Anti-Money Laundering & Combating Terrorist Financing

Guidance

Introduction

Overriding Principle 2 of the ***CLC Code of Conduct*** requires you to maintain high standards of work. The approach set out below aims to help you comply with that principle. You are not obliged to adopt this approach, but it offers you an example of the minimum commitment that the ***CLC*** considers is likely to be needed for compliance.

Should you use the provided example as your starting point, it is likely that you would need to make amendments to ensure that it matches your particular circumstances.

The procedures you adopt should apply a risk-based approach, taking into account the nature of your work, ***client***s, and the number of ***employee***s.

Contents:

---

1. AML/CTF *Example Policy*

IMPORTANT

It is essential that that the business and its ***employee***s comply with the letter and spirit of this policy since failure to do so may amount to a criminal offence for which it is possible to be sentenced to a term of imprisonment.

1. As a business, we are committed to complying with the ***anti-money laundering legislation***, in particular the Proceeds of Crime Act 2002, the Terrorism Act 2000 (each as amended) and the Money Laundering Regulations 2017 (as amended by the Money Laundering and Terrorist Financing (Amendment) Regulations 2019).

2. We must at all times take steps to ensure that our business is not used to launder the proceeds of crime or to assist terrorist financing.

3. We must explain to ***client***s the need to obtain proof of identity and the limitations on our duty of confidentiality to them either in our ***terms of engagement*** or otherwise in writing.

4. We accept that the ***Nominated Officer*** has full autonomy in carrying out their duties.

5. We will ensure that you are given appropriate and regular training to help you comply with AML/CTF, this policy and the procedures of the business.

6. We will communicate to you details of any types of business we have decided not to accept.

7. We will regularly monitor and review our policies, procedures and training.

8. We require all of the business's members to follow carefully the procedures set out in the Procedures Manual.

---

2. AML/CTF *Example Procedure*

IMPORTANT

It is essential that that the business and its ***employee***s comply with the letter and spirit of these procedures since failure to do so may amount to a criminal offence for which it is possible to be sentenced to a term of imprisonment.

<u>Procedures</u>

1. You must not act or continue to act for a ***client*** until all requirements for ***Customer Due Diligence*** (***CDD***) or Enhanced ***Customer Due Diligence*** (EDD) have been met.

   If these cannot be met, you must:

   a) not establish a new business relationship; or

   b) terminate any existing business relationship.

   You must then consider whether to make an internal report to the ***Nominated Officer***.

2. The purpose of ***CDD*** and EDD is to help you decide whether your ***client***s are the persons they say they are and that you can:

   a) know with some certainty whether your ***client***s are acting on behalf of another (called a ***beneficial owner***);

   b) establish there is nothing to prevent you providing the service requested;

   c) assess whether the purpose of the instruction is consistent with the lifestyle and economic means of your ***client***s;

   d) establish there are no obvious elements which suggest that any transaction is unusual or overly complex in the context of those instructions.

3. Whenever instructed by any ***client*** you must obtain evidence as early as possible that:

a) the ***client*** is the person he or she claims to be, for example, by a current signed passport or current UK photo driving licence or by using an electronic ID system; and

b) a person of that name lives at the address given, for example, by a utility bill less than 3 months old or mortgage statement.

4. Further examples of acceptable ID evidence are set out in the Acting for Lenders and Mortgage Fraud Code and ***Guidance***. Photocopies should always be certified as being true copies of the original and signed and dated by the person making the copies.

5. You should find out whether there is a ***beneficial owner*** in which case you must be satisfied who that person is. A ***beneficial owner*** is the person who ultimately owns and controls the ***client*** on whose behalf a transaction is being conducted. There may be more than one. If the ***client*** is a ***company*** you must identify who owns 25% or more of the structure and who exercises effective management and control. If your client is a non-natural person you must take reasonable measures to understand the person's ownership and control structure.

6. If you discover any discrepancy between the information you collect about a non-natural client and information collected from a relevant register, you must report the discrepancy to Companies House as soon as is reasonably possible.

7. EDD checks must be made in any situation which by its nature can present a higher risk of money laundering or terrorist financing. Under the Money Laundering Regulations 2017, EDD is no longer mandatory if you do not see your client although should be considered as one of the risk factors.

8. You must apply EDD when any of the following apply: the transaction is complex; the transaction is unusually large; there is an unusual pattern of transactions or the transaction or transactions have no apparent economic or legal purpose.

9. You must apply EDD and ongoing monitoring when the client or counterparty is established in a high risk third country.

10. Politically Exposed Persons (PEPs), which include local PEPs, are deemed to be higher risk. The approval by senior management is required for establishing or continuing the business relationship with a PEP, a family member of known close associate of a PEP.

11. In addition to the usual steps taken to verify identity for ***CDD***, you should obtain at least one additional document of identity or verify identity electronically through [state specific source the business uses].

Checking identity by electronic means

12. You must obtain "satisfactory evidence of identity", which must be reasonably capable of establishing (and does in fact establish to the satisfaction of the person who obtains it) that the potential ***client*** is the person they claim to be. Electronic evidence obtained should provide you with a strong level of certainty that any individual is the person they claim to be and that a person of that name lives at the address given using the ***client***'s full name, address and date of birth as its basis.

