LAW SOCIETY OF KENYA

AML / CFT / CPF COMPLIANCE
FREQUENTLY ASKED QUESTIONS FOR LAW FIRMS

This document sets out common compliance questions that law firms encounter in meeting their Anti-Money Laundering (AML), Countering the Financing of Terrorism (CFT) and Countering Proliferation Financing (CPF) obligations under Kenyan law. It is intended as a practical reference guide and does not constitute legal advice.

GENERAL UNDERSTANDING

Q1. Does AML/CFT/CPF apply to my law firm?

Yes, if your firm provides any of the following services: managing client money or assets; buying and selling real property on behalf of clients; managing of client money, securities or other assets; management of bank, savings or securities accounts; organisation of contributions for the creation, operation or management of companies; acting as a nominee director or shareholder; creation, operation or management of buying and selling of business entities or legal arrangements; or providing trust services. See Section 48 of the Proceeds of Crime and Anti-Money Laundering Act, 2009 (POCAMLA). Most general practice firms will fall within scope on at least one of these activities.

Q2. What is the difference between AML, CFT and CPF?

AML targets the concealment of proceeds of crime. CFT targets the financing of terrorist activities - which may involve clean money not just criminal proceeds. CPF targets the financing of the proliferation of weapons of mass destruction, largely through sanctions compliance. All three share common controls but have distinct reporting obligations and risk indicators.

Q3. Which laws govern these obligations in Kenya?

The overall legislation governing AML/CFT/CPF in Kenya is the Proceeds of Crime and Anti-Money Laundering Act (POCAMLA) 2009 together with the Proceeds of Crime and Anti-Money Laundering Regulations 2013. Other relevant laws include the Prevention of Terrorism Act 2012, The Prevention of Terrorism (Implementation of The United Nations Security Council Resolutions on Prevention, Suppression and Disruption of Proliferation Financing) Regulations and The Prevention of Terrorism (Implementation of The United Nations Security Council Resolutions On Suppression Of Terrorism) Regulations, 2024.

The Law Society of Kenya Guidelines for the Kenya Legal Profession on Anti-Money Laundering, Countering the Financing of Terrorism and Proliferation Financing provide sector-specific guidance.

The Financial Reporting Centre (FRC) is the overall regulatory and supervisory body for reporting institutions.

The Law Society of Kenya serves as the primary regulator of the legal profession, having been designated as a Self-Regulatory Body (SRB) pursuant to Section 36A of the POCAMLA and Section 4A of the LSK Act.

Q4. What is a DNFBP and why does it matter?

A Designated Non-Financial Business or Profession is a category established by FATF for sectors outside banking that are nevertheless vulnerable to financial crime. Law firms fall within this category. Being a DNFBP means you have many of the same legal obligations as a bank/financial institutions, just calibrated to your professional context. See **Section 2** of the POCAMLA.

Q5. Can a sole practitioner be held liable for AML/CFT failures?

Yes. The obligations apply to all advocates in private practice regardless of firm size. A sole practitioner must still conduct CDD, maintain records, file STRs and have a written AML/CFT/CPF policy. The FRC and LSK can investigate and sanction individual practitioners.

CUSTOMER DUE DILIGENCE (CDD)

Q6. When must we conduct CDD on a client?

Client Due Diligence (CDD) is a continuous obligation and must be undertaken throughout the course of a client relationship. It should be conducted when establishing a new client relationship and reviewed or updated whenever an occasional transaction is undertaken or when continuing to act for an existing client. CDD is not a one-time exercise but an ongoing process aimed at ensuring that client information remains accurate and up to date. Section 45 of POCAMLA and Regulations 14 - 19 of the Proceeds of Crime and Anti-Money Laundering Regulations, 2023 (POCAMLR).

Q7. What does CDD involve for an individual client?

At minimum: full legal name; national ID or passport number and a copy of the document; PIN certificate; physical and postal address; source of funds for the matter; and the purpose of the transaction. You should also screen the client against sanctions lists and PEP databases. See Section 45(1A) (a) of the POCAMLA and Regulation 15 of the POCAMLR.

Q8. What does CDD involve for a corporate client?

For a company you must verify: the company name and registration number; the Certificate of Incorporation and CR12 (or equivalent); the registered address; the nature of the business; the identity of directors; and crucially, the identity of all Ultimate Beneficial Owners (UBOs) — meaning any individual who ultimately owns or controls more than 10% of the entity. You should also screen the directors and beneficial owners against sanctions lists and PEP databases. See Section 45(1A) (B) of the POCAMLA and Regulation 16 of the POCAMLR.

