GAZETTE NOTICE NO. 1421

THE CAPITAL MARKETS ACT

(*Cap*. 485A)

GUIDELINES ON THE PREVENTION OF MONEY LAUNDERING AND TERRORISM FINANCING IN THE CAPITAL MARKETS

ARRANGEMENT OF GUIDELINES

THE CAPITAL MARKETS ACT
(*Cap*. 485A)

IN EXERCISE of the powers conferred by section 12 A (1) of the Capital Markets Act, the Capital Markets Authority, issues the following Guidelines—

GUIDELINES ON THE PREVENTION OF MONEY LAUNDERING AND TERRORISM FINANCING IN THE CAPITAL MARKETS

Citation

1. These Guidelines may be cited as the Guidelines on the Prevention of Money Laundering and Terrorism Financing in the Capital Markets, 2015.

Interpretation

2. (1) In these Guidelines, unless the context otherwise requires—

"Act" means the Proceeds of Crime and Anti-Money Laundering Act, 2009;

"AML" means anti-money laundering;

"Authority" means the Capital Markets Authority;

"CDD" means customer due diligence;

"CIS" means collective investment scheme;

"EDD" means enhanced due diligence;

"Financial Action Task Force" means the intergovernmental body established in 1989 by ministers of member jurisdictions, representing most major international financial centers to set standards and promote effective implementation of legal, regulatory and operational measures from combating money laundering, terrorist financing and other related threats to the integrity of the international financial system;

"Financial Reporting Centre" means the Centre established under section 21 of the Act;

"market intermediary" means a person approved or licensed to transact business by the Capital Markets Authority under Part IV of the Capital Markets Act;

"Regulations" means the Proceeds of Crime and Anti-Money Laundering Regulations, 2013; and

"terrorism financing" includes the offence specified under section 5 of the Prevention of Terrorism Act, 2012.

General Description of money laundering and terrorist financing

2.2 (1) Despite the variety of methods employed, the money laundering process is accomplished in three stages. These stages, described below, may comprise of numerous transactions by the persons engaged in money laundering that could alert an institution of the criminal activity.

(a) Placement – A person engaged in money laundering introduces his or her illegal profits into the financial system;

(b) Layering – In this phase, the person engaged in money laundering engages in a series of conversions or movements of the funds to distance them from their source. The funds might be channeled through the purchase and sales of investment instruments;

(c) Integration – This is the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, an integration scheme places the laundered proceeds back into the legitimate economy in such a way that they re-enter the financial system appearing as normal business funds.

(2) The three basic steps may occur as separate and distinct phases. Alternatively, they may occur simultaneously or, more commonly, they may overlap. How the basic steps are used depends on the available laundering mechanisms and the requirements of the criminal organizations.

(3) Money laundering in the capital markets can take place in all the three stages, as capital markets are no longer predominantly cash based, they are more likely to be used in the layering stage rather than placement stage of money laundering. However, where the transactions are in cash, there is still the risk of capital markets being used at the placement stage. Capital markets offer a vast array of opportunities for transforming money into a diverse range of assets. For liquid assets, they allow a high frequency of transactions which aid the layering process. Hence, capital markets are particularly attractive to persons engaged in money laundering for layering their illicit proceeds for eventual integration into the general economy.

(4) The capital markets are global in nature and with the increasing developments in technology, payment systems, and other direct gateways into the markets, the speed and the relative anonymity of these avenues make them an option for persons engaged in money laundering.

(5) The capital markets have an additional distinguishing money laundering risk factor in that not only can it be used to launder illicit funds that result from illegal activity outside of the financial markets but it can also be used to generate illicit funds from the market itself, for example, in cases of insider trading. Factors presenting higher risk might include –

(a) services that inherently have provided more anonymity;

(b) ability to pool underlying customers' funds, collective investment schemes, real estate investment trusts, mutual funds, among others;

(c) liquid securities with high volumes so that ease of detection is much less than illiquid securities where volumes are lower and therefore irregularities are easier to detect;

(d) options contracts which are executed through an exchange are risky due to the relative ease of access by persons engaged in money laundering via brokers, the global nature of exchanges, the volume of transactions conducted on an exchange which present monitoring challenges and the ability to rapidly enter and exit the markets.

(6) Persons engaged in money laundering can buy or sell futures via brokers thus layering transactions on Exchanges. This is done through taking large positions and providing illicit funds to cover margin calls. They can also realize profits or losses at any time since exiting the market is as simple as entering into the reverse transaction thus recouping outstanding margin deposits and bringing the funds back into the broader financial system with seeming legitimacy. The distribution channel for products may alter the risk profile of a customer and may include online sales, postal or telephone channels where a non-face-to-face account opening approach is used. Business sold through intermediaries may also increase risk as the business relationship between the customer and a market intermediary may become indirect.

(7) Trust, nominee and fiduciary accounts are a popular vehicle for criminals wishing to avoid the identification procedures and mask the origin of the money accrued from criminal activities they wish to launder. Particular care needs to be exercised when the accounts are set

up in locations with strict bank secrecy or confidentiality rules. Where the market intermediary has not previously verified the identity of a trustee or has no current relationship with a trustee, verification of the identity of the trustee or where there are several trustees, the identity of all the trustees should be undertaken in line with the normal procedures as set out in Regulation 19 of the Proceeds of Crime and Anti Money Laundering Regulations, 2013.

