



**FRC
KENYA**

December 2025

GUIDANCE NOTES ON

**Suspicious Transaction and
Activity Reporting for Lawyers,
Notaries and other Independent
Legal Professionals in Kenya.**

Financial Reporting Centre
Old Mutual Tower 13th Floor
Upper Hill.
P.O. Box Private Bag - 00200,
Nairobi, Kenya
Email: info@frc.go.ke
Phone: + 2547098580005
<https://www.frc.go.ke>



DISCLAIMER

These Guidelines are intended to assist Lawyers, notaries, and other independent legal professionals in Kenya to understand and comply with their anti-money laundering, counter-financing of terrorism, and counter-proliferation financing (AML/CFT/CPF) obligations as set out in the following acts and regulations;

- The Proceeds of Crime and Anti-Money Laundering Act (POCAMLA), 2009;
- Law Society of Kenya Act, CAP. 18
- Prevention of Terrorism Act (POTA), 2012
- The Proceeds of Crime And Anti-Money Laundering Regulations, 2023;
- The Prevention of Terrorism (Implementation of The United Nations Security Council Resolutions On Suppression Of Terrorism) Regulations, 2024;
- The Prevention of Terrorism (Implementation of The United Nations Security Council Resolutions on Prevention, Suppression and Disruption of Proliferation Financing) Regulations, 2023

This guidance is a general, informative document and is not intended to replace any of the above-mentioned AML/CFT/CPF Acts and Regulations. This Guidance should not be construed as legal advice and should be read together with the said laws. The legal and regulatory framework governing anti-money laundering, combating the financing of terrorism, and countering proliferation financing is dynamic and subject to frequent amendment. Legal practitioners should therefore rely on the current laws, regulations, and directives issued by the Financial Reporting Centre (FRC), the Law Society of Kenya (LSK), and any other competent authority.

Table of Contents

DISCLAIMER	i
Table of Contents	ii
Table of Acronyms /Abbreviations	iv
1. INTRODUCTION	1
2. MONEY LAUNDERING, TERRORISM FINANCING AND PROLIFERATION FINANCING ...	3
2.1 Money Laundering	3
2.1.1 Stages of Money Laundering	3
2.2 Terrorism Financing	5
2.3 Proliferation Financing	6
3. SUSPICIOUS TRANSACTION/ACTIVITY REPORTING	7
3.1 Obligation to report (Section 44 of POCAMLA and Regulation 38 of POCAMLA-Regulations, 2023).....	7
3.2 What constitutes a suspicious reportable activity?	7
4. DETECTING AND IDENTIFYING SUSPICION	9
5. ML/TF INDICATORS FOR LEGAL PROFESSION	10
5.1 Red flags about the client.....	10
5.2 Red flags relating to clients' funds	11
5.3 Red flags relating to the client's choice of lawyer.....	13
5.2 Red flags on the nature of retainer	13
5.4 Red flags on the transactional patterns	13
6. FILING A SUSPICIOUS REPORT	14
6.1 Internal process for reporting suspicion to the Money Laundering Reporting Officer (MLRO)	14
6.2 When to file a suspicious report	15
6.3.1 Profiling of your Client.....	15
6.3.2 Details of suspicious transactions or activity:	15
6.4 Suspicious report submission process	16
6.5 Post-Reporting Obligations	16
6.6 Decision not submit a suspicious report	17
7. Protection of Information and Informers, Tipping-off and other Offences	17
7.1 Protection of Information and Informers.....	17
7.2 Tipping-off.....	17

7.3 Offences and Penalties.....	17
8. CASE STUDIES	19
8.1 Misuse of Client Accounts	19
8.2 Potential misuse of Legal Firms by PEPs	20
8.3 Legal professional sets up multiple international company structures	20
8.4 Potential abuse of power of attorney	21
9. Links to FATF guidance notes for Legal Professionals.....	22

Table of Acronyms /Abbreviations

POCAMLA	The Proceeds of Crime and Anti-Money Laundering Act
LSK	Law Society of Kenya
POTA	Prevention of Terrorism Act
POCAML-Regulations	The Proceeds of Crime and Anti-Money Laundering Regulations
FRC	Financial Reporting Centre (FRC),
ML	Money laundering
TF	Terrorism Financing
PF	Proliferation Financing
AML	Anti-money laundering
CFT	Counter-financing of Terrorism
CPF	counter Proliferation financing
DNFBPs	Designated Non-Financial Businesses and Professions
PEP	Politically exposed person (PEP)
MLRO	Money Laundering Reporting Officer (MLRO)

1. INTRODUCTION

Money laundering, terrorism financing and, proliferation financing present major threats to Kenya's financial system, national security, and the integrity of professional services. Because these crimes increasingly involve cross-border transactions and the misuse of legitimate professional services, all sectors—particularly the legal profession—must implement strong measures to safeguard against abuse.