13. You must satisfy yourself that any system or product used must be sufficiently robust to provide the appropriate level of assurance customers are who they say they are and that it is secure from fraud and misuse. Data accessed from a single source (e.g.

the Electoral Roll) will not normally be sufficient on its own. Some databases will offer a higher degree of confidence than others.

14. Before using a commercial agency for electronic verification, you must be satisfied that:

    a) The information supplied by the data provider is considered to be sufficiently extensive, reliable and accurate; and

    b) The agency has processes which allow its users to capture and store the information that they have used to verify an identity.

    The process should be cumulative and you may consider it appropriate to seek additional evidence (e.g. a copy of a document bearing a signature and a date of birth) in all cases or, at least, where any ***client*** poses a higher risk of identity fraud, money laundering or terrorist financing, or where the result of any electronic verification check gives rise to concern or uncertainty over the ***client***'s identity.

15. You may wish to consider whether the provider meets each of the following criteria, namely that it:

    a) Is recognised to store personal data through registration with the Information Commissioner's Office;

    b) Uses a range of positive information sources that can be called upon to link an applicant to both current and previous circumstances;

    c) Accesses negative information sources such as databases relating to identity fraud and deceased persons;

    d) Accesses a wide range of alert data sources; and

    e) Has transparent processes that enable you to know what checks were carried out, what the results of these checks were and what they mean in terms of how much certainty they give to the identity of the subject of the identity enquiry.

16. Data from more robust sources where inclusion is based on proof of identity (such as government departments) ought to be included (under paragraph 12(b)). Negative information checks (under paragraph 12(c)) minimise the risk of impersonation fraud.

17. It is also important for:

    a) The process of electronic verification to meet a standard level of confirmation before it can be relied on. In circumstances which do not give rise to concern or uncertainty, the standard level would be expected to be:

        i One match on an individual's full name and current address *and*

        ii A second match on an individual's full name and *either* their current address or their date of birth.

    If the result of a standard verification check gives rise to concern or uncertainty over the ***client***'s identity, the number of matches required to provide reasonable satisfaction as to their identity should increase.

b) You should ensure you understand the basis of the system you use in order to be satisfied that the sources of the underlying data reflect the ***CLC***'s requirement and cumulatively meet the standard level of confirmation set out above as commercial agencies use various methods of displaying results (e.g. by the number of documents checked or through scoring mechanisms, etc).

Good Practice – Due Diligence

18. a) Ongoing management/review of relationships with third parties.

b) Open source internet searches against other firms and its staff, including adverse information published by any relevant regulatory bodies and credit-checking.

c) Scrutinising, clarifying and verifying the information received from parties connected to the transaction, considering risks presented by new mortgage products.

d) Systems and processes for checking the identity of foreign ***client***s.

e) Checking that deposit/other monies or assets appear to be from a legitimate source.

f) Considering whether property valuations appear to be reasonable.

g) If your ***client*** changes while you are acting on a transaction, contact both the old and new ***client*** so you understand the reason for the change and are satisfied that it appears to be for a legitimate reason.

h) Electronic identification check with each ***client*** as soon as instruction is received; use a service provider accessing a unique system which matches identity of ***client*** using ID and verifying confidential information known only to ***client*** and provider.

19. You keep a record and take copies of all relevant documentation about the ***client***'s identity and address and we must keep them for at least 5 years.

20. You make reasonable enquires and take copies of all relevant documentation relating to the source of funds and we must keep them for at least 5 years.

21. If you are not satisfied with the documentation or explanation you are given you should consider whether to make further enquires (either orally or in writing), where appropriate, seeking ***guidance*** from a supervisor or someone with more experience within the business.

22. Examples of Warning Signs which you should take into account in deciding whether to make an internal suspicion report are set out in the Acting for Lenders and Prevention & Detection of Mortgage Fraud Code and ***Guidance***, paragraph 16, and include:

- secretive ***client***s;
- involvement of unconnected third parties
- unusual instructions
- variance in signatures
- an existing ***Client*** asks you to rely on former identity checks i.e. 'reliance' exemptions

- where a ***Client*** is introduced by a third party who is not well known to the ***Authorised Person*** or the firm
- ***Client*** declines to be met or come to the office and/or uses an intermediary to communicate with the body and/or asks the body to contact him at his business or another address rather than at his home address
- the ***Client***'s credit history is not aligned to their age (it might be longer or shorter than expected)
- monies paid by someone other than ***Client***
- the transaction does not seem consistent with your knowledge of the ***Client***'s financial position and income sources
- impatient parties putting pressure on you to complete the transaction quickly where the reason for urgency is not immediately apparent
- where another ***Authorised Person*** has previously been acting
- document not signed in front of you
- reliance on the diligence of another party
- discrepancies in value recorded in documents
- where a ***Client*** shares an address with one or more parties to the transaction
- overpayments of money.