(8) Terrorists or terrorist organizations require financial support in order to achieve their aims. There is often a need for them to obscure or disguise links between them and their funding sources. It follows then that terrorist groups shall similarly find ways to launder funds, regardless of whether the funds are from a legitimate or illegitimate source, in order to be able to use them without attracting the attention of the authorities.

Responsibility of the Board and management

3. (1) The Board of directors of a market intermediary shall be responsible for the—

(a) establishment of appropriate policies and procedures for the detection and prevention of money laundering and terrorist financing and ensuring their effectiveness; and

(b) the market intermediary's compliance with these Guidelines, the Proceeds of Crime and Anti Money Laundering Act, 2009, and all other legal and regulatory requirements thereto.

(2) A market intermediary shall formulate and implement internal controls and other procedures that will deter criminals from using its facilities for money laundering and terrorist financing and ensure that business is conducted in conformity with the law and high ethical standards and that service is not provided where there is good reason to suppose that transactions are associated with money laundering activities or terrorist financing.

(3) A market intermediary shall co-operate fully with law enforcement agencies and relevant regulatory bodies, and shall take appropriate measures to disclose information to the Financial Reporting Centre and other enforcement agencies.

(4) A market intermediary shall review its policies, procedures and controls at least once in every two years to ensure their effectiveness as required by the Regulations.

Risk- Based Approach

4. (1) Where customers are assessed to be of higher money laundering risk, a market intermediary shall take enhanced measures to manage and mitigate those risks. Where the risks are lower, simplified measures may be applied. Simplified measures include reducing the frequency of customer identification updates or reducing the degree of ongoing monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

(2) A market intermediary shall identify, assess and take effective action to mitigate money laundering risks and adopt a holistic approach to the Risk Based Approach and should avoid a silo approach when assessing the relationship between risks.

(3) A market intermediary may assess the money laundering risks of individual customers by assigning money laundering risk rating to their customers.

(4) While there is no agreed upon set of risk factors and no single methodology to apply these risk factors in determining the money laundering risk rating of customers, a market intermediary shall consider the following factors:

(a) In relation to country risk, customers with residence in or connection with high risk jurisdictions for example—

(i) those that have been identified by the Financial Action Taskforce, as jurisdictions with strategic AML deficiencies;

(ii) countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations;

(iii) countries which are vulnerable to corruption; or

(iv) countries that are believed to have strong links to terrorist activities.

(b) In assessing country risk associated with a customer, consideration may be given to data available from the United Nations, the International Monetary Fund, the World Bank, the Financial Action Taskforce, among others and the market intermediary's own experience or the experience of other group entities where the market intermediary is part of a multi-national group, which may have indicated weaknesses in other jurisdictions.

(c) The following are examples of customers who might be considered to carry lower money laundering risks –

(i) customers who are employed or with a regular source of income from a known legitimate source which supports the activity being undertaken;

(ii) the positive reputation of the customer, e.g. a well-known, reputable public or private company, with a long history that is well documented by independent sources, including information regarding its ownership and control; or

(iii) a public entity.

(d) Some customers, by their nature or behaviour might present a higher risk of money laundering. Factors might include –

(i) a politically exposed person, or the public profile of the customer indicating involvement with, or connection to, politically exposed persons;

(ii) complexity of the relationship, including use of corporate structures, trusts and the use of nominee accounts where there is no legitimate commercial rationale;

(iii) a request to use numbered accounts or undue levels of secrecy with a transaction;

(iv)) involvement in cash-intensive businesses;

(v) nature, scope and location of business activities generating the funds or assets, having regard to sensitive or high-risk activities;

(vi) where the origin of wealth cannot be easily verified; or

(vii) retail participants who tend to have a greater level of money laundering risk associated to them in contrast to wholesale customers who usually will have a

regulatory status and an established business. Persons engaged in money laundering will tend to avoid licensing obligations and regulatory scrutiny preferring the opacity of private corporations and trusts.

(5) A market intermediary shall keep records and relevant documents of the risk assessment for a minimum of seven years from their official date of creation or issuance, as appropriate, so that it can demonstrate to the Financial Reporting Centre or other competent authorities—

(a) how it assesses the customer's money laundering risk; and,

(b) that the extent of CDD and ongoing monitoring is appropriate based on that customer's money laundering risk.

(6) A securities or derivatives exchange shall have surveillance systems and mechanisms that are designed to detect activities that might be a result of market manipulation for instance, wash selling, pump and dump or insider trading which are predicate offences to money laundering.

(7) The surveillance staff at a securities or derivatives exchange, on noticing activity that may amount to market manipulation, insider trading or any other anomaly, should alert the market intermediary involved in that particular trade to cross check on whether the transaction can be classified as suspicious thus requiring further investigation and reporting to the Financial Reporting Centre as a suspicious transaction.

Customer Identification

5. (1) A market intermediary shall obtain satisfactory evidence of the identity and legal existence of the persons applying to do business with it. The evidence shall be verified by reliable documents or other verifiable and independent means. A market intermediary shall not engage in any business transactions with a client who fails to provide evidence of their identity. A market intermediary shall not keep anonymous accounts or accounts in fictitious names of their clients.

(2) A collective investment scheme manager shall verify the identity of a customer using reliable and independent sources. The collective investment scheme manager shall retain copies of all reference documents used in identity verification and the identification information.

(3) A market intermediary shall implement and maintain appropriate guidelines for its agents and employees to assist them in learning and establishing essential facts about their customers' backgrounds. A market intermediary shall keep records of enforcement of these guidelines for not less than seven years from the date of any action taken against the employee or agent.

