data.
- Data Subjects must provide explicit consent for their data to be processed.
- Increased fines for breaches – up to €20 million or 4% of a firm's global annual turnover, whichever is the greater.

The Art World & Cybercrime

The Art World is an attractive target owing to the high values which are transacted frequently.

Taking into account, process, competency and the infrastructure you are likely to expect in a large corporation, the art ecosystem by comparison is lacking in these areas.

Since 2017, the Art Market has had to contend with the threat of ***business email compromise*** attacks and in particular ***invoice fraud***. As of June 2020, invoice fraud increased by 155%, with one of the most recent high profile cases involving Dickinson and the Rijksmuseum Twenthe where $3.1 million was lost.

While many are becoming more familiar and aware of these threats, there are still those without a secure method of delivery, relying on phone calls and encrypted PDF invoices.

PDF Encryption is not a viable level of protection as there are many, widely available free services that unlock password protected PDF documents.

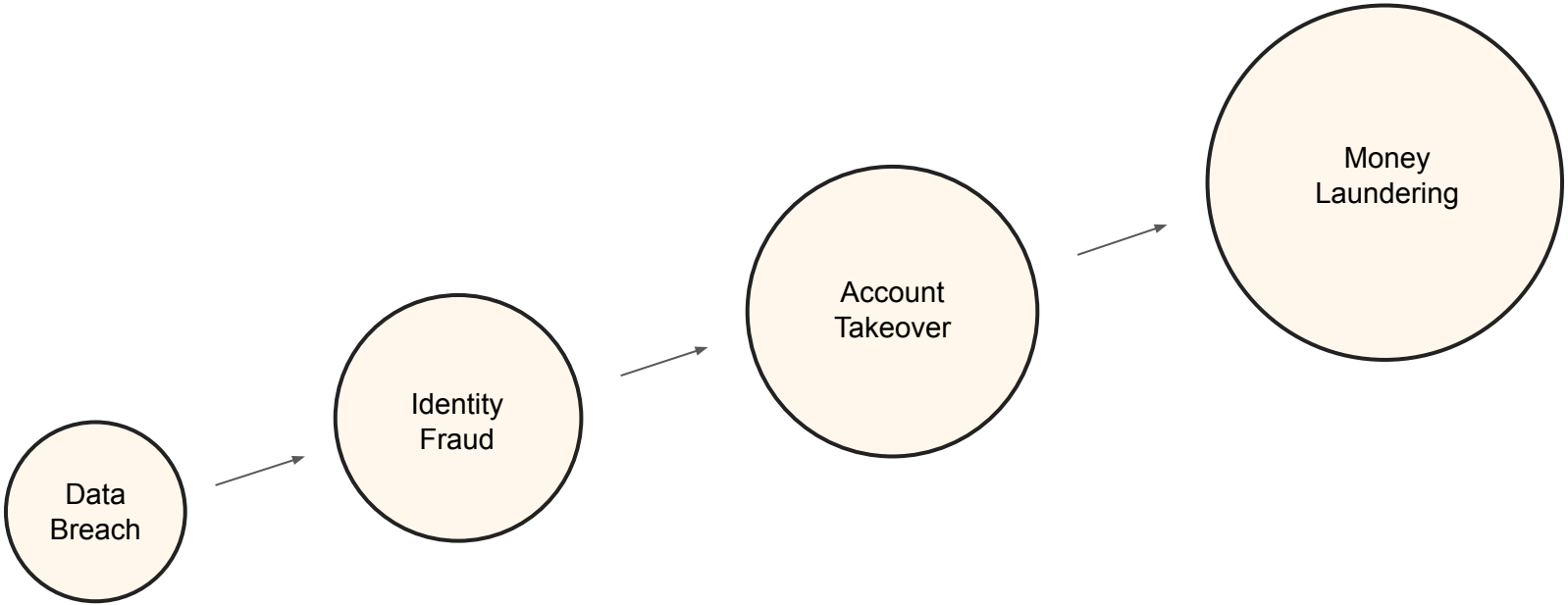
In light of the ongoing vulnerabilities of the Art World, any AMP now receiving ID documents over email, exposes the business to risk of GDPR fines as a result of ***identity theft***.

Email accounts are easily compromised and it is difficult to know if an account has been breached.

You are strongly advised to seek alternative processes and systems - such as those available in Arcarta - for the sending and receiving of any sensitive information.

Data Breach To Money Laundering

In today's world a breach of data security can lead to money laundering in 4 simple steps.



Identity theft can occur following any event where the security of someone's personal data is compromised.

This includes:

- Social or professional environment shoulder surfing.
- The hacking of databases or computer records - lots of companies store data in simple excel spreadsheets.
- The deliberate and malicious sharing of data.
- Well intentioned, but unauthorised sharing of data, possibly even to people we think we can trust!
- Emails containing personal information or with documents attached, sent insecurely allowing them to be intercepted.