Kenya's Anti-money laundering and counter-financing of terrorism (AML/CFT) framework is anchored in POCAMLA, POTA, and their subsequent regulations. These laws, together with FRC guidelines, provide mechanisms for detecting, preventing, and disrupting money laundering, terrorism financing, and proliferation financing.

In Kenya, Lawyers, notaries, and other independent legal professionals are classified as Designated Non-Financial Businesses and Professions (DNFBPs) under Section 2 of POCAMLA. The AML/CFT/CPF framework applies to Lawyers, notaries, and other independent legal professionals who undertake activities listed under Section 48 of POCAMLA on behalf of their clients. These activities may be exploited by criminals to conceal the origin, movement, or ownership of illicit funds, and they include:

- ✓ **Buying and selling of real estate;** The activity of buying and selling of real estate applies to both residential and commercial purchase, sale, lease, and mortgage transactions, and transactions that finance a purchase or sale of real estate.
- ✓ **Managing of client money, securities, or other assets;** It involves handling the clients' funds where legal practitioner controls the use, application or disposition of funds or has a signatory authority over the client's financial account.
- ✓ **Management of bank, savings, or securities accounts;**
- ✓ **Organization of contributions for the creation, operation, or management of companies;** this involves legal practitioners preparing for or carrying out a transaction where investors contribute capital to a legal entity and would conceivably cover financing and refinancing transactions.

- ✓ **Creation, operation, or management of buying and selling of business entities or legal arrangements;** are activities involving setting up, running, or controlling companies, trusts, partnerships, and similar structures
- ✓ Acting as a formation agent of legal persons;
- ✓ Acting as, or arranging for another person to act as, a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- ✓ Providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- ✓ Acting as, or arranging for another person to act as, trustee of an express trust;
- ✓ Acting as or arranging for another person to act as a nominee shareholder for another person

However, they are not required to report suspicious transactions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.

Lawyers, notaries, and other independent legal professionals have an obligation to apply the preventative measures outlined in POCAMLA, POTA, and subsequent regulations. Section 44 of POCAMLA and Regulation 38 of POCAML-Regulations, 2023 require Lawyers, notaries, and other independent legal professionals to file suspicious reports to the Centre. This guidance will offer sector-specific guidelines for lawyers, notaries, and other independent legal professionals to understand their legal obligations under the AML/CFT/CPF legal framework; Identify suspicious transactions and red flags specific to the legal profession, and report suspicious transactions and activities to the Centre.

2. MONEY LAUNDERING, TERRORISM FINANCING AND PROLIFERATION FINANCING

2.1 Money Laundering

Money laundering is the process through which criminals conceal or disguise the illicit origin of property or funds arising from criminal activity, and introduce them into the formal economy as if they were legitimate.

According to Section 3 and 4 of POCAMLA, Money laundering occurs when a person knows (or should reasonably know) that property comes from criminal activity and then **handles it in any way that helps hide its illegal origin**. This includes entering into agreements or transactions involving the property, or performing any act that:

- Conceals or disguises the nature, source, location, movement, or ownership of the property,
- Helps someone avoid prosecution for a crime, or
- Reduces or removes property gained from criminal activity.

Further, any person who **acquires, uses, or possess** property while knowing (or having reason to know) that it is the proceeds of crime, commits an offence.

2.1.1 Stages of Money Laundering

Money laundering commonly occurs in three stages:

(a) Placement

This initial stage involves introducing criminally tainted money into the financial system.

Examples include;

- Depositing large amounts of cash into bank accounts;
- Splitting large transactions (“smurfing”) into smaller deposits;
- Use of Client/Trust Accounts to receive illicit funds

- Facilitation of Real Estate Transactions with illicit funds
- Setting up complex corporate structures, shell Companies, and trusts in offshore jurisdictions with weak Anti-Money Laundering (AML) controls

(b) Layering

A complex series of transactions is used to obscure the audit trail and distance the funds from their criminal origin. Examples include:

- Creating complex corporate structures, shell companies, trusts, and offshore entities with hidden beneficial owners
- Facilitating large financial transactions using trust accounts to move money through various domestic and international bank accounts.
- Investing in high-value legitimate assets such as real estate, luxury goods or securities on behalf of clients.

(c) Integration

Laundered funds re-enter the legitimate economy, appearing clean and usable. Examples include:

- Facilitating the purchase of high-value assets like land, real estate, luxury goods and Securities.
- Facilitating acquisition of legitimate business Investments and acquisitions
- Repatriating funds as “legitimate” income or loans.