Customer due diligence

6. (1) A market intermediary shall conduct ongoing due diligence and scrutiny of customers' identity and their investment objectives. This shall be done throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the market intermediary's knowledge of the customer, its business and its risk profile.

(2) For customers that require additional caution to be exercised when transacting with them, such customer's activities shall be monitored on a regular basis for suspicious transactions. Where a customer fails to comply with the due diligence requirements, the market intermediary shall not commence business relations, or, where there is an existing business relationship, the market intermediary shall terminate such relationship and consider lodging a suspicious transaction report with Financial Reporting Centre. A market intermediary, when handling new account applications, shall identify if the applicant is a domestic or foreign politically exposed person and if so, the market intermediary shall take adequate control measures and conduct periodic reviews.

(3) A market intermediary shall adopt risk-based approach where they employ enhanced customer due diligence process for higher risk categories of customers, business relationships or transactions.

(4) A market intermediary shall perform such customer due diligence measures as may be appropriate to its existing customers having regard to own assessment of materiality and risk.

(5) Where the market intermediary obtains information or documents from the customer or a third party, it should take reasonable steps to assure itself that such information or documents are reliable and where appropriate, reasonably up to date at the time they are provided to the market intermediary.

(6) On face-to-face transactions verification, a market intermediary may, where due to a perception of increased risk, additional documentation is required, request a reference letter from a current employer, professional or members' organization, bank statements, a lease for a rental house or business premises or seek further independent verification of a passport or a national identity card submitted.

(7) For prospective customers who are not normally resident in Kenya but who wish to open an account with a market intermediary in Kenya, it is important that verification procedures similar to those for Kenyan resident customers be carried out and the same information obtained. More importantly, the copy of passport, national identity card or documentary evidence of his or her address shall be certified by—

(a) the embassy, consulate or High Commission of the country of issue,

(b) Commissioner of oaths or Notary Public, or

(c) senior officer of the market intermediary whose full name and title shall appear on the face of the copy. The senior officer shall stamp, date and sign with the words "originals sighted by me".

(8) A market intermediary may independently verify identity with a reputable institution authorized to carry out this role in the applicant's country of residence. For prospective non-resident customers who wish to open investment accounts by post, independent verification of identity should therefore be sought from a reputable institution authorized to carry out this role in the applicant's country of residence. Verification details requested should cover and may include but not be limited to the true name or names used, current permanent address and verification of signature.

(9) Because of the possible difficulties of identifying beneficial ownership, and the complexity of their organizations and structures, corporate and legal entities are the most likely vehicles for money laundering, particularly when fronted by a legitimate trading company. The following measures should be taken—

(a) Particular care should be taken to verify the legal existence of the applicant and to ensure that any person purporting to act on behalf of the applicant is fully authorized. The principal requirement is to look behind the corporate entity to identify those who have ultimate control over the business and the company's assets, with particular attention paid to any shareholders or others who inject a significant proportion of the capital or financial support. Enquiries should be made to confirm that the company exists for a legitimate trading or economic purpose and that it is not merely a "shell company'" where the controlling principals cannot be identified.

(b) The CDD measures for legal persons should include reasonable actions to understand whether the customer is acting as an agent or a beneficial owner, as well as the business nature and the purpose of trade.

(c) Before a business relationship is established, measures should be taken by way of a company search or other commercial enquiries to ensure that the applicant company has not been, or is not in the process of being, dissolved, struck off, wound-up or terminated.

(d) As with personal accounts or facilities, the "know your customer" principle is an on-going process. If changes to the company structure or ownership occur subsequently or if suspicions are aroused by a change in the nature of the business transacted or the profile of payments through a company account, further checks should be made to ascertain the reason for the changes.

(e) In addition, enquiries should be made from time to time to establish whether there have been any changes to directors or shareholders or to the original nature of the business or activity. Such changes could be significant in relation to potential money laundering activity even though authorized signatories have not changed.

(10) In the case of partnerships, unit trusts and other unincorporated businesses whose partners have not previously been verified by the market intermediary, the identity of all partners and signatories to the account should be verified. Additionally, the partnership agreement, the trust deed or other relevant documentation should be obtained. In cases where a formal partnership arrangement exists, a mandate from the partnership authorizing the opening of an account and conferring authority on those who will operate it should be obtained.

(11) Trust, nominee and fiduciary accounts are a popular vehicle for criminals wishing to avoid the identification procedures and mask the origin of the money accrued from criminal activities they wish to launder. Particular care needs to be exercised when the accounts are set up in locations with strict bank secrecy or confidentiality rules. Where the market intermediary has not previously verified the identity of a trustee or has no current relationship with a trustee, verification of the identity of the trustee, or where there are several trustees, the identity of all the trustees should be undertaken in line with the normal procedures as set out in Regulation 16 of the Proceeds of Crime and Anti Money Laundering Regulations, 2013.

(12) In cases where a nominee opening an account on behalf of another whose identity has not been previously identified by the market intermediary, the identity of that nominee or any other person who will have control of the account shall be verified.

(13) Nominee accounts may be established by and in the name of persons in order to engage in securities transactions on behalf of their clients. When the market intermediary opens a nominee account for a customer who is an institution supervised by the Authority, the risk of the omnibus account being used for money laundering or terrorist financing is generally lower. The market intermediary can consider if it may perform simplified CDD measures, so that there is no need to identify and verify the underlying clients of the market intermediary. However, when the market intermediary opens a nominee account for a customer who is a foreign financial institution, the risks associated with the account in some circumstances may be considered to be potentially higher, and enhanced CDD measures may be appropriate.

