1. Introduction

CDC defines money laundering as the process by which the true origin and ownership of the proceeds of criminal activities are disguised in order to be used without suspicion. Money laundering takes many forms including:

- Trying to turn money raised through criminal activity into 'clean' money ('classic' money laundering)
- Handling income from acquisitive crimes such as theft, fraud and tax evasion
- Handling stolen goods
- Being directly involved with any criminal or terrorist property, or entering into arrangements to facilitate the laundering of criminal or terrorist property
- Criminals investing the proceeds of their crimes in any financial products

For the purposes of this Toolkit 'money laundering' covers both terrorist and non-terrorist financing.

- Money laundering: a global problem
  Money laundering is a global problem and frequently occurs across borders. Recent advances in technology and the increasing number of online business transactions have exacerbated the problem. Money laundering techniques are flexible by nature and easily adapt to the business environment of any jurisdiction. Money launderers often have vast resources at their disposal and receive professional assistance to carry out their activities. Countries with developing economies or those undergoing changes in their financial system are particularly vulnerable and can be lucrative markets for money launderers.

- The money laundering process
  There are three recognised parts to a money laundering process:
  1. **Placement**: This is the physical placement or depositing or cash into banks and other financial institutions such as currency exchanges. Deposited cash and assets are then converted into other financial instruments such as traveller's cheques, payment orders or are used to purchase expensive items for resale.

Money launderers often use banks and financial institutions in less regulated countries to deposit cash and then transfer it to banks in regulated environments as 'clean' funds

- **Smurfing**: This is a form of Placement where many small cash deposits are made instead of a single large one. Smurfing allows money launderers to evade local regulatory reporting requirements applicable to cash transactions. Cash based businesses are an obvious point of entry into the financial sector for illegal funds.

2. **Layering**: This is the separation of the proceeds of criminal activity from their source through the use of many financial transactions (layers). Layers may include multiple transfers of funds between financial institutions, early surrender of annuities without regard to penalties; cash collateralised loans, letters of credit with false invoices/bills of lading. The use of layers of financial transactions can disguise the origin of funds, disrupt any audit trail and provide anonymity. Money launderers seek to move funds around and change both the form of the funds and their location to make it harder for law enforcement authorities to identify 'dirty' money.

3. **Integration**: This is the final part of the money laundering process and involves integrating laundered money back into the financial system in such a way that it re-enters as apparently legitimate funds that can be retained over the long term.

- Criminal activities
  Criminal proceeds are not limited to cash but can also include other assets. Criminal activities associated with money laundering includes drug running and dealing, theft, robbery, bribery and corruption, fraud, abduction, extortion, and the evasion of tax.

- Terrorist financing
  There are a number of similarities between the movement of terrorist property and the laundering of criminal property and some terrorist groups are known to have well-established links with organised crime. However, there are two key differences between terrorist property and criminal property:
  - Often only small amounts are required to commit individual acts of terrorism. This increases the difficulty of tracking terrorist property

- Terrorist organisations can sometimes be funded from legitimate income such as charitable donations. It is difficult to identify the stage at which legitimate funds become terrorist property

Terrorist organisations usually require significant funding and large amounts of property to adequately resource their activities. Terrorist property and funds are often controlled via a number of sources and use modern techniques to manage funds and move them between jurisdictions without detection.

- Politically Exposed Persons
  Politically Exposed Persons (PEPs) are people who hold or have held (during the previous year) prominent public positions, either domestically or internationally. PEPs include:
  - Head of State or government
  - Senior politicians (e.g. Ministers and Deputy or Assistant Ministers)
  - Senior government, judicial or military officials
  - Senior executives of state-owned corporations or important political party officials
  - Members of Parliament
  - Members of Supreme Courts, of constitutional courts, or of other high-level judicial bodies
  - Members of courts of auditors or of the Boards of central banks
  - Ambassadors, chargé d'affaires and high-ranking officers in the armed forces
  - Members of the administrative, management or supervisory bodies of state-owned enterprises
  - The family members and close associates of PEPs should also be treated as PEPs

The involvement of PEPs or their close family members and associates should not automatically stop a transaction from going ahead. The involvement of a PEP in a transaction instead should be regarded as an orange light and trigger enhanced due diligence, including further checks and additional internal procedures to ensure their wealth has been legitimately generated.

Establishing whether individuals or legal entities should be regarded as a PEP or their close associate is not straightforward and can present difficulties. Search engines, both general and specific (subscription required) can often help identify potential PEPs, however close associates and family members can prove more difficult to identify.

If an employee or Partner suspects or holds information to suggest a customer or counterparty may be a PEP or involved with a PEP they should contact the Business Integrity (BI) Officer immediately. No transaction should be undertaken until the deal/investor sign off sheet has been approved by the BI Officer.