But We Are Not a Bank!

These regulations can seem quite overwhelming and non banking institutions wonder why they have to do all of these checks if our bankers are doing them already?

All regulated entities and sectors have a responsibility to comply with the laws and regulations in their own right.

This is a fair challenge though, and no, as an AMP you are not a bank – but your bank is, and you are their customer!

Banks are now under more pressure than ever to know their customers.

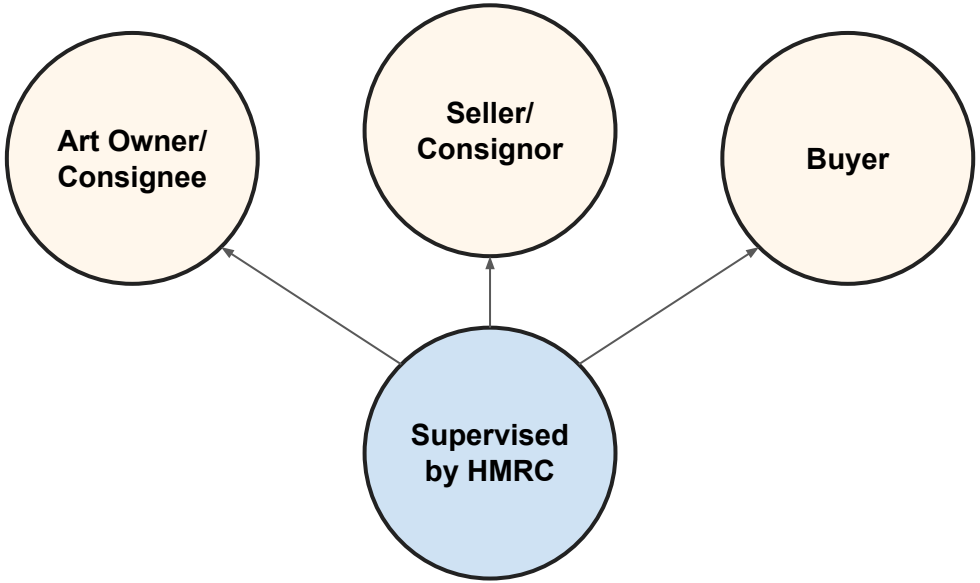
Just as you are now under pressure to prove that you know who your customers are and what risk they pose to you.

Banks face fines and even the prospect of losing their banking licence if they get it wrong.

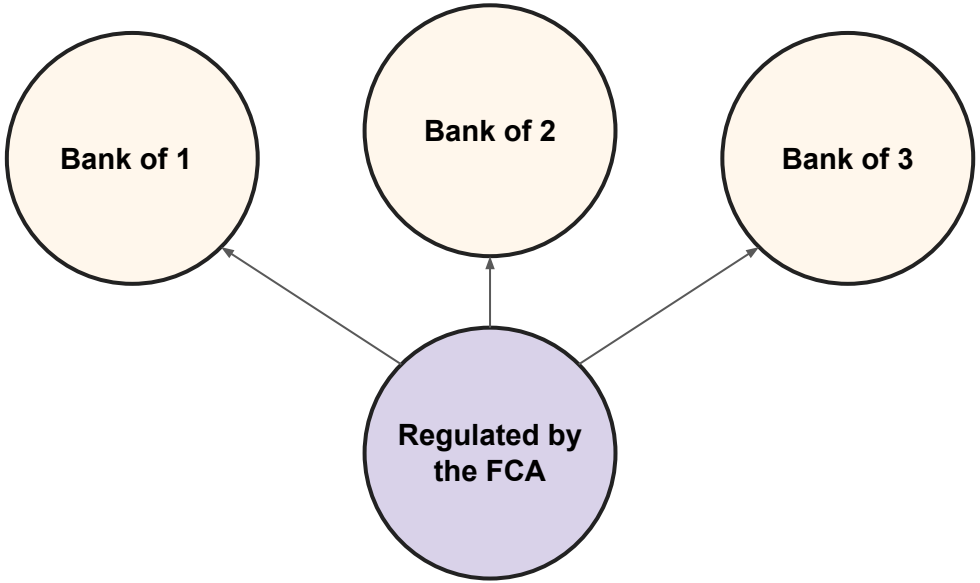
They want to make sure that they know everything about you and your business, to ensure that you don’t pose any unacceptable risks to them.

It is also important to remember, that each AMP will have an interaction with the other, and each has a relationship with their own bank. Regardless of who supervises or regulates them for money laundering purposes.