According to the updated [National Money Laundering Risk Assessment Report of 2023](#), the ML threat in the legal profession was assessed as medium high while the vulnerability was rated high. Lawyers frequently handle transactions associated with: purchase, sale, leasing and financing of real state; operation of client accounts; trust and company services; advisory services; administration of estates and trusts; citizenship and immigration services;

escrow and notary services, that can be exploited during placement, layering and integration stages.

2.2 Terrorism Financing

Terrorism financing is the act of **providing funds or financial support**, directly or indirectly, to an individual, group, or Organisation for the purpose of: committing, planning, or facilitating terrorist acts, or supporting terrorist operations or networks.

Under **POTA**, Terrorism financing involves **collecting, providing, possessing, or dealing with money, property, weapons, or services**—directly or indirectly—with the intention, knowledge, or reasonable belief that they will support terrorist acts, terrorist groups, or individuals involved in terrorism.

It includes:

- Funding, providing, or facilitating **property, funds, services, or travel** for planning, preparing, or carrying out terrorist acts or for terrorist training;
- **Supporting or soliciting support** for terrorist groups, including providing logistical help such as travel documents, shelter, communication devices, or other assistance;
- **Dealing in, transferring, concealing, or controlling** property owned or used by terrorist groups;
- Possessing property or weapons **intended for use in terrorism**;
- Offering or providing **weapons** to terrorist groups or individuals for terrorist purposes; and
- **Harboring, directing, or assisting** persons who commit or intend to commit terrorist acts.

Lawyers may be unknowingly used to:

- Set up non-profit organizations or corporate structures used to transfer funds;
- Facilitate real estate or asset purchases used to store value;

- Manage trust accounts used for movement of funds;
- Conduct cross-border transactions that hide beneficiaries.

2.3 Proliferation Financing

Proliferation financing involves the provision of funds, services, or economic resources used for the development, acquisition, manufacture, transfer, or transportation of **weapons of mass destruction (WMDs)** or related materials.

Proliferation financing often relies on complex corporate structures, front companies and intermediaries, international trade transactions, falsified shipping documents, and movement of dual-use goods (items with legitimate and military application).

The legal sector may be exploited to establish companies or execute transactions that obscure the identity of sanctioned individuals or entities.

3.SUSPICIOUS TRANSACTION/ACTIVITY REPORTING

3.1 Obligation to report (Section 44 of POCAMLA and Regulation 38 of POCAMLA-Regulations, 2023)

Lawyers, notaries and other independent legal professionals must notify the Centre within two days upon forming suspicion on activities or transactions that may suggest money laundering, terrorism financing, or proliferation financing. They are required to provide enough information to explain the nature and basis of their suspicion and must include any supporting documents they possess.

Lawyers, notaries and other independent legal professionals must conduct ongoing monitoring of all complex, unusual, large, suspicious transactions or such other transactions as may be specified by the regulations —whether completed or attempted—and pay close attention to patterns with no clear economic or lawful purpose.

When a transaction or activity appears suspicious or potentially linked to money laundering, terrorism financing, proliferation financing, or the proceeds of crime, the institution must report it to the Centre within two days after forming the basis of suspicion. All attempted suspicious transactions must also be reported except in scenarios where the information is protected by legal professional privilege.

3.2 What constitutes a suspicious reportable activity?

- **Unusual Activity or Transaction** - Unusual activity or an unusual transaction can be any activity or transaction that deviates from the profile provided while on boarding the client. It should prompt the collection of information and facts to understand the bigger picture. The gathering and assessment of additional information should be used to determine whether there is a reasonable suspicion that the activity or transaction is linked to money laundering, terrorist financing, proliferation financing and/or other illegal activity or whether there is a reasonable explanation for it. Unusual activity or an unusual transaction should not automatically result in the filing of a suspicious report with the Centre.

- **Suspicious activity** – It refers to any incident, event, individual or activity that seems out of place or at odds with your client’s usual activity. Where a suspicious activity occurs, a Suspicious Activity Report (SAR) should be filed with the Centre.
- **Suspicious transactions** -Are transactions in which there are reasonable grounds to suspect that the client’s funds, properties or assets involved are linked to the proceeds of crime. The funds, properties or assets could have been derived from an illegal activity or are intended to be used for an illegal activity. Where a suspicious transaction occurs, a Suspicious Transaction Report (STR) should be filed with the Centre.
- **Suspicious activity or transaction** – A suspicious transaction or activity is when you suspect or have reasonable grounds to suspect that funds involved in the transaction or activity are the proceeds of crime, or are related to terrorism financing. Where a suspicious activity and transaction occur, a Suspicious Transaction Activity Report (STAR) should be filed with the Centre.

