# ANTI MONEY LAUNDERING POLICY
# ADOPTED BY KEYNOTE CAPITALS LIMITED

## INTRODUCTION

Money Laundering has become a big issue which each and every country is trying to combat. It is suspected that one of the ways of laundering money is through securities market transactions. Hence, pursuant to the recommendations made by the Financial Action Task Force (formed for combating money laundering), Government of India had notified the Prevention of Money Laundering Act in 2002. This Act forms the core of the legal frame work to combat money Laundering. Subsequently, Government of India had issued a Notification dated 1st July 2005 defining Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information, Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries under Anti Money Laundering The Government of India set up Financial Intelligence Unit-India (FIU-IND) on 18th November 2004 as an independent body to report directly to the Economic Intelligence Council (EIC) headed by the Finance Minister. FIU-IND has been established as the central national agency responsible for receiving, processing, analyzing and disseminating information relating to suspect financial transactions. FIU_IND is also responsible for coordinating and stretching efforts of national and international intelligence and enforcement agencies in pursuing the global efforts against money laundering and related crimes.

In view of this, SEBI had issued the Guidelines on Anti Money Laundering Standards vide their notification No.ISD/CIR/RR/AML/1/06 dated 18th January 2006. Vide letter No.ISD/CIR/RR/AML/2/06 dated 20th March 2006 SEBI had also issued the obligations of the intermediaries registered under Section 12 of SEBI Act, 1992.

The objective of the SEBI guidelines is that a registered intermediary and any of its representatives should implement, identify and discourage any money laundering or terrorist financing activities. The overriding principle is that the registered intermediary should be able to satisfy themselves that the measures taken by them are adequate, appropriate and follow the spirit of these measures and the requirements as enshrined in the Prevention of Money Laundering Act, 2002 (PMLA) and the Government of India Notification dated 1stJuly 2005.

As per these SEBI guidelines, all intermediaries have been advised to ensure that proper policy frameworks are put in place as per the Guidelines on Anti Money Laundering Standards notified by SEBI.

NSE and BSE vide their circular dated January 25, 2006 had suggested the criteria on which suspicious secondary market transactions can be identified by a SEBI registered broker. CDSL vide their circular dated November 13, 2007 had notified criteria for generating alerts

**Responsibilities of Keynote Capitals Limited :**

By virtue of being a SEBI Registered stock broker of BSE and NSE, Depository Participant of CDSL and Portfolio Manager, it is mandatory on the party of **KCL** to have appropriate Anti Money Laundering policy.

The objectives of this policy are**:**

a) To ensure that appropriate statement of policies and procedures, are issued, on a group
basis, wherever applicable, for dealing with money laundering and terrorist financing reflecting the current statutory and regulatory requirements.

b) The contents of these Guidelines are understood by all staff members.

c) The policies and procedures are reviewed regularly to ensure their effectiveness.

d) Customer acceptance policies and procedures, which are sensitive to the risk of money
laundering and terrorist financing are adopted.

e) Customer Due diligence (CDD), to the extent that is sensitive to the risk of money laundering and terrorist financing depending on the type of customer, business relationship or transactions is undertaken

f) Staff Members' awareness and vigilance to guard against money laundering and terrorist
financing is developed.

**Keynote Capitals Ltd** (**KCL**) has resolved that it would as an internal policy shall take adequate measures to prevent money laundering and shall make a frame-work to report cash and suspicious transactions FIU as per the guidelines of PMLA Rules, 2002.

**Compliance w.r.t. Principle Officer and adoption of written policy.**

We have appointed Mr. Vineet Suchanti as Principle Officer & Mr. Rakesh Choudhari as Designated Director under the provision of PMLA, 2014 and Registered with FIU-INDIA on their website. We have also adopted and implemented written guidelines prescribed under PMLA, 2002 and intimated the same to FIU-INDIA. It is the policy of the firm to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets.

**Principal Officer :**

Mr. Vineet Suchanti being the Principal Officer will be responsible for implementation and Compliance of the provisions of PMLA, 2002 and **KCL**'s AML Policy. Mr. Vineet Suchanti will be responsible for ensuring that **KCL** discharges their legal obligation against Money Laundering to report suspicious transactions to the concerned authorities. The Principal Officer will act as a central reference point and will play an active role in the identification and assessment of potentially suspicious transactions. The Principal Officer will constantly review the AML Policy of **KCL** covering the areas of identification/verification/acceptance of customers and the parameters of identification of suspicious transaction.