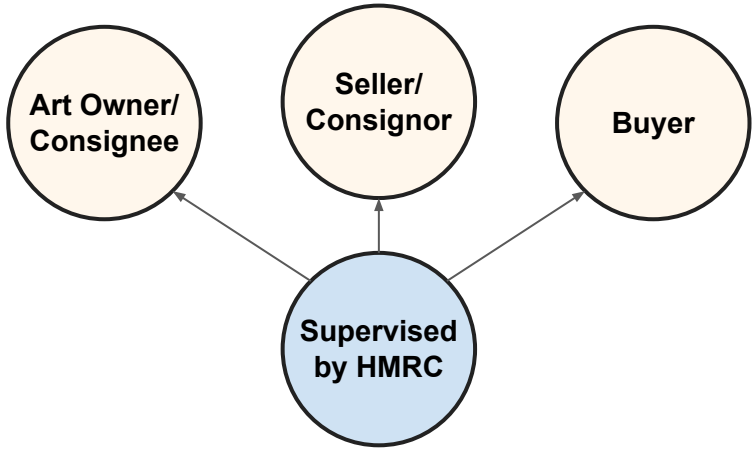
For example, an AMP may sit in one space, complying with the HMRC rules.

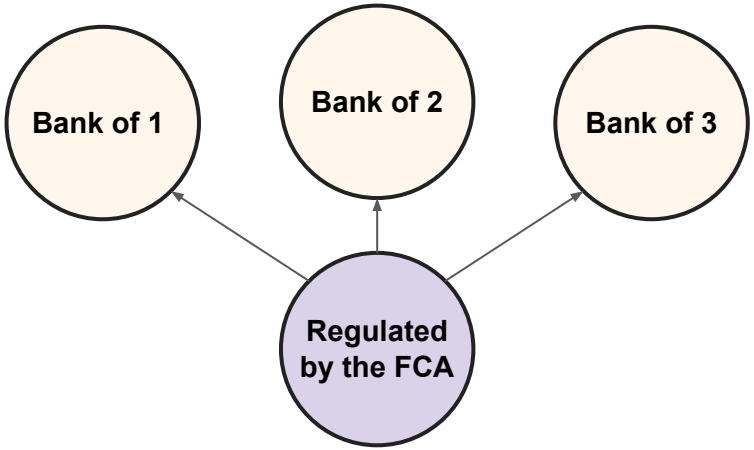


But their banks all sit together in another space, all complying with the FCA rules.



So the bank is applying the same rules to the AMP as the AMP is applying to its customers, just under different supervision.





Sharing Due Diligence

Working with other Art Market Participants

As Art Market Participants work with one another throughout the course of business, there may be instances where one party requires the other to demonstrate their due diligence processes.

This will include ***what*** has been performed and to what ***level***.

If one business is acting as an ***Intermediary***, they may be asked to share more about any underlying customer (the ***Ultimate Beneficial Owner***).

Sharing information about the ultimate beneficial owner is particularly relevant when:

- A UK registered Art Market Participant is dealing with a US-based business - as the US is not currently regulated.

- As part of a risk-based approach when the transaction is considered unusually large, or where there are multiple intermediaries involved.

As a UK AMP - as of 30th June 2022 - it may not always be necessary for you to know the identity of the ultimate customer when you are dealing with an intermediary based in the UK.

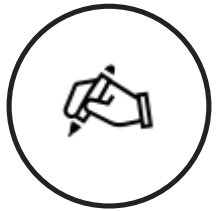
For a more comprehensive overview of your responsibilities when dealing with, or acting as an intermediary, follow the link below:

https://www.arcarta.com/events/updates-to-guidance

Activity:

Can you think of any situations that may see you - or an AMP with whom you're working - acting as an intermediary?

You will find the answers on the following page.



Consider the situations below:

1. You accept works on consignment from other galleries or dealers.
2. You co-own/have half shares in works with other galleries.
3. You sell at auction on behalf of your clients.
4. You buy at auction on behalf of your clients.
5. You deal with agents, advisors, consultants, interior designers or decorators.
6. A Family Office is acting on behalf of a private client.

If you’re ever unsure, an easy way to know if you’re acting as an intermediary would be to ask:

“Do I own the work of art I am selling outright?”

If not, then you’re viewed as acting as an agent and you may need to disclose information to another Art Market Participant if they too are regulated.

It is important to remember that your AML responsibilities cannot be delegated and there is a risk present when not carrying out Customer Due Diligence yourself.

You will be held responsible for any oversight or mistakes made by the intermediary.

You are advised to treat each case on an individual basis as part of your risk-based approach.

Summary

In this section we explored the steps we should take when ***Monitoring*** transactions and customers.

We have covered the definition of ***Suspicious Activity*** and important things to remember when reporting to the NCA.

The ***Data Protection Considerations*** section made us aware of the risks present when sending and receiving sensitive information and how to prevent cybercrime.

We understand the process when working with - or acting as an - ***intermediary.***

If you are still feeling unsure about any of the subjects we've covered in this section, feel free to return to and review those areas again.