Q9. When conducting Customer Due Diligence (CDD), who bears the cost?

The cost of conducting Customer Due Diligence is generally borne by the advocate or law firm as part of its compliance obligations under the AML/CFT/CPF framework. However, firms may factor compliance-related expenses into their overall legal fees or charge clients for specific disbursements where permitted by the engagement terms. Regardless of who ultimately bears the cost, advocates remain responsible for ensuring that appropriate CDD measures are conducted before and during the business relationship.

Q10. What is a UBO and why does it matter?

An Ultimate Beneficial Owner is the natural person who ultimately owns or controls a legal entity, either through direct shareholding, indirect control or other means such as nominee arrangements. Identifying UBOs is critical because money launderers commonly use layers of corporate structures to obscure the true owner. Under Kenyan law and FATF standards, you cannot simply accept a company as your client without looking through to the human beings behind it. See the definitions section of the POCAMLR.

Q11. What is Enhanced Due Diligence (EDD) and when does it apply?

EDD is a higher level of scrutiny applied to higher-risk clients or transactions. It typically involves obtaining additional documentation on source of wealth, senior management approval before onboarding, more frequent monitoring and deeper scrutiny of documents supplied. EDD is is applied when dealing with: Politically Exposed Persons and their family members and close associates; clients from high-risk jurisdictions identified by FATF; complex or unusually large transactions; and any situation where standard CDD cannot be satisfactorily completed. See Regulation 20 POCAMLR.

Q12. What is a Politically Exposed Person (PEP)?

A PEP is an individual who holds or has held a prominent public function; such as a head of state, senior government official, judge, senior military officer, or senior executive of a state-owned enterprise. Their immediate family members and known close associates are also treated the same was as PEPs. PEPs present higher corruption and bribery risk. See Regulation 26(5) of the POCAMLR.

Q13. Can we rely on CDD done by another lawyer or bank?

Yes, in limited circumstances. reliance on third parties who are themselves subject to equivalent AML/CFT obligations is allowed, but you remain ultimately responsible for the adequacy of the CDD. You must obtain written confirmation that the third party holds the CDD materials and will make them available on request, and you must satisfy yourself that the third party's regime is adequate.

Q14. What is Simplified Due Diligence (SDD) and when can we apply it?

SDD allows reduced CDD measures for clients assessed as low risk, for example, listed public companies, government entities, or regulated financial institutions. However, SDD does not mean no CDD; it means fewer documents and less frequent review. You cannot apply SDD if there is any suspicion of financial crime. See Regulation 21 of POCAMLR,

Q15. When should we decline to act or terminate a retainer?

You must decline to act where you cannot complete satisfactory CDD, where a client refuses to provide identification, where a client is a sanctioned person or entity, or where proceeding would involve you in a transaction you suspect to be connected to money laundering or terrorism financing. Where you terminate a retainer on these grounds, you must be careful not to 'tip off' the client that an STR has been or may be filed.

RISK ASSESSMENT

Q16. What is a firm-wide risk assessment and do we need one?

Yes, every firm must prepare and maintain a written risk assessment that identifies and evaluates the money laundering, terrorism financing and proliferation financing risks the firm faces given its client base, practice areas, geographic exposure, and delivery channels. This is the foundation of your compliance programme. The LSK & FRC may request to see the firm’s risk assessment report during an inspection. The obligation to conduct a risk assessment is housed under Regulation 7 of the POCAMLR.

Q17. When should we update our risk assessment?

The firm’s risk assessment report must be updated whenever there is a material change in your practice, for example adding a new practice area, taking on clients from a high-risk jurisdiction, or following a new FATF or FRC guidance publication.

Q18. What are the red flags we should be alert to in our practice?

Common red flags in legal practice include: clients who are reluctant to provide identification or explain the source of funds; clients who offer or insist on paying in cash; transactions with no apparent commercial rationale; unusual urgency without explanation; third parties paying fees on behalf of the client; clients who are indifferent to costs or outcomes; property transactions significantly above or below market value; and instructions involving multiple jurisdictions with no obvious business reason. A suspicion does not equate certainty of crime. See further details on suspicious indicators here.

REPORTING OBLIGATIONS

Q19. What is a Suspicious Transaction Report (STR) and when must we file one?

An STR is a report filed with the LSK/FRC when you know, suspect or have reasonable grounds to suspect that a transaction or proposed transaction is connected to money laundering or terrorism financing. The threshold is suspicion, not certainty, if something feels wrong, you must file. The standard of suspicion is that of a reasonable advocate. The obligation to file arises as soon as suspicion forms, not after you have investigated and confirmed it. See Section 44(2) of the POCAMLA.