(14) A CIS manager shall perform CDD measures when unit holders subscribe or take part in the CIS or the CIS manager enters into negotiations with an entity with a view to signing a trust deed for establishment.

(15) Upon determining a customer as "high risk", the market intermediary should undertake EDD processes on the customer which should include

(a) enquiring on the purpose for opening an account;

(b) enquiring the level and nature of trading activities intended;

(c) enquiring on the ultimate beneficial owners;

(d) enquiring on the source of funds;

(e) obtaining senior management's approval for opening an account; and

(f) conducting enhanced ongoing monitoring of the business relationship.

(16) EDD should be carried out when:

(a) there is a transaction that is significant, having regard to the manner in which the account is ordinarily operated;

(b) there is a substantial change in the market intermediary's own customer documentation standards;

(c) there is a material change in the way that business relations with the customer are conducted;

(d) the market intermediary becomes aware that it may lack adequate identification information on a customer; and

(e) the market intermediary becomes aware that there may be a change in the ownership or constitution of the customer or the person authorized to act on behalf of the customer in its business relations with the market intermediary.

(17) Where the market intermediary obtains information or documents from the customer or a third party, it should take reasonable steps to assure itself that such information or documents are reliable and where appropriate, reasonably up to date at the time they are provided to the market intermediary.

(18) Where the customer is unable to produce original documents, the market intermediary may accept documents that are certified to be true copies by the originators of the documents, or if this is not possible, certified by magistrates, advocates, commissioners for oaths or notaries public.

(19) A market intermediary may often encounter cases where, to its knowledge, the customer is a manager of a portfolio of assets and is operating the account in that capacity. In such cases, the underlying investors of the portfolio will be beneficial owners. However, the Authority recognizes that a market intermediary may not be able to perform CDD on the underlying investors. For instance, the portfolio manager may be reluctant, for legitimate commercial reasons, to reveal information on the underlying investors to the market intermediary. In such circumstances, the market intermediary should evaluate the risks arising from each case and determine the appropriate CDD measures to take. In this regard and for each client in this category, the market intermediary shall prepare a report of the evaluation and make the same available to the Authority upon request.

(20) A market intermediary may consider whether simplified CDD measures could be applied, so that identification and verification of the underlying investors as beneficial owners are dispensed with. In addition, where a collective investment scheme is the customer for a market intermediary, the latter should take steps to identify whether it is an exchange-listed CIS, and if it is, the market intermediary shall conduct higher CDD measures.

Record Keeping

7. (1) A market intermediary shall ensure that—

(a) all requirements imposed by law relating records and documentation are met;

(b) all records of customers, business relationship and transactions remain up-to-date, relevant and accessible;

(c) any transaction undertaken by the market intermediary can be reconstructed so as to provide, if necessary, evidence for prosecution of criminal activity; and

(d) the records can be accessed and shared within a reasonable time or such period imposed by law, where any inquiry or order is made by the Authority, the Financial Reporting Centre or any other relevant law enforcement agency.

(2) A market intermediary shall undertake periodic or *ad hoc* reviews of existing customer records.

(3) A market intermediary shall retain documents and records pertaining to a matter which is under investigation or which has been the subject of the Financial Reporting Centre for such longer period as may be necessary in accordance with any request or order from the Authority, the Financial Reporting Centre or from other relevant competent authorities.

(4) A market intermediary shall maintain and keep records of all transactions 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. Retention may be by way of original documents, stored on computer disk or in other electronic form.

New technology and non-face-to-face transactions

8. (1) A market intermediary shall establish policies and procedures to address any specific risks associated with the use of new technology and non-face-to-face business relations or transactions, and these shall be documented and be easily accessible to the employees of the market intermediary.

(2) On non-face-to-face transactions verification, a market intermediary shall, adopt procedures which are more robust as those for face-to-face verification to confirm the identity of the client and to provide for reasonable steps to avoid single or multiple fictitious applications or substitution (impersonation) or fraud for the purposes of money laundering. The procedures adopted shall-

(a) ensure that a person bearing the name of the applicant exists and lives or is resident at the address provided; and

(b) ensure that the applicant is actually that person.

(3) Stringent measures and procedures shall be undertaken while using new technologies and non-face-to-face business transactions.

(4) A market intermediary should take one or more of the following measures to mitigate the heightened risk associated with not being able to have face-to-face contact when establishing business relations:

(a) telephone contact with the customer at a residential or business number that can be verified independently;

(b) confirmation of the customer's address through an exchange of correspondence or other appropriate method;

(c) subject to the customer's consent, telephone confirmation of the customer's employment status with the customer's employer's personnel department at a listed business number of the employer;

(d) confirmation of the customer's salary or any other source of income details by requiring the presentation of recent bank statements from a bank;

(e) certification of identification documents by magistrates, commissioners of oaths or notaries public presented by the customer; or

(f) any other reliable verification checks adopted by the market intermediary for non-face-to-face business.

(5) A market intermediary may use the following as a means of verification—

(a) recent utility bill, personal identification number issued by the Kenya Revenue Authority, bank reference; or

(b) computerized system, for internal or external application database checks, to check for any inconsistencies in the information provided.