The Principal Officer will give an orientation to all the concerned staff of **KCL** on the guidelines of FIU/SEBI and the identification of Suspicious Transactions on a regular basis. Some of these suggested measures may not be applicable in every circumstance to each business activity. However, keeping in mind, the specific nature of its business, type of customer and transactions in each business division, **KCL** has to satisfy itself that the measures taken are adequate and appropriate to follow the spirit of these guidelines.

## Anti Money Laundering Policy & Procedures

The Guidelines under this policy, we have taken into account the requirements of the Prevention of the Money Laundering Act, 2002 as applicable to the intermediaries registered under Section 12 of the SEBI Act. The detailed guidelines in Part II have outlined relevant measures and procedures to prevent money laundering and terrorist financing.

In light of the above, senior management of the company is fully committed to establishing appropriate policies and procedures for the prevention of money laundering and terrorist financing and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. The senior management of the company :

(a) issue a statement of policies and procedures, on a group basis where applicable, for dealing with money laundering and terrorist financing reflecting the current statutory and regulatory requirements;

(b) ensures that the content of these Guidelines are understood by all

staff members;

(c) Regularly reviews the policies and procedures on prevention of money laundering and terrorist financing to ensure their effectiveness. Further in order to ensure effectiveness of policies and procedures, the person doing such a review is different from the one who has framed such policies and procedures;

(d) adopts customer acceptance policies and procedures which are sensitive to the risk of money laundering and terrorist financing;

(e) undertakes customer due diligence ("CDD") measures to an extent that is sensitive to the risk of money laundering and terrorist financing depending on the type of customer, business relationship or transaction; and

(f) develops staff members' awareness and vigilance to guard against money laundering and terrorist financing.

**Policies and procedures to combat Money Laundering covers:**

a. Communication of group policies relating to prevention of money laundering and terrorist financing to all management and relevant staff that handle account information, securities transactions, money and customer records etc. whether in branches, departments or subsidiaries;

b. Customer acceptance policy and customer due diligence measures, including requirements for proper identification;

c. Maintenance of records;

d. Compliance with relevant statutory and regulatory requirements;

e. Co-operation with the relevant law enforcement authorities,

including the timely disclosure of information; and

f. Role of internal audit or compliance function to ensure compliance with policies, procedures, and controls relating to prevention of money laundering and terrorist financing, including the testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front line staff of their responsibilities in this regard.

We have adopted written procedures to implement the anti money laundering provisions as envisaged under the Anti Money Laundering Act, 2002. Such procedures includes inter alia, the following three specific parameters which are related to **the overall 'Client Due Diligence Process':**

a. Policy for acceptance of clients

b. Procedure for identifying the clients

c. Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR)

## Customer Due Diligence

The customer due diligence ("CDD") measures comprise the following:

(a) Obtaining sufficient information in order to identify persons who beneficially own or control securities account. Whenever it is apparent that the securities acquired or maintained through an account are

beneficially owned by a party other than the client, that party should be identified using client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

(b) Verify the customer's identity using reliable, independent source documents, data or information;

(c) Identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the customer and/or the person on whose behalf a transaction is being conducted;

(d) Verify the identity of the beneficial owner of the customer and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c); and

(e) Conduct ongoing due diligence and scrutiny, i.e. perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the registered intermediary's knowledge of the customer, its business and risk profile, taking into account, where necessary, the customer's source of funds.

**Policy for acceptance of clients:**

We have developed a customer acceptance policies and procedures that aim to identify the types of customers that are likely to pose a higher than the average risk of money laundering or terrorist financing. By establishing such policies and procedures, they will be in a better position to apply customer due diligence on a risk sensitive basis depending on the type of customer business relationship or transaction. In a nutshell, the following safeguards are followed while accepting the clients:

a) No account is opened in a fictitious / benami name or on an anonymous basis.

b) Factors of risk perception (in terms of monitoring suspicious transactions) of the client are clearly defined having regard to clients' location (registered office address, correspondence addresses and other addresses if applicable), nature of business activity, trading turnover etc. and manner of making payment for transactions undertaken. The parameters are enable to classify of clients into low, medium and high risk. Clients of special category (as given below) may, if necessary, be classified even higher. Such clients require higher degree of due diligence and regular update of KYC profile.