2. Why is combating money laundering so important for companies and investors?

There are significant reputational and commercial risks if investing alongside a person who is using a portfolio company to launder money. These include:

The true value of the company is likely to be uncertain as turnover and bank balances may be artificially inflated.
Should law enforcement authorities start to investigate the company it may be difficult to sell it, and assets can be frozen or seized.
The fund manager and its investors risk criticism and reputation damage for associating with or investing alongside criminals.

Most of the jurisdictions in which CDC and other funds invest as well as the major offshore centres where many fund administrators and fund managers are based, have well developed anti-money laundering laws. Money laundering is usually punishable by substantial prison time.

Similar to commercial operations, criminal and terrorist organisations require access to

working capital to function well. Any disruption to the flow of capital can damage their operations and thereby help to reduce crime including drug running, theft of national assets or resources and terrorist attacks.

3. Advice for Fund Managers

Fund managers should consider the following:

- Be wary of cash-based businesses, as these are an obvious point of entry into the financial sector for illegal funds. Fund managers should be conscious of this when conducting financial due diligence

- If unnecessary receipts and payments are revealed during financial due diligence these may be payments to a target company bank account from third parties made during the 'layering' part of the money laundering process

To design a robust anti-money laundering system a fund manager should consider the following features, and cover the points set out below in a compliance manual. Refer to CDC governance and business integrity checklist for questions to guide fund managers to assess money laundering risks linked to portfolio companies.

- Anti-money laundering policy
  There should be a clear statement that the fund and its employees will not engage in or tolerate money laundering in portfolio companies. The anti-money laundering (AML) policy should state that all employees are required to report any knowledge or suspicion of money laundering, and that employees will be protected from any adverse consequences for refusing to participate in a transaction where there is evidence of money laundering, even if it means the company loses business. The AML policy should also make clear that any breach will be considered an act of gross misconduct. Click here for an example AML policy.

  Fund managers should make a public statement of their AML policy.

- Appointment of a Money Laundering Reporting Officer/BI Officer
  Appointing a suitably senior Partner or Director to oversee a fund manager's AML systems and its management of money laundering risk helps demonstrate to investors

that the issue is being seriously addressed. It also shows staff that it is an important concern and is likely to result in a more controlled and ordered approach to money laundering risk. The duties of the officer are likely to include:

Establishing and maintaining policies and procedures: The Officer should establish and maintain specific policies, procedures and training to guard against the firm being used for the purposes of money laundering.

Providing a pre-investment sign off: The Officer should review all KYC material before an investment is made or sold or an investor admitted to a fund. The Officer should sign a checklist to confirm they are satisfied with the checks undertaken and that they indicate no evidence of money laundering.

Annual reporting: The Officer should report annually to the Partners detailing compliance with the money laundering rules. The report should review the operation of the firm's AML policies during the year and detail any reports made by staff during the year.

Staff training: The Officer should train or arrange training to ensure all staff understand the fund's AML system, how it works and their responsibilities under it.

Record keeping: The Officer should be responsible for ensuring that KYC files are kept for at least five years from the date when the relationship with the customer/investor ended.

Dealing with reports from staff: The Officer should be responsible for appropriately dealing with any reports by staff about money laundering risks and is responsible for reporting these (where appropriate) to relevant local law enforcement bodies and subsequent liaison if necessary.

- Compliance manual

  The AML policy and practices should be set out in the fund manager's compliance or other internal controls manual. The compliance manual should cover as a minimum, the points below and clearly define roles and responsibilities.

  The compliance manual should set out a process to ensure that before any obligation to invest has been entered into a fund manager has:

- Assessed the risk of investment being used to launder money at any of the three stages set out above. Or is funded either directly or indirectly by laundered money
- Identified the controllers (e.g. directors) and the major legal and the ultimate beneficial owners (UBOs) of the investment
- Obtained information from independent sources to confirm the identities of the controllers and the major legal and ultimate beneficial owners

See below for detailed guidance on who should be subject to KYC checks and the documents required. Note AML legislation differs for each jurisdiction and local legal advice must always be sought.

- Who are a fund manager's customers

  The term customer has a very wide definition under AML legislation and practice but it is commonly understood as meaning:
  - The investors in a fund
  - A target company and its existing management and shareholders
  - The purchaser of an investment and its management and shareholders

- When should KYC checks be completed

  As a matter of practical guidance, in the private equity industry identification evidence is usually obtained during:

  Fund raising: Before the admission of an investor into the fund.

  Investment and exit: When it is reasonably certain that the deal will complete but before the fund manager becomes legally obliged to complete an investment. Where there are subsequent changes to the Board of Directors, consideration should be given to the need to verify the identity of the new directors or shareholders before the changes takes place.

In relation to the co-investors: Where a fund is looking to include co-investors in a deal, checks should take place when it is reasonably certain that the transaction will complete but before the completion of the investment.