4.DETECTING AND IDENTIFYING SUSPICION

POCAMLA requires lawyers, notaries, and other independent legal professionals to monitor on an ongoing basis all complex, unusual, suspicious, large or such other transactions as may be specified in the law, whether completed or not, and shall pay attention to all unusual patterns of transactions, and to insignificant but periodic patterns of transactions which have no apparent economic or lawful purpose.

Determining whether a transaction or activity is suspicious is based on the knowledge of your client and, their nature of business. Lawyers, notaries, other independent legal professionals, and their employees are better positioned to identify transactions that lack justification or do not fall within the usual methods of a legitimate business.

To identify unusual customer transactions, Lawyers, notaries, and other independent legal professionals should consider:

- (a) The nature and type of individual transactions;
- (b) The nature of a series of transactions;
- (c) The amount of the transactions, paying special attention to particularly substantial transactions;
- (d) The geographical origin/destination of a payment or receipt;
- (e) The customer's usual pattern of activities or turnover;
- (f) The Customer's residence status (whether a Kenyan national, a foreign resident, or an offshore/non-resident person or legal entity);
- (g) Type and location of services provided (for example, the creation, liquidation, raising of capital, distribution of dividends, registration, deregistration, transfer or jurisdiction, purchase, sale, or other act involving legal persons or arrangements);
- (h) Speed, frequency, and consistency of transactions (e.g. whether there is a requirement to expedite the transaction beyond what is considered usual, or a customer engages in multiple transactions or activities in a relatively short time span, especially when such transactions or activities appear to be inconsistent or in conflict with each other or with the customer's stated business purpose or socio-economic profile).

5.ML/TF INDICATORS FOR LEGAL PROFESSION

Looking for and recognizing red flags helps alert legal professionals to the potential for misuse and helps them to identify possible money laundering and terrorist financing activities. It is key to note that the mere presence of a red flag indicator is not necessarily a basis for a suspicion of money laundering or terrorist financing – a client may be able to provide a legitimate explanation.

The Indicators can be categorized according to:

- The client;
- The clients' funds;
- The clients' choice of lawyer;
- The nature of the retainer;
- The transactional patterns

5.1 Red flags about the client

Client's Behavior Or Identity	Concealment Techniques	The Relationship Between the Client And Counterparties
<ul style="list-style-type: none"> • Client is secretive or evasive about: <ul style="list-style-type: none"> ▪ Their identity or that of the beneficial owner; ▪ the source of funds; ▪ The purpose of the transaction • Client is known to have convictions, or to be currently under investigation for crime. • Client is related to or a known associate of a person listed as being involved or suspected of involvement with terrorists or terrorist financing operations; • The client is a positive match against UN 	<ul style="list-style-type: none"> • Use of intermediaries without good reason • Avoidance of personal contact for no good reason • Reluctance to disclose information, data and documents that are necessary to enable the execution of the transaction • Use of false or counterfeited documentation • The client is a business entity that cannot be found on the Internet 	<ul style="list-style-type: none"> • Ties between the parties of a family, employment, corporate or any other nature generate doubts as to the real nature/reason for transaction • Multiple appearances of the same parties in transactions over a short period of time • The parties attempt to disguise the real owner or parties to the transaction • The natural person acting as a director or representative does not appear to be a suitable representative • The parties are: <ul style="list-style-type: none"> ▪ native to, resident in, or incorporated in a higher-risk country; ▪ connected without apparent business reason; ▪ of an unusual age for executing parties;

<p>Security Council Resolutions Sanctions List</p> <ul style="list-style-type: none"> • Unusually familiar with the ordinary standards provided for by the law in satisfactory customer identification, data • Entries and STRs, or asks repeated questions on related procedures • The client, their representative, or beneficial owners being native to, resident in, or incorporated in a high-risk jurisdiction. • Client has no proper identification papers; • There is no information available on the client and his business; • No linkage between the client and the jurisdiction of the source or destination of funds. 		<ul style="list-style-type: none"> ▪ • not the same as the persons actually directing the operation
--	--	--