c) Documentation requirement and other information to be collected in respect of different classes of clients depending on perceived risk and having regard to the requirement to the Prevention of Money Laundering Act 2002, guidelines issued by RBI and SEBI from time to time.

d) Ensure that an account is not opened where the intermediary is unable to apply appropriate clients due diligence measures / KYC policies. This may be applicable in cases where it is not possible to ascertain the identity of the client, information provided to the intermediary is suspected to be non genuine, perceived non co-operation of the client in providing full and complete information. We do not continue to do business with such a person and file a suspicious activity report. We also evaluate whether there is suspicious trading in determining whether to freeze or close the account. We are cautious to ensure that it does not return securities of money that may be from suspicious trades.

e) The circumstances under which the client is permitted to act on behalf of another person / entity are clearly laid down. It should be specified in what manner the account should be operated, transaction limits for the operation, additional authority required for transactions exceeding a specified quantity / value and other appropriate details. Further the rights and responsibilities of both the persons (i.e the agent- client registered with the intermediary, as well as the person on whose behalf the agent is acting should be clearly laid down). Adequate verification of a person's authority to act on behalf the customer should also be carried out.

f) Necessary checks and balance to be put into place before opening an account so as to ensure that the identity of the client does not match with any person having known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency

worldwide.

## Risk-based Approach

It is generally recognized that certain customers may be of a higher or lower risk category depending on circumstances such as the customer's background, type of business relationship or transaction etc. As such, the registered intermediaries should apply each of the customers due diligence measures on a risk sensitive basis. The basic principle enshrined in this approach is that the registered intermediaries should adopt an enhanced customer due diligence process for higher risk categories of customers. Conversely, a simplified customer due diligence process may be adopted for lower risk categories of customers. In line with the risk-based approach, the type and amount of identification information and documents that registered intermediaries should obtain necessarily depend on the risk category of a particular customer.

## Clients of special category (CSC):

Such clients include the following-

a. Non resident clients

b. High networth clients,

c. Trust, Charities, NGOs and organizations receiving donations

d. Companies having close family shareholdings or beneficial ownership

e. Politically exposed persons (PEP) of foreign origin

f. Current / Former Head of State, Current or Former Senior High profile politicians and connected persons (immediate family, Close advisors and companies in which such individuals have interest or significant influence)

g. Companies offering foreign exchange offerings

h. Clients in high risk countries (where existence / effectiveness of money laundering controls is suspect, where there is unusual banking secrecy, Countries active in narcotics production, Countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent, Countries against which government sanctions are applied, Countries reputed to be any of the following – Havens / sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent.

i. Non face to face clients

j. Clients with dubious reputation as per public information available etc.

## Client identification procedure:

- The 'Know your Client' (KYC) policy clearly spells out the client identification procedure to be carried out at different stages i.e. while establishing the intermediary – client relationship, while carrying out transactions for the client or when the intermediary has doubts regarding the veracity or the

adequacy of previously obtained client identification data

- We try and put in place necessary procedures to determine whether their existing/potential customer is a politically exposed person (PEP). Such procedures would include seeking additional information from clients, accessing publicly available information etc.

- We obtain senior management approval for establishing business relationships with Politically Exposed Persons. Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, registered intermediaries shall obtain senior management approval to continue the business relationship.

- We take reasonable measures to verify source of funds of clients identified as PEP.

- We obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.

- We observe due diligence in compliance with the Guidelines. Each original document is seen prior to acceptance of a copy.

- In case of Failure by prospective client to provide satisfactory evidence of identity, the same is noted and reported to the higher authority within the company.

- SEBI has prescribed the minimum requirements relating to KYC for certain class of the registered intermediaries from time to time as stated earlier in this para. Taking into account the basic principles enshrined in the KYC

norms which have already been prescribed or which may be prescribed by SEBI from time to time, all registered intermediaries should frame their own internal guidelines based on their experience in dealing with their clients and legal requirements as per the established practices. Further, the intermediary should also maintain continuous familiarity and follow-up where it notices inconsistencies in the information provided. The underlying objective should be to follow the requirements enshrined in the PML Act, 2002 SEBI Act, 1992 and Regulations, directives and circulars issued there under so that the intermediary is aware of the clients on whose behalf it is dealing.

