1 Introduction

1.1 This policy contains the procedures I have adopted to comply with my obligations under the MLR.

2 Definition of money laundering and terrorist financing

2.1 Money laundering is the process through which the origin of the proceeds of crime is changed so that the proceeds appear to be legitimate.

2.2 Terrorist financing is providing or collecting funds to be used to carry out an act of terrorism.

3 The role of a Notary in the AML and CTF regime

3.1 A Notary Public is an independent legal professional for the AML and CTF regimes.

3.2 As a Notary Public, I have obligations under the AML and CTF regimes to spot and report money laundering and terrorist financing. Failure to meet these obligations can lead to criminal penalties, substantial fines and damage to my reputation.

4 The stages of Money Laundering.

Placement—placing criminal property into the financial system.

Layering—moving money that has been placed in the financial system to obscure its origin.

Integration—the money ultimately reappears in the financial system as legitimate funds.

My notarial practice is at the greatest risk of becoming involved in the layering stage but could be involved in any stage.

5 Red Flags

5.1 I am alert to the warning signs of money laundering and terrorist financing, and I am obliged to make the sort of enquiries that a reasonable person with the same qualifications, knowledge and experience as I would make.

5.2 Typical signs (Red Flags) of money laundering and terrorist financing can be:

5.2.1 obstructive or secretive clients

5.2.2 clients who do not appear to be running the transaction.

5.2.3 corporate clients that I can't find online or that use free email addresses.

5.2.4 clients who have unusual knowledge of the AML and CTF regime

5.2.5 clients based a long way from me with no apparent reason for instructing me.

5.2.6 clients who provided false or stolen identification documentation

5.2.7 clients or instructions involving high-risk third countries—which means a country that has been identified by the EC as high-risk. The EC formally adopted a new list of high-risk third countries in 2019, amending the list contained in Commission Delegated Regulation (EU) 2016/1675. See the

current list at
https://ec.europa.eu/commission/presscorner/detail/en/IP_19_781

5.2.8 corporate clients with unusual or excessively complex structures

5.2.9 long-term clients that start making requests that are out of character.

5.2.10 clients who request arrangements that do not make commercial sense.

5.2.11 client who has criminal associations

5.2.12 instructions that change for no logical reason

5.2.13 clients who want to pay me higher fees than usual.

5.2.14 clients who put me under pressure to meet them and witness their signatures via video conference.

5.2.15 clients who put me under pressure to relax my usual identity verification procedures or to accept unusual documents in support of my verification when I do not feel comfortable doing so or it does not make sense.

6 Money laundering offences under POCA

6.1 The principal offences - carry a maximum penalty of 14 years imprisonment, a fine or both.

6.1.1 POCA section 327

An offence is committed if someone conceals, disguises, converts, transfers, or removes from the UK criminal property. This includes concealing or disguising its nature, source, location, disposition, movement, ownership or any rights concerning it.

6.1.2 POCA section 328

An offence is committed if someone enters into or becomes concerned in an arrangement which they know or suspect facilitates the acquisition, retention, use or control of criminal property by or on behalf of another.

6.1.3 POCA section 329

An offence will be committed if someone acquires, uses, or has possession of criminal property.

6.2 The Regulated Sector Offence of Failure to Disclose

Failure by a staff member to make an ISAR to the Nominated Officer where they know or suspect money laundering is an offence which is punishable by up to five years imprisonment, a fine or both.

6.3 Tipping off and prejudicing an investigation

6.3.1 An offence will be committed if someone discloses that they or anyone else has made [an ISAR to the Nominated Officer or] a SAR to the NCA of information which came to them during business, and that disclosure is likely to prejudice any investigation that might be conducted.

6.3.2 The offence of prejudicing an investigation will be committed if someone discloses that an investigation is being contemplated or carried out and that disclosure is likely to prejudice that investigation.

7 Terrorist financing offences

7.1 The TA introduces offences like those contained in POCA, for example, the offences of use or possession or laundering money for terrorist purposes, becoming involved in an arrangement which you suspect can be used for terrorist purposes, and tipping off. It also has a specific offence for fundraising for terrorist activities.

8 MLR

8.1 The MLR require me to introduce systems and controls to combat money laundering and terrorist financing. They apply to notaries concerning certain types of work only. Failure to comply with the MLR can carry a maximum penalty of two years' imprisonment, a fine or both.

9 Reporting suspicions – a SAR

9.1 POCA and TA impose obligations to report knowledge or suspicion of money laundering or terrorist financing by way of a SAR.

9.2 Knowledge and Suspicion

'Knowledge' under POCA means actual knowledge.

'Suspicion' is a possibility which is more than fanciful. A vague feeling of unease will not suffice. There is no requirement for the suspicion to be clear or firmly grounded on specific facts, but there must be a belief that is beyond mere speculation. The test for whether you hold a suspicion is generally subjective, but there is an objective element to the test, ie would a reasonable person, with the same knowledge, experience and information, have formed a suspicion.