(6) A market intermediary shall use the following types of information as minimum acceptable standard for determining the legitimacy of funds and transactions-

(a) for multiple or nominee accounts, or similar or related transactions, a written statement from the client confirming the reason and the need for multiple or nominee accounts, or similar or related transactions;

(b) for large or unusual transfers or payments of funds, appropriate documentation as to the identity of the recipient or sender of the transferred or paid funds, and the reason underlying the transfer or payment;

(c) for large or unusual investments, a written statement from the client confirming that the investments are *bona fide* and consistent with the goals and objectives of the client's reasonable and normal business activities;

(d) for large and unusual foreign transactions, a written confirmation from the client indicating the nature, reason and appropriate details of the foreign transactions sufficient to determine the legitimacy of such transactions.

Foreign branches and subsidiaries.

9. A market intermediary that is incorporated in Kenya shall develop a group policy on anti-money laundering and countering financing of terrorism and this policy shall apply to all its branches and subsidiaries where applicable outside Kenya.

Suspicious transactions.

10. (1) Where the form or amount of any transaction appears unusual in relation to the customer, or if the economic purpose or legality of the transaction is not immediately clear, a market intermediary shall clarify the economic background and purpose of the transaction or business relationship. Special attention shall be given to complex and unusual patterns of transactions. Appendix I provides indicators of potential money laundering activities in the capital markets.

(2) If a market intermediary becomes aware of suspicious activities or transactions which indicate possible money laundering activities, the market intermediary shall report the same to the Financial Reporting Centre immediately or in any case within seven days of the date of the transaction or occurrence of the activity that is considered suspicious.

(3) A market intermediary shall disclose sufficient information which indicates the nature of and reason for the suspicion, and where the market intermediary has additional supporting documents, the documents shall also be availed.

(4) A market intermediary shall establish robust reporting mechanisms for suspicious transactions.

(5) A market intermediary shall keep a record of all transactions referred to the Financial Reporting Centre together with all internal findings and analysis done in relation to them.

Reporting requirements.

11. A market intermediary shall report to the Financial Reporting Centre all cash transactions carried out by it, equivalent to or exceeding USD 10,000 or its equivalent in any other currency

whether or not the transaction appears to be suspicious in accordance with Regulation 34 of the Proceeds of Crime and Anti Money Laundering Regulations, 2013.

The role of the Authority.

12. (1) The Authority shall undertake its reporting obligations in accordance with Regulation 33 of the Proceeds of Crime and Anti Money Laundering Regulations, 2013.

(2) The Authority shall take into account a market intermediary's compliance with the Act and the Regulations and these Guidelines, as well as measures put in place to ensure continued compliance, in determining the suitability of the market intermediary and persons managing or controlling the market intermediary for the maintenance of a license or an approval by the Authority.

Continuous monitoring.

13. (1) A market intermediary shall monitor on an ongoing basis, its business relationships with its customers.

(2) A market intermediary shall, during the course of business relations, observe the conduct of the customer's account and scrutinize transactions undertaken to ensure that the transactions are consistent with the market intermediary's knowledge of the customer, its business and risk profile and where appropriate, the source of funds.

(3) A market intermediary shall periodically review the adequacy of customer identification information and ensure that the information is kept up to date, particularly for the high risk category of customers.

(4) The extent of monitoring should be linked to the risk profile of the customer which has been determined through the risk assessment. To be most effective, resources should be targeted towards business relationships presenting a higher risk of money laundering. Financial institutions shall take additional measures when monitoring business relationships that pose a higher risk. High risk relationships, for example those involving politically exposed persons, non-face-to-face customers, will require more frequent and intensive monitoring. In monitoring high-risk situations, relevant considerations may include -

(a) whether adequate procedures or management information systems are in place to provide relevant staff (e.g. Compliance Officer, Money Laundering Reporting Officer, front line staff, relationship managers, Account Opening Personnel and Operation Managers) with timely information that might include, as a result of EDD or other additional measures undertaken, any information on any connected accounts or relationships; and

(b) how to monitor the sources of funds, wealth and income for higher risk customers and how any changes in circumstances will be recorded.

Internal policies, compliance and training.

14. (1) A market intermediary shall develop, adopt and implement internal programmes, policies, procedures and controls to prevent and detect any offence under the Act. Such programmes and policies shall include—

(a) the establishment of procedures to ensure high standards of integrity of its employees or persons acting on their behalf;

(b) on-going training programmes and capacity building sessions to ensure that the requirements under the Act, Regulations and Guidelines are well understood and implemented;

(c) a money laundering compliance function led by the money laundering reporting officer;

(d) an independent audit function to check compliance with the legal requirements;

(e) a strong and sound internal control system.

(2) Timing and content of training for various sectors of staff will need to be adapted by individual market intermediaries for their own needs. The following shall be considered in frequency and content of the training -

(a) For new employees, a general appreciation of the background to money laundering, and the subsequent need for reporting of any suspicious transactions to the money laundering reporting officer should be provided to all new employees who will be dealing with customers or their transactions, irrespective of the level of seniority preferably within the first month of their employment. They should be made aware of the importance placed on the reporting of suspicions by the market intermediary, the legal requirement to report, and the personal statutory obligation in this respect.

(b) Members of staff who are dealing directly with the public are the first point of contact with potential persons engaged in money laundering and their efforts are therefore vital to the market intermediary's reporting system for such transactions. Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious.

(c) Those members of staff responsible for account opening and acceptance of new customers should receive the basic training given to front line staff. In addition, further training should be provided in respect of the need to verify a customer's identity and on the business' own account opening and customer verification procedures. They should also be familiarized with the business' suspicious transaction reporting procedures.