- Every intermediary shall formulate and implement a client identification programme which shall incorporate the requirements of the Notification No. 9/2005 dated July 01, 2005 (as amended from time to time), which notifies rules for maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing of information and verification of records of the identity of the clients of the banking companies, financial institutions and intermediaries of securities market and such other additional requirements that it considers appropriate to enable it to determine the true identity of its clients. A copy of the client identification programme shall be forwarded to the Director, FIU- IND.

- It may be noted that while risk based approach may be adopted at the time of establishing business relationship with a client, no exemption from obtaining the minimum information/documents from clients as provided in the PMLA Rules is available to brokers in respect of any class of investors with regard to the verification of the records of the identity of clients.

## Record Keeping

We ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made there-under, PML Act, 2002 as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars.

We maintain such records as are sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour.

In case of any suspected drug related or other laundered money or terrorist property, the competent investigating authorities would need to trace through the audit trail for reconstructing a financial profile of the suspect account. To enable this reconstruction, registered intermediaries should retain the following information for the accounts of their customers in order to maintain a satisfactory audit trail:

(a) the beneficial owner of the account;

(b) the volume of the funds flowing through the account; and

(c) for selected transactions:

- the origin of the funds;
- the form in which the funds were offered or withdrawn, e.g. cash, cheques, etc.;

- the identity of the person undertaking the transaction;
- the destination of the funds;
- the form of instruction and authority.

Registered Intermediaries should ensure that all customer and transaction records and information are available on a timely basis to the competent investigating authorities. Where appropriate, they should consider retaining certain records, e.g. customer identification, account files, and business correspondence, for periods which may exceed that required under the SEBI Act, Rules and Regulations framed there-under PMLA 2002, other relevant legislations, Rules and Regulations or Exchange bye-laws or circulars.

We have put in place a system of maintaining proper record of transactions prescribed under Rule 3, notified under the Prevention of Money Laundering Act (PMLA), 2002 as mentioned below:

(i) all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;

(ii) all series of cash transactions integrally connected to each other which have been valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds rupees ten lakh;

(iii) all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;

(iv) all suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

**Information to be maintained**

We maintain and preserve the following information in respect of transactions referred to in Rule 3 of PMLA Rules:

I. the nature of the transactions;
II. the amount of the transaction and the currency in which it denominated;
III. the date on which the transaction was conducted; and
IV. the parties to the transaction.

**Retention of Records**

We have taken appropriate steps to evolve an internal mechanism for proper maintenance and preservation of such records and information in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities. Further, the records mentioned in Rule 3 of PMLA Rules have to be maintained and preserved for a period of ten years from the date of cessation of the transactions between the client and intermediary.

As stated in para 5.5, intermediaries are required to formulate and implement the client identification program containing the requirements as laid down in Rule 9 and such other additional requirements that it considers appropriate. The records of the identity of clients have to be maintained and preserved for a period of ten years from the date of cessation of the transactions between the client and intermediary.

Thus the following document retention terms should be observed:

(a) All necessary records on transactions, both domestic and international, should be maintained at least for the minimum

period prescribed under the relevant Act (PMLA, 2002 as well SEBI Act, 1992) and other legislations, Regulations or exchange bye-laws or circulars.

(b) Records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence should also be kept for the same period.

In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they should be retained until it is confirmed that the case has been closed.

## Monitoring of transactions

Regular monitoring of transactions is vital for ensuring effectiveness of the Anti Money Laundering procedures. This is possible only if the intermediary has an understanding of the normal activity of the client so that they can identify the deviant transactions / activities.

We give special attention to all complex, unusually large transactions / patterns which appear to have no economic purpose. The intermediary may specify internal threshold limits for each class of client accounts and pay special attention to the transaction which exceeds these limits.

The intermediary should ensure a record of transaction is preserved and

maintained in terms of section 12 of the PMLA 2002 and that transaction of suspicious nature or any other transaction notified under section 12 of the act is reported to the appropriate law authority. Suspicious transactions should also be regularly reported to the higher authorities / head of the department.

Further the compliance cell randomly examines a selection of transaction undertaken by clients to comment on their nature i.e. whether they are in the suspicious transactions or not.

## Suspicious Transaction Monitoring & Reporting

Intermediaries should ensure to take appropriate steps to enable suspicious transactions to be recognised and have appropriate procedures for reporting suspicious transactions. While determining suspicious transactions, intermediaries should be guided by definition of suspicious transaction contained in PML Rules as amended from time to time.