9.3 After a SAR has been lodged with the NCA they have seven working days following receipt to decide whether to give consent. If they give consent or do not refuse consent, I have a defence to a principal money laundering or terrorist financing offence so I can continue to act within the limits of the consent requested. If the NCA refuse consent they have a further 31 days to act. If I hear nothing within this period, I am deemed to have consent. In exceptional circumstances, the NCA may apply to court under the provisions of the Criminal Finance Act 2017 to extend the period for a further 31-day period, up to a maximum of 186 days over the original 31 days.

10 CDD

10.1 CDD is required when I am instructed to act on the types of transaction listed in Regulation 12 of the MLR (which I have set out below in subclauses numbered 10.1.1 – 10.1.5) and the exemptions set out in the Legal Sector Guidance do not apply:

10.1.1 The buying and selling of real property or business entities.

10.1.2 The managing of client money, securities or other assets.

10.1.3 The opening or management of bank, savings or securities accounts.

10.1.4 The organisation of contributions necessary for the creation, operation or management of companies.

10.1.5 The creation, operation or management of trusts, companies or similar structures.

10.2 The Legal Sector Guidance, which is approved by HM Treasury, states that the MLR do not apply to work undertaken by a notary as a public certifying officer where he or she has no substantive role in the underlying transaction. As such, the MLR do not apply to many aspects of my practice, including the taking of affidavits and declarations, protests, translating, certifying the execution of documents and authentication work in general. Although the MLR will not apply to work of that nature, as I offer notarial services, I am still subject to obligations under the Notaries Practice Rules and Code of Practice positively to identify intervening parties and to keep records of the method of identification employed. I will determine with each new instruction whether the MLR will apply and will undertake CDD as required.

10.3 There are four components of CDD:

10.3.1 identifying and verifying the client's identity

10.3.2 identifying the beneficial owner where this is not the client.

10.3.3 obtaining details of the purpose and intended nature of the business relationship.

10.3.4 conducting ongoing monitoring of business relationships with my clients.

10.4 There are three levels of CDD:

10.4.1 Simplified Due Diligence (SDD)

10.4.2 enhanced due diligence (EDD)

10.4.3 Regular Due Diligence (RDD)

10.5 Beneficial owners

Where the client is beneficially owned by another person, I take reasonable measures to verify the identity of the beneficial owner so that I am satisfied that I know who they are, and if the beneficial owner is a trust, company, foundation or similar entity, I take reasonable measures to understand the ownership and control structure of that entity.

10.6 Person acting on the client's behalf.

Where a person is purporting to act on behalf of the client, I verify that they are authorised to act on the client's behalf, identify them, and verify their identity on the basis of documents or information obtained from a reliable independent source.

10.7 I conduct CDD if required:

10.7.1 when I establish a business relationship with a client

10.7.2 when I carry out an occasional transaction for a client

10.7.3 when I suspect money laundering or terrorist financing

10.7.4 when I doubt the authenticity or adequacy of documents or information previously obtained for the purposes of identification or verification

10.7.5 where the client has not been in regular contact for *three years* or more

10.7.6 concerning existing clients, when their circumstances change.

10.8 I determine the extent of my CDD measures on a risk-sensitive basis, depending on the type of client, business relationship and the matter. I must also be able to demonstrate to the Faculty Office, my supervisory body, that the extent of my CDD measures is appropriate given the risks of money laundering and terrorist financing identified in my firm-wide risk assessment and as identified by the Faculty Office.

10.9 If I am not acting as a public certifying officer and the instructions fall within the list of transaction types set out in Regulation 12 of the MLR, I start by assessing the risk of money laundering or terrorist financing posed by the specific client and I decide the necessary level of CDD for the client itself.

10.10 I then go on to consider the risks associated with the business relationship, including the service, transaction, delivery channel risks, and geographical risks and I take into account risks attached to certain sectors identified as being subject to an increased risk of corruption, for example, construction, mining and arms' manufacturing.

10.11 I do not usually conduct the full CDD process for each new matter I open for an existing client. On those occasions, I consider the instructions I typically receive from the existing client and the type of work I'm being asked to do for the client in this instance. If the instructions have changed from the usual instructions I receive from that client, I start again from the beginning and re-assess the risk presented by the business relationship with that client.

10.12 Once I have completed my risk assessment, I decide what level of CDD to apply and what information and documentation I need from the client or from independent sources.

10.13 Sometimes clients are unable to provide standard verification documents, but if that is consistent with the client's profile and circumstances and I am not suspicious I consider accepting other forms of documentation from that client.

11 CDD records

If I am required to conduct CDD on a client, I keep a copy of my risk analysis form and the supporting records. The documents are retained in line with my document retention policy.

12 CDD—different levels of CDD

12.1 Simplified due diligence (SDD)

SDD is a downward adjustment of the level of measures I take to comply with CDD requirements where the business relationship or transaction presents a low risk of money laundering or terrorist financing. I must consider my firm-wide risk assessment, information provided by the Faculty Office and the risk factors set out in the MLR.