(d) A higher level of instruction covering all aspects of money laundering procedures should be provided to those with the responsibility for supervising or managing staff. This will include the offences and penalties arising for non-reporting and for assisting persons engaged in money laundering, procedures relating to the service of production and restraint orders, internal reporting procedures and the requirements for verification of identity and the retention of records and disclosure of suspicious transaction reports.

(e) For the money laundering reporting officer, an in-depth training covering all aspects of the legislation and internal policies will be required. In addition, the money laundering reporting officer will require extensive initial and on-going instruction on the validation,

investigation and reporting of suspicious transactions and on the feedback arrangements and on new trends and patterns of criminal activity.

(3) A market intermediary shall develop appropriate compliance management arrangements, including at least, the appointment of a money laundering reporting officer.

Audit.

15. A market intermediary shall maintain an independent and adequately resourced audit function which is able to regularly assess the effectiveness of the market intermediary's internal policies, procedures and controls, and its compliance with regulatory requirements.

Tipping off.

16. (1) It is an offence for anyone who knows, suspects or has reasonable grounds to suspect that a disclosure has been made, or that the authorities are acting, or are proposing to act, in connection with an investigation into money laundering or terrorist financing, to inform the person who is the subject of a suspicion, or any third party of the disclosure, action or proposed action.

(2) Preliminary enquiries of a customer in order to verify his identity or to ascertain the source of funds or the precise nature of the transaction being undertaken may not trigger a tipping off offence before a suspicious transaction report has been submitted in respect of that customer unless the enquirer knows that an investigation is underway or the enquiries are likely to prejudice an investigation.

(3) Where it is known or suspected that a suspicious transaction report has already been disclosed to the Financial Reporting Centre or other authorized agency and it becomes necessary to make further enquiries, great care shall be taken to ensure that a customer does not become aware that their identity has been brought to the attention of the authorities.

Reliance on third parties.

17. (1) A market intermediary may rely upon a third party to perform any part of the CDD measures specified in Part IV of the Regulations, subject to the criteria set out in Regulation 28. However, the ultimate responsibility for ensuring that CDD requirements are met remains with the market intermediary.

(2) For the avoidance of doubt, reliance on third parties does not apply to—

(a) outsourcing or agency relationships, where the agent is acting under a contractual arrangement with the market intermediary to carry out its CDD function. In such a situation the outsource or agent is to be regarded as synonymous with the market intermediary; and

(b) business relationships, accounts or transactions between market intermediaries for their clients.

(3) The reliance on third parties often occurs through introductions made by another member of the same financial services group, or in some jurisdictions from another market intermediary or third party.

(4) Categories of third party intermediaries which may be relied upon include—

(a) domestic intermediaries: market intermediaries may rely upon other domestic intermediaries, subject to such intermediaries also being reporting institutions under the Act and who are able to satisfy the market intermediary that they have adequate procedures in place to prevent money laundering.

(b) a market intermediary may only rely upon an overseas intermediary carrying on business or practicing in an equivalent jurisdiction where the intermediary—

(i) falls into one of the following categories of businesses or professions which are subject to that jurisdiction's anti-money laundering reporting obligations—

(aa) an institution that carries on a business similar to that carried on by the market intermediary;

(bb) a notary public;

(cc) an auditor, a chartered or certified accountant, or a tax advisor; and

(dd) a registered trust company carrying on trust business.

(ii) is required under the law of the jurisdiction concerned to be registered or licensed or is regulated under the law of that jurisdiction;

(iii) has measures in place to ensure compliance with anti-money laundering requirements.

(iv) is supervised for compliance with those requirements by an authority in that jurisdiction which performs functions similar to the Capital Markets Authority, the Retirement Benefits Authority, the Central Bank of Kenya, the Insurance Regulatory Authority or the Sacco Societies Regulatory Authority.

(5) Compliance with the requirements set out above for both domestic and overseas intermediaries shall require the market intermediary—

(a) to review the intermediary's AML policies and procedures; and

(b) to make enquiries concerning the intermediary's stature and regulatory track record and the extent to which any group's AML standards are applied and audited;

(c) after carrying out the actions set out in subparagraphs (a) and (b) to satisfy itself that the anti-money laundering legal framework applicable to the proposed third party is comparable to that applicable in Kenya and that the third party's legal framework is satisfactorily applied and observed by the third party.

Combating the financing of terrorism.

18. (1) Where relevant, the references to a "customer" in this paragraph include beneficial owners, beneficiaries and beneficial owners of beneficiaries.

(2) Market intermediaries shall, upon receipt from the Authority, keep updated the various resolutions passed by the United Nations Security Council (UNSC) on counter terrorism measures in particular the UNSC Resolutions 1267 (1999), 1373 (2001), 1718 (2006), 1988 (2011) and such other relevant Resolutions which require sanctions against individuals and entities belonging or related to the Taliban and the Al-Qaida organization among others.

(3) Market intermediaries shall maintain a database of names and particulars of listed persons in the UN Consolidated List and such lists as may be issued under Regulation 13 of the Prevention of Terrorism (Implementation of the United Nations Security Council Resolutions on Suppression of Terrorism) Regulations 2013 in relation to the domestic list by the Counter Financing of Terrorism Inter-Ministerial Committee.

(4) Market intermediaries shall ensure that the information contained in the database is updated and relevant, and made easily accessible to its employees at the head office, branch or subsidiary.

(5) Upon receipt of the designations or sanctions list from the Capital Markets Authority, market intermediaries shall conduct regular checks on the names of new customers, as well as regular checks on the names of existing customers and potential customers, against the names in the database. If there is any name match, market intermediaries shall take reasonable and appropriate measures to verify and confirm the identity of its customer.