- Who should be subject to KYC checks
  Note: AML legislation around the world differs and local legal advice must always be sought.

  The following should be subject to KYC checks:

  Investors:

  - All individual investors in the fund who own, directly or indirectly, 15% or more of the fund
  - All institutional and corporate investors in the fund who own more than 15% of the fund and the UBOs of those institutions and corporations who hold more than 15% of the institution or corporation

  Vendors and target companies:

  - The target company itself
  - The owners and UBOs of the target company who individually directly or indirectly own 15% or more of the equity of that company
  - The directors of the target company (or their local equivalent) and any individuals with a significant managerial relationship with a target company
  - Any new management being introduced to the transaction

  Purchasers of fund's portfolio companies:

  - The purchaser vehicle
  - The directors of the purchaser (or their local equivalent) and any individuals with

a significant managerial relationship in the purchaser

- The owners of the purchaser and the UBOs who individually directly or indirectly own 15% or more of the equity of the purchaser

It is also worth keeping in mind that the person a fund manager is dealing with could be acting on behalf of an undisclosed principal.

- What should be obtained as part of the KYC checks
  The documents and checks required to identify and verify identity differ depending upon the nature of the person subject to the KYC check. Generally it is possible to identify all parties who are subject to a KYC check from the legal and financial due diligence reports prepared for a transaction, from corporate records such as registers and accounts and from company searches. When dealing with a corporate target, steps should be taken to fully understand the legal form, structure and ownership of the company. It is recommended that a structure chart is created to help in this process. It will then be necessary to verify those identities using independent sources.

  If a customer is unable or unwilling to supply the necessary information, the BI Officer should be informed before proceeding any further. This should not be discussed with the client as it can constitute 'tipping off' if the client is or could be involved in money laundering.

  Copies of the documents mentioned below should be dated showing when the copy was made and signed to confirm accuracy of the copy. That signatory should add their name, firm name, address, profession and if appropriate their registration number with the relevant local professional body.

  Provided that they have compared the original and a copy then a document may be certified by: (i) an executive of the fund manager; and/or (ii) an independent lawyer, accountant or notary public.

  The information that should be obtained is set out below. Further guidance on the KYC process can be found in the UK's JMLSG Guidance Notes which provide international standard insights.

  Information to be obtained:

For an individual: The following should generally be obtained to verify the identity of an individual. A certified photocopy of:

- Their original passport or other government-issued document with a picture of the individual – e.g. a driving licence or identity card
- If the above does not contain the usual residential address of the individual, a recent utility bill or bank statement (less than three months old) showing both name and address is required. The names and addresses should match what is known of the individual

Copies should be clearly legible as law enforcement authorities may use them to confirm address and visually identify a person.

For a corporate entity: A certified photocopy of:

- The certificate of incorporation
- The memorandum and articles of association or the local equivalents
- The directors and shareholder registers or the local equivalents

If there is a reputable local company register available to the public then a company search may provide this information. Legal due diligence will confirm its accuracy.

For a trust: A certified photocopy of:

- The trust deed
- The identity of the individual or corporate trustees, beneficiaries and any controllers or protectors of the trust should be verified

For Partnerships and other non-corporate entities: A certified photocopy of:

- The partnership or other constitutional document

- The identity of any partner or similar local equivalent owning or controlling more than 15% of the vehicle should be verified

For public sector bodies and state owned companies: A certified photocopy of:

- The certificate of incorporation
- The memorandum and articles of association or the local equivalents (e.g. the local law establishing the company)
- The directors and shareholders registers

If there is a reputable local company register with information available to the public then a company search may provide this information. Legal due diligence will confirm its accuracy.

For sovereign wealth funds and development finance institutions (DFIs):

The nature of the sovereign wealth fund or DFI will have been ascertained at the 'Identify' stage of the KYC process. A risk based approach to verifying the identity of such bodies can be taken and in some cases (e.g. in the case of CDC, CalPERS or CPPIB it may not be necessary to do more than confirm that the fund manager is dealing with the wealth fund or DFI).

- Transaction sign-off process
  To ensure that a disciplined approach to the KYC process is followed fund managers should adopt a *pro-forma*checklist/sign off form. The form should detail the checks to be undertaken on the various parties to a transaction and the results of those checks before an investor is admitted. It should require sign off by the BI Officer and the deal leader before the fund manager becomes committed or an investor admitted to a transaction. Where a transaction involves a PEP further sign off by a senior member of management who is not connected with the transaction should be required.