Q20. What is the standard of suspicion for filing a Suspicious Transaction Report (STR)?

The standard for filing an STR is **reasonable suspicion, not proof**. An advocate does not need to confirm that a crime has occurred. An STR should be filed where there are reasonable grounds to suspect that a transaction, attempted transaction, or funds may be linked to money laundering, terrorism financing, proliferation financing, or other criminal activity. The advocate's role is to report the suspicion, not to investigate or prove the offence.

Q21. What are some of the red flags to look out for (indicators)?

Red flags are warning signs that may indicate potential money laundering, terrorism financing, or other illicit activity. Examples include clients who are unwilling to provide identification information, cannot explain the source of funds, request unusual secrecy, use complex transaction structures without a clear purpose or engage in transactions that are inconsistent with their known profile. Where such indicators are present, advocates should conduct further checks and consider whether an STR is warranted.

Q22. Do I need to report a transaction even when the advocate does not handle any funds?

Yes. The obligation to submit a Suspicious Transaction Report (STR) is not dependent on whether an advocate handles, receives or transfers funds on behalf of a client. If, in the course of providing legal services, an advocate knows, suspects or has reasonable grounds to suspect that a transaction, attempted transaction or activity may be linked to money laundering, terrorism financing, proliferation financing, or the proceeds of crime, an STR should be submitted to the appropriate authority.

Q23. Where and how do we file an STR?

The Law Society of Kenya (LSK) is currently developing an AML module within its ERP System that is intended to serve as a platform through which advocates will be able to submit Suspicious Transaction Reports (STRs), Suspicious Activity Reports (SARs), and Cash Transaction Reports (CTRs). The module has not yet been launched, as it remains under development and is undergoing the necessary design and implementation processes before being made available for use.

Until the Society formally communicates a change in the reporting arrangements, advocates should continue submitting any required Suspicious Transaction Reports and Suspicious Activity Reports through the existing prescribed FRC reporting channels.

Q24. What is the tipping off prohibition?

It is a criminal offence under POCAMLA to disclose to a client or any other person that an STR has been filed or that they are under investigation. This means once you have filed or decided to file an STR, you cannot inform the client that you have done so, and you must not take any action that would alert them. You may need to continue acting normally, or find a legitimate reason to withdraw, without revealing your true reason. See Section 8 POCAMLA.

Q25. Are we protected if we file an STR in good faith?

Yes. POCAMLA provides statutory protection to any person who makes a disclosure in good faith. You will not be liable for breach of confidentiality, contract, or any other civil claim arising from an STR filed genuinely. However this protection does not extend to fabricated or malicious reports (Section 10 of the POCAMLA).

Q26. Is there an obligation to report even if we do not proceed with the transaction?

Yes. The obligation to report arises when suspicion forms, regardless of whether the transaction proceeds. If a client instructs you and then withdraws before completion, but you formed a suspicion during the instruction, you are still required to file a Suspicious Activity Report.

RECORD KEEPING

Q27. What records must we keep and for how long?

You must retain CDD documents, transaction records, correspondence and internal reports for a minimum of seven (7) years from the date of the transaction. Records should be stored in a manner that allows them to be retrieved promptly if requested by the FRC or law enforcement. See Section 46 of the POCAMLA.

Q28. Can records be kept electronically?

Yes, electronic records are acceptable provided they are stored securely, cannot be altered without detection and can be produced in a legible format when required. You should have a clear document retention and destruction policy.

INTERNAL CONTROLS AND GOVERNANCE

Q29. Do we need to appoint a Money Laundering Reporting Officer (MLRO) and if yes, what are some of their functions?

Yes. Every firm must designate a senior person as the MLRO. In a law firm this is typically a partner or senior advocate. The MLRO receives internal suspicion reports from staff, decides whether to escalate them to the LSK/FRC, maintains the compliance programme and is the firm's primary point of contact with the LSK. See Regulation 12 of POCAMLR.

The MLRO's responsibilities include:

- ✓ Receiving and reviewing internal suspicious activity reports from staff;
- ✓ Determining whether to file an STR with the LSK/FRC;
- ✓ Maintaining AML/CFT/CPF policies, procedures, and controls;
- ✓ Overseeing staff AML training programmes;
- ✓ Acting as the firm's point of contact with the LSK;
- ✓ Keeping records of all STRs filed and the basis for filing or declining to file; and
- ✓ Conducting or commissioning periodic AML risk assessments.