(6) Once confirmation has been obtained, market intermediaries shall—

(a) immediately freeze the customer's funds or block the transaction, where applicable, if it is an existing customer without delay and without notice to the entity;

(b) within twenty four hours of detecting the funds and freezing them, file a suspicious transaction report with the FRC;

(c) reject the potential customer, if the transaction has not commenced; and

(d) inform the Authority and other relevant bodies.

(7) Market intermediaries shall submit a suspicious transaction report when there is an attempted transaction by any of the persons listed in the Consolidated List or lists issued by the Counter Financing of Terrorism Inter-Ministerial Committee under Regulation 13 of The Prevention of Terrorism (Implementation of the United Nations Security Council Resolutions on Suppression of Terrorism) Regulations, 2013.

(8) Market intermediaries shall ascertain potential matches with the Consolidated List to confirm whether they are true matches to eliminate "false positives". Market intermediaries shall make further inquiries from the customer or where relevant, the counter-party to assist in determining whether the match is a true match.

(9) Market intermediaries may consolidate their database with the other recognized lists of designated persons or entities issued by other jurisdictions.

Appendix I (para. 10(1))

Indicators of potential money laundering activities in the capital markets

I Customer due diligence

1. The customer provides the market intermediary with unusual or suspicious identification documents that cannot be readily verified or are inconsistent with other statements or documents that the customer has provided. This indicator may apply to account openings and to interaction subsequent to account opening, such as wire transfers.
2. During the account opening process, the customer refuses to provide information to complete CDD/KYC (e.g. occupation, prior financial relationships, etc.).
3. The customer, whether a person or entity, is reluctant to provide the market intermediary with complete information about the nature and purpose of the customer's business, prior financial relationships, anticipated account activity, the entity's officers and directors or business location.
4. The customer, whether a person or entity, is located in a jurisdiction that is known as a bank secrecy haven, a tax shelter or high-risk geographic locations.
5. The customer is reluctant to meet personnel from the market intermediary in person, is very secretive or evasive or becomes defensive when asked to provide more information.
6. The customer refuses to identify a legitimate source of funds or provides the market intermediary with information that is false, misleading, or substantially incorrect.
7. The customer engages in frequent transactions with money services businesses.
8. The customer's background, whether a person or entity, is questionable or does not meet expectations based on business activities.
9. The customer has no discernible reason for using the firm's service or, the firm's disadvantageous location does not discourage the customer.
10. The customer refuses to provide information regarding the beneficial owners of an account opened for an entity, or provides information that is false, misleading or substantially incorrect.
11. The customer's address is associated with multiple other accounts that do not appear to be related.
12. The customer has a history of changing financial advisors or using multiple firms or banks. This indicator is heightened when the customer uses firms located in numerous jurisdictions.
13. The customer is known to be experiencing extreme financial difficulties.
14. The customer is, or is associated with, a PEP or senior political figure.
15. The customer refuses to invest in more appropriate securities when those securities would require a more enhanced CDD/KYC procedure.
16. The customer with a significant history with the securities firm abruptly liquidates all of his or her assets in order to remove wealth from the jurisdiction.

17. The customer appears to be acting as a fiduciary for someone else but is reluctant to provide more information relating to whom he or she may be acting for.
18. The customer is publicly known to have criminal, civil or regulatory proceedings against him or her for crime, corruption or misuse of public funds or is known to associate with such persons. Sources for this information include news items or Internet searches.
19. The customer inquires as to how quickly he or she can liquidate accounts or earnings without explaining why or provides suspicious reasons for doing so.
20. The customer opens an account or purchases a product without any regard to loss, commissions or other costs associated with that account or product.
21. The customer has commercial or other types of relationships with risky persons or institutions.
22. The customer acts through intermediaries, such as money managers or advisers, in order not to have his or her identity registered.
23. The customer exhibits unusual concern with the securities firm's compliance with government reporting requirements or the firm's AML policies.
24. The customer is reluctant to provide the securities firm with information needed to file reports or fails to proceed with a transaction once asked for documentation or learns of any recordkeeping requirements.
25. The customer is interested in paying higher charges to the securities firm in order to keep some of his or her information secret.
26. The customer tries to persuade an employee of the securities firm not to file a required report or not to maintain required records.
27. The customer funds, deposits, withdraws or purchases financial or monetary instruments below a threshold amount in order to avoid any reporting or recordkeeping requirements imposed by the jurisdiction.
28. The customer requests that account openings and closings in his or her name or in the name of family members be done without producing a paper trail.
29. Law enforcement has issued search warrant to the market intermediary regarding a customer or account.

II Fund transfers and deposits

1. Wire transfers are sent to, or originate from, financial secrecy havens, tax shelters or high-risk geographic locations for instance jurisdictions known to produce narcotics or psychotropic drugs or related to terrorism, without an apparent business reason or connection to a securities transaction.
2. Wire transfers or payments from unrelated third parties whether foreign or domestic or where the name or account number of the beneficiary or remitter has not been supplied.