5.2 Red flags relating to clients' funds

Size of funds	Source or Destination of funds	Mode of payment
<p>There is no legitimate explanation for:</p> <ul style="list-style-type: none"> • A disproportionate amount of private funding, or cash considering the individual's socio-economic, or company's economic profile; • A significant increase in share capital for a recently incorporated company or successive contributions over a short period of time to the same company; 	<p>The source or destination of funds is unusual because:</p> <ul style="list-style-type: none"> • Third party funding either for the transaction or for fees/taxes involved with no apparent connection or legitimate explanation; • Funds are received from or sent to a 	<ul style="list-style-type: none"> • The asset is purchased with cash and then rapidly used as collateral for a loan. <p>There is no legitimate explanation for:</p> <ul style="list-style-type: none"> • An unusually short repayment period having been set; • Mortgages being repeatedly repaid significantly prior to the initially agreed maturity date;

<ul style="list-style-type: none"> • A receipt by the company of an injection of capital or assets that is high in comparison with the business, size or market value of the company performing; • An excessively high or low price attached to securities being transferred; • A large financial transaction, by a recently incorporated company, where it is not justified by the corporate purpose, the activity of the client's or its group companies; • The client deposits cash in the law firms' account and the client or third party borrows against those funds as collateral. 	<p>foreign country when there is no apparent connection between the country and the client;</p> <ul style="list-style-type: none"> • Funds are received from or sent to higher-risk countries; • Funds are received or sent to multiple bank accounts or foreign accounts without good reason; • Private expenditure is funded by a company, business or government; • The collateral being provided for the transaction is currently located in a higher-risk country. • Funds are from, or are sent to, countries with high levels of secrecy (tax havens); • The client is not located near you and is asking for types of services that are not common for you to provide, or outside your area(s) of law entirely; • The client expresses a sense of great urgency and asks you to cut corners; • The funds received are inconsistent with the client's occupation or 	<ul style="list-style-type: none"> • Finance being provided by a lender, either a natural or legal person.
---	--	---

	socio-economic profile.	
--	-------------------------	--

5.3 Red flags relating to the client's choice of lawyer

- The client willing to pay substantially higher fees than usual, without good reason;
- The client changing legal advisors a number of times within a short span of time or engagement of multiple legal advisers without good reason;
- The required service being refused by another lawyer, or the relationship with another lawyer being terminated.

5.2 Red flags on the nature of retainer

- The client actively avoids personal contact without good reason
- The client is willing to pay fees without the requirement for legal work to be undertaken
- Requests for unexplained speed in completing a transaction
- The client appears very disinterested in the outcome of the retainer
- Frequently changing legal structures and/or directors of legal persons
- Creation of complicated ownership structures when there is no legitimate or economic reason
- Involvement of structures with multiple countries where there is no apparent link to the client or transaction, or no other legitimate or economic reason
- Consecutive property transactions with rapidly increasing value or purchase price
- Abandoned transactions with no concern for the fee level or after receipt of funds i.e. no transfer of title after payment for property.
- The retainer exclusively relates to keeping documents or other goods, holding large deposits of money, or otherwise using the client account without the provision of legal services
- There are unexplained changes in instructions, especially at the last minute
- Requests for payments to third parties without substantiating reason or corresponding transaction
- Situations where advice on setting up legal arrangements may be misused to obscure ownership or real economic purpose

5.4 Red flags on the transactional patterns

- Use of client account without an underlying legal transaction
- Structuring of payments by client in the firms client account to avoid reporting thresholds or raise suspicion
- Complex or unusual transactions by client, possibly with unrelated parties
- Payments for unspecified services

- Client insisting on loss-making transactions where the loss is avoidable i.e. shares are redeemed at a price lower than the prevailing purchase price
- Absence of documentation to support the client's story, previous transactions, or company activities
- Payments in excess of the services provided
- Transactions with companies whose identity is difficult to establish

6.FILING A SUSPICIOUS REPORT

6.1 Internal process for reporting suspicion to the Money Laundering Reporting Officer (MLRO)

Where a client, or a potential client, attempts to conduct business or engage in a transaction that raises suspicion or where it seems that the activity or transaction, or attempted activity or transaction gives rise to a suspicion or raises initial concerns that money laundering, terrorism financing or proliferation financing is being attempted or is occurring, this suspicion must be reported to the MLRO by the staff.

A staff member of the firm shall make an internal disclosure of their suspicion to the firm's MLRO in accordance with their internal reporting procedures.

The MLRO will obtain further information and make an assessment of the disclosure to determine whether the facts give rise to a suspicion of money laundering, terrorist financing or proliferation financing. Further, it may involve asking additional questions from staff or client, obtaining additional customer due diligence (CDD), and trying to understand the background and the events leading up to and surrounding the potential suspicious activity or transaction. The aim of the assessment is to look at the totality of the circumstances to determine whether the client or their transaction is merely unusual, or whether there are subjective grounds for a suspicion of money laundering, terrorism financing or proliferation financing that would require the filing of a suspicious report with the Centre. Where there are reasonable grounds for suspicion, the MLRO shall file a suspicious report with the Centre.