  Prior to signing a KYC checklist/form, the BI Officer should be satisfied that the following issues have been addressed:

- What is the risk that the transaction could be part of a money laundering scheme?
- What is the risk that a participant in the transaction could be engaging in money laundering?
- Are there any factors in the transaction which lead me to suspect money laundering is taking place?
- Have we identified all parties we should undertake KYC checks on?
- Have we obtained KYC materials on those people and confirmed their identity and residence?
- Was this information obtained from reliable independent sources?
- Are the results of other due diligence exercises – e.g. the legal and financial due diligence consistent with the results of the KYC checks undertaken?
- Is there a risk that the people the fund manager is dealing with are acting on behalf of an undisclosed investor?
- Should we have done more?

- Investment monitoring

  Fund managers should regularly review and update KYC materials during the course of investments to ensure they remain up to date and should ensure that the appropriate due diligence is performed on any new shareholders, directors or other controllers. The BI Officer should periodically confirm that individual files can be recovered from storage.

  Investments are typically subject to regular performance reviews and valuations. It is good practice to include a short AML commentary in investment review papers. Consideration should be given to periodically reviewing the nature and scope of the portfolio company's business to confirm that new KYC risks have not arisen.

- Annual governance and business integrity reporting
  Each year the BI Officer should provide the fund's Board of Directors with a written review of the impact, adequacy and application of the fund's AML policy and procedures. This should be contained in an annual report and provide senior management with a balanced understanding of:
    - The obligations that the fund must meet
    - The operation and effectiveness of the systems and controls that the fund manager has in place to meet those obligations, how they reduce the risk that it will be used to further
    - financial crime and/or money laundering and how they could be improved
    - Any important developments in AML practice or law and recommending any necessary updates to take account of these
    - Assess how changes in the fund manager's structure or business plan have been or will be incorporated into the AML management system
    - The monitoring that has been undertaken during the year
    - Any suspicious transactions during the year and what was done about them
    - The training delivered during the year
    - Suspicious transactions notified to local law enforcement authorities
    - An assessment of the types of AML risks faced by the firm
    - How any international best practice publications have been used

  These reviews help a fund manager demonstrate to law enforcement authorities and investors that the firm takes its responsibilities seriously. The report should also be provided to the fund's Investment Committee.

- Suspicious transactions reporting
  Employees of the fund manager should be required to report to the firm's BI Officer

any suspicion of money laundering. The BI Officer should then take local professional advice on what, if any, further action needs to be taken.

The types of transactions used to launder money are almost unlimited and it is therefore difficult to define a suspicious transaction. Suspicious transactions are most likely to be transactions that are inconsistent with a customer's known business or circumstances. Examples of what might constitute suspicious transactions are set out below. These are not meant to be exhaustive but are intended to highlight transactions and situations which may merit further examination:

- Counterparties with complicated corporate structures including offshore jurisdictions – particularly if the need for the structure is not easily understood or its design is driven by secrecy
- Customers for whom verification of identity proves difficult and who are reluctant to provide details
- Customers who wish to use cheques drawn on an account other than their own or to have funds due to them paid into an account that is not their own
- Changes in settlement details at the last moment without satisfactory explanation
- Requests to transfer investments to apparently unrelated third parties
- Customers whose investment and lifestyle appear to be unrelated to their occupation

Where a disclosure is made before a transaction has occurred, the transaction should be halted pending the BI Officer's consent to its proceeding.

- Record keeping
  Proper records of such checks must be kept – local law enforcement authorities may need them to help identify, arrest and prosecute offenders.

- Training
  AML training should be given to all staff to illustrate the importance of AML systems

to the firm, its senior management and investors. Training should ensure that staff are able to identify transactions which carry a risk of money laundering, including which indicators to look out for. Training should also make staff aware of their responsibilities under AML rules.

Training is likely to involve initial education such as an introductory awareness course, which is followed up by updates and refresher courses. It may be given via a computer-based scheme, at a 'team' meeting or by an external professional brought in for the purpose.

- Working with lawyers, accountants and fund administrators
  Some fund managers find it helpful to ask the lawyers or accountants engaged on a transaction to collect the relevant KYC documents and certify them as necessary before providing them in a 'KYC Bundle'. While this is very helpful, ultimately the BI Officer and the deal leader at the fund manager remain responsible for the accuracy and completeness of the checks and the documents.

  Funds that use the 'onshore advisor offshore manager' model need to consider what KYC obligations may arise and liaise with the relevant administrator to ensure that the KYC process is integrated, comprehensive and effective.

See Fund BI management system for guidance on the anti-corruption systems that fund managers should have in place themselves and Investment cycle for guidance on where anti-money laundering should fit into the fund's investment process.

4. Further resources

- Further information and guidance
  - CDC – How we do it – Business Integrity
  - JMLSG Guidance Notes
  - Financial Action Task Force Recommendations
  - Basel Committee – Sound Management of Risks Related to Money Laundering and Financing of Terrorism

- Wolfsberg Group
- European Union Third Money Laundering Directive
- US SEC AML Source Tool
- Financial Action Task Force Guidance on Politically Exposed Persons