Q30. What training are we required to provide to staff?

All fee earners and relevant support staff must receive AML/CFT training. Training must cover how to identify suspicious activity, how to report internally to the MLRO, the tipping off prohibition, and the firm's own policies and procedures. Training must be documented and refreshed regularly, at least annually and whenever there are significant regulatory changes.

Q31. What should our AML/CFT policy cover?

At minimum: the firm's risk appetite and risk assessment methodology; CDD procedures for different client types; EDD triggers and procedures; the STR filing process; the role and responsibilities of the MLRO; record keeping procedures; staff training requirements; and sanctions screening procedures. See Regulation 28(a) of POCAMLR.

SANCTIONS AND PROLIFERATION FINANCING

Q32. What are our sanctions screening obligations?

Before accepting any new client and before executing any transaction, you must screen the client and all relevant parties (counterparties, beneficial owners, third-party payors) against: the UN Security Council consolidated sanctions list; Kenya's national sanctions designations. See Regulation 12(2) of the The Prevention of Terrorism (Implementation of The United Nations Security Council Resolutions on Prevention, Suppression and Disruption of Proliferation Financing) Regulations.

Q33. What do we do if a client matches a sanctions list?

You must immediately freeze any assets you hold for that person, refuse to proceed with the transaction and report to the LSK/FRC.

Q34. What is proliferation financing and how does it differ from terrorism financing?

Terrorism financing funds terrorist acts or organisations. Proliferation financing specifically funds the development, acquisition, manufacture, possession or transfer of nuclear, chemical, biological, or radiological weapons.

PENALTIES AND ENFORCEMENT

Q35. What are the consequences of non-compliance?

Under POCAMLA, penalties for non-compliance range from substantial fines to criminal prosecution of individuals. The FRC can issue administrative sanctions, direct compliance measures, and refer matters to the Director of Public Prosecutions. The LSK can impose disciplinary sanctions separately (Section 4A (2)(c) LSK Act).

Q36. Has the LSK or FRC actually inspected law firms in Kenya?

Yes. The LSK has been conducting inspections, both onsite and offsite, in order to assess the compliance of law firms with AML/CFT/CPF laws and regulations. The exercise is normally conducted in conjunction with FRC. The inspection exercise is mandatory and not optional for firms.

The inspection does not imply any suspicion of misconduct, wrongdoing, or non-compliance on the part of the firm. It is a routine supervisory exercise undertaken by the Law Society of Kenya as part of its mandate to monitor and assess compliance with applicable AML/CFT/CPF obligations and may be conducted on any law firm within its supervisory scope.

DATA PRIVACY, CONFIDENTIALITY AND PRIVILEGED INFORMATION

Q37. How does the duty of confidentiality interact with AML reporting obligations?

AML reporting obligations under POCAMLA 2009 override the general duty of confidentiality owed to clients. A law firm is not in breach of client confidentiality by filing an STR or disclosing information to the FRC/LSK. See Section 17 of the POCAMLA.

Q38. Does legal professional privilege exempt a law firm from filing an STR?

Yes. Professional Privilege is a qualified exemption. Information received in the course of seeking legal advice or in contemplation of litigation may be privileged. However, privilege does not apply where the legal advice itself is sought to facilitate crime or fraud. See Section 18 POCAMLA.

Q39. Will the LSK or FRC share my firm's information, or my clients' information with KRA or other government agencies?

No. Information acquired during inspections, both onsite and offsite, or during a risk assessment exercise, is confidential and shall only be used for purposes of assessing compliance. Such information shall not be shared with KRA.

Q40. In the event I file a report, will FRC inform my Client that I have made such a report?

No. Information submitted to the Financial Reporting Centre, including Suspicious Transaction Reports (STRs), is protected by strict confidentiality requirements. FRC officers are prohibited from disclosing the existence, contents or source of an STR except as authorized by law. The FRC does not notify clients that an STR has been filed against them. Any dissemination of information by the FRC is limited to competent authorities and only for lawful purposes related to intelligence analysis, investigation, prosecution or other functions permitted under the law. Accordingly, clients are not informed by FRC staff that a report has been submitted concerning them.

FRC members of staff are required by law to take an oath of confidentiality and any sharing of information is a breach of the statutory requirement of confidentiality. See Section 32 of the POCAMLA.

For further guidance, contact the Financial Reporting Centre (FRC) at **www.frc.go.ke** or the Law Society of Kenya at **www.lsk.or.ke**