The MLRO is not responsible for proving that money laundering, terrorism financing or proliferation financing is actually happening. Instead, their task is to review the internal report, gather any additional relevant information, understand the circumstances, analyze

all available details, and decide whether there is enough evidence to form a belief or suspicion that such criminal activity may be taking place.

6.2 When to file a suspicious report

An MLRO shall file a suspicious report with the Centre within two days upon establishing reasonable grounds for suspicion in the specified manner.

However, where the information was obtained in circumstances where it is subject to professional secrecy or legal professional privilege, the MLRO is not required to report.

An MLRO must not inform their clients or any other person that a suspicious report has been filed with the Centre.

6.3 What is to be included in a suspicious report?

A suspicious report shall entail the **reason for suspicion** and **basis of suspicion**. The reason for suspicion shall entail both the identification of the suspicious person and the identification of transaction or activity.

6.3.1 Profiling of your Client

- Natural person (name, nationality, Identification Card/Passport, Date of Birth);
- Legal person (name, registration number, date of registration, directors/shareholders, beneficial owners, nominee directors or partners).
- Politically exposed person (PEP) relation
- Occupation or nature of business of the suspicious person
- Date of establishment of a relationship with the law firm and services or accounts offered or held with your law firm
- Location of person (high-risk jurisdiction or area)
- Nature in which the suspicious person is involved in the suspicious transaction or activity

6.3.2 Details of suspicious transactions or activity:

- The date of service or transaction
- Description of the nature of the transaction or service
- Declared source of funds;
- Transaction details;
- Declared purpose of funds
- Country of origin or destination of funds

The basis of suspicion highlights why the identified transactions are suspicious with their corresponding ML/TF indicators. Indicators are informed by a description of suspicion and the suspicious transaction or activity.

A suspicious transaction or activity report should be supported by the **necessary documents** depending on the transaction or activity:

- i. Client on-boarding forms
- ii. Record of transactions of the client
- iii. Additional supporting documents:
 - Bank slips, receipts
 - Agreements and advisories – land sale, service, real estate
 - Invoices – Commercial and Pro-forma
 - Customer due diligence and enhanced due diligence documentation

A suspicious transaction or activity is said to be of quality where it is reported within the timelines, contains unique identifiers for both natural and legal persons, identifies the suspicious transaction or activity and probable offence.

6.4 Suspicious report submission process

Reporting institutions should use the prescribed system to submit suspicious reports to the Centre.

6.5 Post-Reporting Obligations

Upon receipt of a suspicious report, the Centre reviews the submission and may request additional information where necessary. Lawyers, notaries, and other independent legal professionals should ensure that they maintain and keep records of all transactions, both domestic and international for a minimum period of seven years from the date the relevant business or transaction was completed or following the termination of an account or business relationship.

Lawyers, notaries and other independent legal professionals should ensure that they keep all records obtained through customer due diligence measures such as copies or records of official documents like passports, identification cards or similar documents, account files and business correspondence including the results of any analysis undertaken such as inquiries to establish the background and purpose of complex, unusual, large transactions for a period of seven years.

Lawyers, notaries and other independent legal professionals shall ensure that all customer due diligence information and transaction records under the Act and these regulations shall,

as and when required be made available swiftly to domestic competent authorities upon request.

Lawyers, notaries and other independent legal professionals have the discretion to decide to continue or terminate a customer relationship after filing a suspicious transaction or activity. Where the reporting institution chooses to continue with the relationship, it must put mechanisms to continually monitor customer transactions and activity and report any additional suspicious transactions or activities.

6.6 Decision not submit a suspicious report

Where the MLRO decides that the internal disclosure does not substantiate a suspicion of money laundering, terrorism financing or proliferation financing, the MLRO must document the reasons for their decision and keep records of this along with the original internal disclosure by the staff. This is a crucial step to take when deciding not to externalize a suspicious report to the FRC or LSK. This will help demonstrate compliance with AML/CFT obligations or could help in submitting a suspicious report.

7. Protection of Information and Informers, Tipping-off and other Offences

7.1 Protection of Information and Informers

Where any information relating to a suspicious report filed with the Centre, the information and the identity of the person giving the information shall be kept confidential.

7.2 Tipping-off

Lawyers, Notaries and other Independent Legal Professionals are prohibited by law from disclosing the fact that a suspicious report or related information is being filed with the Centre.

Any Lawyer, Notary or other Independent Legal Professional who knows or ought reasonably to have known that a report is being prepared or has been or is about to be sent to the Centre and discloses to another person such information or other matters relating to a report commits an offence.