This list is not exhaustive and you will need to exercise your skill and judgment to assess any circumstances involved in a transaction which may seem to you or to an ordinary member of the public to be unusual or out of the ordinary.

23. You should not accept cash payments in excess of [amount][1] made either to yourself or to any practice bank account. Deposits should not be paid in cash.

24. If the nature of the transaction, the documentation or information you have been given would have aroused suspicions for a reasonable and honest ***Authorised Person***, then you must immediately make an internal suspicion report in writing using our prescribed form to [name] who is our ***Nominated Officer*** (or in his absence [name]). [The business should suggest a procedure to support its ***employee***s when dealing with customer enquiries once a report has been made.]

25. Once you have made a report to the ***Nominated Officer***, no further action should be taken regarding the transaction without the specific authority of the ***Nominated Officer***.

26. You must not disclose your suspicions or the fact that you have made a report to the ***Nominated Officer*** to any other person, in particular the person who is the subject of

[1] CLC Practices should, with regard to their practice-wide risk assessment and risk profile, consider whether they will accept cash payments. If they do, they should enforce a limit for the amount of any such payment which should apply individually and in aggregate to each client matter.

such a report, since this may amount to "tipping off", which is also serious criminal offence for which you could be imprisoned.

27. You must respond ***promptly*** to requests from the ***Nominated Officer*** for any further information.

28. Further ***CDD***/possible warning signs/good practice ***guidance*** can be found in the Acting for Lenders and Prevention & Detection of Mortgage Fraud Code and ***Guidance –*** see, in particular, paragraphs 16 & 17.

---

3. AML/CTF *Example Policy* for the body's appointed *Nominated Officer*

1. The business requires you as its ***Nominated Officer*** to comply with this policy in addition to complying with the business's AML/CTF policy.

2. Failure to carry out your duties may cause you to commit a criminal offence.

3. You will have access to all files, records and information and be given sufficient resources and authority to fulfil the role and be allowed to carry out your duties without fetter, influence or interference.

4. Upon receipt of each internal suspicion report from any of the business's members, you must acknowledge receipt in writing to the person making the report. You must then consider carefully whether a report should be made to the ***National Crime Agency*** (NCA).

5. You must make a report to NCA in the prescribed form where you have actual knowledge or suspicion, or where (based on what an ordinary member of the public might think) there are reasonable grounds to know or suspect a money laundering offence has been committed. You will need Consent from NCA for an ongoing transaction to proceed.

6. If you do make a report to NCA then you must ensure that you maintain regular telephone contact with them where Consent is required.

7. You must maintain a record of each decision you have made and keep it for at least 5 years whether or not you send a report to NCA.

8. You must support and advise members of staff who make internal suspicion reports to you, emphasising the implications for them of "tipping off". In particular you must do this where you are waiting for Consent to proceed from NCA.

---

4. Example of AML/CTF Training Record

Date	Details of training	Name of attendee	Attendee's signature	Trainer's signature

The signature of the attendee acknowledges that training has been received to satisfy the current requirements of the body's AML/CTF policy.

---

5. Example of Internal Reporting Form and Record of Decision

NB: Neither this form nor any copy is to be kept on the *client* file

PART 1

Name of Person making report	
Name of Nominated Officer	
Name(s) of client	
File Reference Number	

Address of Property involved	
Reasons for making the report / reasons for suspicion of money laundering	
Additional Information Signature of person making the report: Date:	
PART 2	
(To be completed by the Nominated Officer) Date received Additional information requested	
External report: Yes / No Reason for decision	Ref

Signature of Nominated Officer	Date

---

6. Example of wording to be incorporated into the *Terms of Engagement*

6.1. Proof of Identity

We must by law obtain satisfactory evidence of your identity and address. Please help us to do so by giving us the information and documentation we ask for. We are unable to proceed with your transaction and will not be able to exchange contracts until this has been provided.

6.2. Confidentiality

As lawyers, we are under a general professional and legal obligation to keep your affairs private. However, we are required, by current legislation, to make a report to the National Crime Agency (NCA) where we know or suspect that a transaction involves Money Laundering or Terrorist Financing. By instructing us to act on your behalf in accordance with these ***terms of engagement*** you give us irrevocable authority to make a disclosure to NCA if we consider it appropriate.

6.3. You agree that this authority overrides any confidentiality or entitlement to legal professional privilege. We shall be unable to tell you if we have made a report.

---

7. External Reporting Form

7.1 A copy of the current Suspicious Activity Report (SAR) form may be accessed on the website for the ***National Crime Agency*** by following the links at http://www.nationalcrimeagency.gov.uk/ and downloading the form. Alternatively, a SAR may be filed electronically by registering for and activating the On-line service on the "Reporting SARs" button.

7.2. For information or assistance with submitting SARs, SARs online queries, consent issues or general Financial Intelligence Unit matters telephone the UK Financial Intelligence Helpdesk on 020 7238 8282 and select the appropriate option. For general UKFUI matters email ukfiusars@nca.x.gsi.gov.uk . Contact details:

http://www.nationalcrimeagency.gov.uk/contact-us/reporting-suspicious-activitysar.

October 2020