12.2 Enhanced due diligence.

EDD is a high-level measure required to mitigate the increased risk presented by certain clients and certain transactions. I apply EDD measures and enhanced ongoing monitoring in any case identified as presenting a high risk of money laundering or terrorist financing in my firm-wide risk assessment or by the Faculty Office, in any transaction with a person based in a high-risk third country, where the client is a PEP, where a client has provided false or stolen identification documentation and where I do not meet my client.

I use internet search engines to determine whether a client or its beneficial owner is a PEP.

For transactions involving PEPs I:

12.2.1 consider whether there are any warning signs of corruption,

12.2.2 consider whether there is any evidence that government or state funds are being used inappropriately.

12.2.3 take adequate measures to establish the source of wealth and the source of funds which are involved in the proposed business relationship or transaction.

12.2.4 conduct enhanced ongoing monitoring of the client.

For all other (non-PEP) high-risk clients I:

12.2.5 as far as I can, examine the background and purpose of the transaction.

12.2.6 increase ongoing monitoring.

12.2.7 seek additional independent, reliable sources to verify information provided by the client.

12.2.8 take additional measures to understand the background, ownership and financial situation of the client and other parties to the transaction.

12.2.9 increase the monitoring of the business relationship.

12.3 Regular due diligence (RDD)

I apply RDD when SDD and EDD are not appropriate.

13 CDD—beneficial owners

13.1 Where the client is beneficially owned by another person, I:

13.1.1 identify the beneficial owner (being anyone who directly or indirectly holds more than 25% of the share capital or voting rights of the entity) and take reasonable measures to verify their identity and

13.1.2 if the beneficial owner is a trust, company, foundation or similar entity arrangement, take reasonable measures to understand the ownership and control structure of that entity.

13.1.3 I obtain at least their name and record any other identifying details which are readily available or ask my client for the information. I assess the verification

I need, considering the client's risk profile, any business structures involved and the proposed transaction.

14 CDD—source of funds

14.1.1 Scrutinising the source of funds is more than asking for the money to come from a bank account in the client's name. I focus on understanding how the client can legitimately fund the transaction.

14.1.2 If I have any concerns about the source of funds, I consider whether I need to submit a SAR.

15 Where I cannot conclude the CDD exercise

15.1 I:

15.1.1 do not carry out a transaction through a bank account with the client or on their behalf.

15.1.2 do not establish a business relationship or carry out an occasional transaction with the client.

15.1.3 terminate any existing business relationship with the client.

15.1.4 do not accept or return funds from the client or on the client's behalf.

15.1.5 consider whether I should submit a SAR to the NCA

16 CDD—Reliance

16.1 The MLR allow me to rely on a third party for the required CDD measures, however:

16.1.1 they are very specific about exactly who I can and cannot rely on

16.1.2 I remain liable for any failure in the third parties' application of those measures.

16.1.3 I am required to obtain from the third party all the information needed to satisfy CDD requirements and enter written arrangements with that third party which enable me to obtain copies of any relevant documents and require the third party to retain those documents.

16.2 The provisions work both ways and I can be relied on by other companies to perform CDD measures on a mutual client. However, agreeing to reliance is a serious matter. Any such requests from other companies are considered carefully. In many instances, my client is not the same as theirs in the transaction, and my position as a public certifying officer may mean that the MLR does not apply to my role in the transaction, and I have not been obliged to collect the information required to satisfy CDD.

16.3 It is my usual policy to refuse to let others rely on my CDD.

17 CDD—ongoing monitoring

17.1 Ongoing monitoring must be performed on all matters to detect unusual or suspicious transactions. I conduct ongoing monitoring by keeping in regular contact with my clients and I revisit the CDD I hold on them every three years.

18 Payment of fees and receipt of transaction funds from a third party

18.1 Where I cannot verify the source of the funds for a transaction or where there does not appear to be a legitimate reason for a third party to be paid, this may be a warning sign of money laundering or terrorist financing.

18.2 If the funds for a transaction or for my fees are coming from a third party, I check that the funds are coming from a legitimate source for legitimate reasons.

19 Cash payments.

I have a policy of never receiving cash payments from clients, whether for the transaction or my fees. I note that payments of my legal fees are exempt from the provisions of the MLR as confirmed by HM Treasury in the Legal Sector Guidance.

20 Training and awareness

All relevant employees will be trained on the law relating to money laundering and terrorist financing at least every *2 years*.

21 Monitoring and reviewing this policy

I will review this policy annually and more frequently if there are any major changes in the law or if there are changes in my practice which impact on this policy.

KEM MASINBO-AMOBI / SOLE PRACTITIONER NOTARY

Drafted and Updated:	04.10.23 – following the introduction of the Fifth Money Laundering Directive
Next review date:	04.10.2023