3. Many small, incoming wire transfers or deposits are made, either by the customer or third parties, using cheques, money orders or cash that are almost immediately withdrawn or wired out in a manner inconsistent with the customer's business or history.
4. Incoming payments made by third-party cheques or cheques with multiple endorsements.
5. Deposit of large amount of small-denomination currency to fund account or exchanges of small notes for bigger notes.
6. Wire transfer activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent business purpose.
7. The securities account is used for payments or outgoing wire transfers with little or no securities activities (e.g. account appears to be used as a depository account or a conduit for transfers).
8. The controlling owner or officer of a public company transfers funds into his personal account or into the account of a private company that he or she owns or that is listed as an authorized signatory.
9. Quick withdrawal of funds after a very short period in the account.
10. Transfer of funds to financial or banking institutions other than those from where the funds were initially directed, specifically when different countries are involved.
11. Transfers or journals between different accounts owned by the customer with no apparent business purpose.
12. Customer requests that certain payments be routed through nostro or correspondent accounts held by the market intermediary or sundry accounts instead of its own account.

III Unusual securities transactions and account activity

1. Transaction where one party purchases securities at a high price and then sells them at a considerable loss to another party. This may be indicative of transferring value from one party to another.
2. A customer's transactions include a pattern of sustained losses. This may be indicative of transferring value from one party to another.
3. The purchase and sale of non listed securities with a large price differential within a short period of time. This may be indicative of transferring value from one party to another.
4. Payments effected by administrators and asset managers in cash, bearer cheques or other transferable instruments without identifying who they are for or providing very little information regarding the underlying account holder or beneficiary.
5. A company uses cash to pay dividends to investors.
6. Use of shell companies to purchase public company shares, in particular if the public company is involved in a cash intensive business.
7. Transfer of assets without a corresponding movement of funds, such as through journaling or effecting a change in beneficial ownership.

8. A dormant account that suddenly becomes active without a plausible explanation (e.g. large cash deposits that are suddenly wired out).
9. A customer's transactions have no apparent economic purpose.
10. A customer who is unfamiliar with a financial product's performance and specifications but wants to invest in it nonetheless.
11. Transactions that show the customer is acting on behalf of third parties.
12. The purchase of long term investments followed by a liquidation of the accounts shortly thereafter, regardless of fees or penalties.
13. Transactions involving an unknown counterparty.
14. Large sum cash purchases of financial instruments and mutual funds holdings followed by instant redemption.

IV Activity that is inconsistent with the customer's business objective or profile

1. The customer's transaction patterns suddenly change in a manner that is inconsistent with the customer's normal activities or inconsistent with the customer's profile.
2. There are unusual transfers of funds or journaling among accounts without any apparent business purpose or among apparently unrelated accounts.
3. The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.
4. The customer's account is not used for its intended purpose.
5. The customer enters into a financial commitment that appears beyond his or her means.
6. The customer begins to use cash extensively.
7. The customer engaged in extremely complex transactions where his or her profile would indicate otherwise.
8. Customer's credit usage is in extreme amounts that do not correspond to his or her financial status or collateral, which is provided by an unrelated third-party.
9. The time zone in customer's location is not consistent with the times that the trades were executed, with no apparent business or other purpose, or there is a sudden change inconsistent with the customer's typical business activity.
10. A foreign based customer that uses domestic accounts to trade on foreign exchanges.
11. The customer exhibits a lack of concern about higher than normal transaction costs.
12. A customer-relationship with the market intermediary that does not appear to make economic sense, for example, a customer who carries out frequent large transactions which do not fit his economic background.
13. Transactions in which funds are withdrawn immediately after being deposited, unless the customer's business activities furnish a plausible reason for immediate withdrawal.
14. Transactions that cannot be reconciled with the usual activities of the customer, for example, switching from trading only lowly priced stocks to predominantly blue chips.

15. Sudden increase in intensity of transactions, without plausible reason, of what was previously a relatively inactive customer trading account.
16. Corporate finance transactions under consideration that do not make economic sense in respect of the business operations of the customer, particularly if the customer is not a listed company.
17. Unexpected repayment of a delinquent account without any plausible explanation.
18. Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.
19. Provision of margin collaterals in the form of large cash amounts.
20. Provision of funds for investment and fund management purposes in the form of large cash amounts.
21. Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity.
22. Large cash withdrawals from a previously dormant or inactive account or from an account which has just received an unexpected large credit from abroad.
23. Crediting of customer trust or margin accounts using cash and by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial.
24. Payments or deposits containing counterfeit notes or forged instruments.
25. Customers making large and frequent cash deposits but payments made from the account are mostly to individuals and firms not normally associated with their business.
26. A large amount of cash is withdrawn and immediately credited into another account.

V Rogue employees

1. The employee appears to be enjoying a lavish lifestyle that is inconsistent with his or her salary or position.
2. The employee is reluctant to take annual leave.
3. The employee is subject to intense job-related demands, such as sales or production goals that may make him more willing to engage in or overlook behaviour that poses AML risks.
4. The employee inputs a high level of activity into one customer account even though the customer's account is relatively unimportant to the organization.
5. The employee is known to be experiencing a difficult personal situation, financial or other.
6. The employee has the authority to arrange and process customer affairs without supervision or involvement of colleagues.
7. The management or reporting structure of the market intermediary allows an employee to have a large amount of autonomy without direct control over his or her activities.
8. The employee is located in a different country to his or her direct line of management, and supervision is only carried out remotely.

9. A management culture within the market intermediary focuses on financial reward over compliance with regulatory requirements.
10. The employee's supporting documentation for customers' accounts or orders is incomplete or missing.
11. Business is experiencing a period of high staff turnover or is going through significant structural changes.

Dated the 15th December, 2015.

JAMES NDEGWA,
Chairman,
Capital Markets Authority.

PAUL MUTHAURA,
Ag. Chief Executive,
Capital Markets Authority.

MR/8827378