7.3 Offences and Penalties

S/No.	Offence	Penalty
1.	Failure to report suspicion regarding proceeds of crime	Natural Person <ul style="list-style-type: none"> Imprisonment for a term not exceeding seven years

		<ul style="list-style-type: none"> • A fine not exceeding two million, five hundred thousand shillings, or to both
		Body corporate <ul style="list-style-type: none"> • A fine not exceeding ten million shillings
2.	Failure to comply with monitoring and reporting requirements	Natural person <ul style="list-style-type: none"> • Imprisonment for a term not exceeding seven years, • A fine not exceeding two million, five hundred thousand shillings, or to both
		Body corporate <ul style="list-style-type: none"> • A fine not exceeding ten million shillings or the amount of the value of the property involved in the offence, whichever is the higher.
3.	Tipping off	Natural person <ul style="list-style-type: none"> • Imprisonment for a term not exceeding seven years • A fine not exceeding two million, five hundred thousand shillings, or to both.
		Body corporate <ul style="list-style-type: none"> • A fine not exceeding ten million shillings or the amount of the value of the property involved in the offence, whichever is the higher.
4.	Misrepresentation	Natural person <ul style="list-style-type: none"> • Imprisonment for a term not exceeding two years, or a fine not exceeding one million shillings, or to both.
		Body corporate <ul style="list-style-type: none"> • A fine not exceeding five million shillings or the amount of the value of the property involved in the offence, whichever is the higher.
5.	Malicious reporting	Natural person <ul style="list-style-type: none"> • Imprisonment for a term not exceeding two years • A fine not exceeding one million shillings, or to both
		Body corporate

8.1 Misuse of Client Accounts

CASE STUDY 1

A law firm was approached by a new client with instructions to assist on a number of asset purchases. The client requested account details of the firm before completing customer due diligence on the client or entering into an engagement letter with her. The client did not give any further instructions following the deposit of funds. Subsequently, the client explained that she no longer intended to purchase the relevant assets and asked for the deposited money to be provided to a third party, rather than returned to her personal account.

Red Flag Indicators;

- Once funds received in client account, the transaction is aborted.
- Client requests that deposited funds are sent to a third party, rather than returned to it.
- The client avoids personal contact without good reason.

		<ul style="list-style-type: none"> • A fine not exceeding five million shillings or the amount of the value of the property involved in the offence, whichever is the higher.
6.	Misuse of information	<p>Natural person</p> <ul style="list-style-type: none"> • Imprisonment for a term not exceeding seven years • A fine not exceeding two million, five hundred thousand shillings, or to both <p>Body corporate</p> <ul style="list-style-type: none"> • A fine not exceeding ten million shillings or the amount of the value of the property involved in the offence, whichever is the higher.

8.CASE STUDIES

8.2 Potential misuse of Legal Firms by PEPs

CASE STUDY 3

A client approached a legal professional to buy two properties in a foreign jurisdiction for USD 11 Million. The purchase price was wholly funded by the purchaser (there was no mortgage), and the funds were sent through a bank in a high risk off-shore jurisdiction. As the contract was about to be signed, there was a change in instructions, and a property investment company was replaced as the purchaser. The two minor children of the client were the shareholders of the company. The foreign client held an important political function in his country and there was publicly available information about his involvement in financial wrongdoing

Red Flag Indicators

- Disproportionate amount of private funding, which is inconsistent with the socio-economic profile of the individual
- Client is using bank accounts from a high-risk Jurisdiction
- Use of a complicated structure with no legitimate reason
- Shareholders of the executing party are under the set legal age

8.3 Legal professional sets up multiple international company structures

CASE STUDY 4

A legal professional was asked to set up a series of companies for clients for the purpose of purchasing real estate. Some companies were incorporated in the lawyer's resident jurisdiction but were owned by companies that the legal professional had incorporated in another jurisdiction. The legal professional and others in the law firm were listed as the board of directors of the companies incorporated in the foreign jurisdiction. They

8.4 Potential abuse of power of attorney

CASE STUDY 5

A legal professional was asked to prepare a power of attorney for a client to give control of all of his assets to his girlfriend, including power to dispose of those assets. The legal professional then prepared a deed of conveyance under which the girlfriend transferred all of the property to the client's brother and sister. The legal professional had just secured bail for the client in relation to a drug trafficking charge. The legal professional was acquitted of money laundering.

Red Flag Indicators:

- A power of attorney is sought for the disposal of assets under conditions which are unusual and where there is no logical explanation
- Unexplained speed and complexity in the transaction.
- Client is known to be under investigation for involvement in crime.

9. Links to FATF guidance notes for Legal Professionals

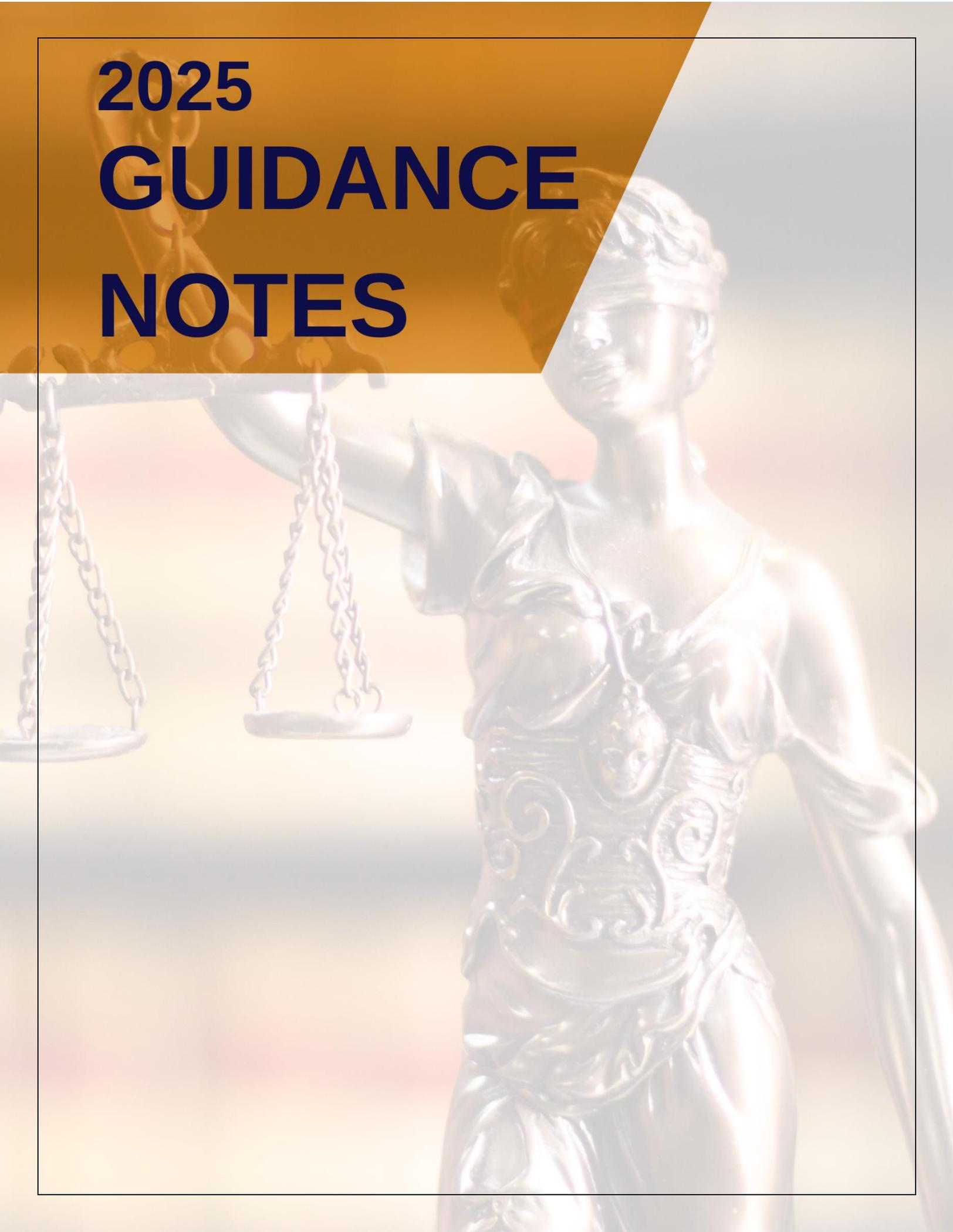
- i. **Guidance for a Risk-Based Approach for Legal Professionals, June 2019**

<https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Risk-Based-Approach-Legal-Professionals.pdf.coredownload.inline.pdf>

- ii. **Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals June 2013 -**

<https://www.bureauft.nl/media/btvjsaxr/money-laundering-and-terrorist-financing-vulnerabilities-of-legal-professionals.pdf>

2025 GUIDANCE NOTES





Contact Us

Financial Reporting Centre
Old Mutual Tower 13th Floor
Upper Hill.
P.O. Box Private Bag - 00200,
Nairobi, Kenya
Email: info@frc.go.ke
Phone: + 2547098580005
<https://www.frc.go.ke>