A list of circumstances which may be in the nature of suspicious transactions is given below. This list is only illustrative and whether a particular transaction is suspicious or not will depend upon the background, details of the transactions and other facts and circumstances:

a) Clients whose identity verification seems difficult or clients

appears not to cooperate

b) Asset management services for clients where the source of the funds is not clear or not in keeping with clients apparent standing /business activity;

c) Clients in high-risk jurisdictions or clients introduced by banks or affiliates or other clients based in high risk jurisdictions;

d) Substantial increases in business without apparent cause;

e) Unusually large cash deposits made by an individual or business;

f) Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;

g) Transfer of investment proceeds to apparently unrelated third parties;

h) Unusual transactions by CSCs and businesses undertaken by shell corporations, offshore banks /financial services, businesses reported to be in the nature of export-import of small items.

Any suspicion transaction should be immediately notified to the Money Laundering Control Officer or any other designated officer within the intermediary. The notification may be done in the form of a detailed report with specific reference to the clients, transactions and the nature /reason of suspicion. However, it should be ensured that there is continuity in dealing with the client as normal until told otherwise and the client should not be told of the report/suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or

more jurisdictions concerned in the transaction, or other action taken.

It is likely that in some cases transactions are abandoned / aborted by customers on being asked to give some details or to provide documents. It is clarified that intermediaries should report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

**Reporting to Financial Intelligence Unit-India**

In terms of the PMLA rules, intermediaries are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Hotel Samrat,
Chanakyapuri,
New Delhi-110021.
Website: http://fiuindia.gov.in

Intermediaries should carefully go through all the reporting requirements and formats enclosed with this circular. These requirements and formats are divided into two parts- Manual Formats and Electronic Formats. Details of these formats are given in the documents (Cash Transaction Report- version 1.0 and Suspicious Transactions Report version 1.0) which are also enclosed with this circular. These documents contain detailed guidelines on the compilation and manner/procedure of submission of the manual/electronic reports to FIU-IND. The related hardware and technical requirement for preparing reports in manual/electronic format, the related data files and data structures thereof are also detailed in these documents.

Intermediaries, which are not in a position to immediately file electronic reports, may file manual reports to FIU-IND as per the formats prescribed. While detailed instructions for filing all types of reports are given in the instructions part of the related formats, intermediaries should adhere to the following:

(a) The cash transaction report (CTR) (wherever applicable) for each month should be submitted to FIU-IND by 15th of the succeeding month.
(b) The Suspicious Transaction Report (STR) should be submitted within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion.
(c) The Principal Officer will be responsible for timely submission of CTR and STR to FIU-IND;
(d) Utmost confidentiality should be maintained in filing of CTR and STR to FIU-IND. The reports may be transmitted by speed/registered post/fax at the notified address.
(e) No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious transactions to be reported.

Intermediaries should not put any restrictions on operations in the accounts where an STR has been made. Intermediaries and their directors, officers and employees (permanent and temporary) should be prohibited from disclosing ("tipping off") the fact that a STR or related information is being reported or provided to the FIU-IND. Thus, it should be ensured that there is no tipping off to the client at any level.

## Designation of an officer for reporting of suspicious transactions

To ensure that the registered intermediaries properly discharge their legal obligations to report suspicious transactions to the authorities, the Principal Officer would act as a central reference point in facilitating onward reporting of suspicious transactions and for playing an active role in the identification and assessment of potentially suspicious transactions. Names, designation and addresses (including e-mail addresses) of 'Principal Officer' including any changes therein shall also be intimated to the Office of the Director-FIU. As a matter of principle, it is advisable that the 'Principal Officer' is of a sufficiently higher position and is able to discharge his functions with independence and authority.

## Employees' Hiring/Employee's Training/ Investor Education

### Hiring of Employees

We have adequate screening procedures in place to ensure high standards when hiring employees. We have identified the key positions within our organization structures having regard to the risk of money laundering and terrorist financing and the size of their business and ensure the employees taking up such key positions are suitable and competent to perform their duties.

### Employees' Training

We have an ongoing employee training programme so that the members of the staff are adequately trained in AML and CFT procedures. Training

requirements have specific focuses for frontline staff, back office staff, compliance staff, risk management staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind these guidelines, obligations and requirements, implement them consistently and are sensitive to the risks of their systems being misused by unscrupulous elements.

## Investors Education

Implementation of AML/CFT measures requires intermediaries to demand certain information from investors which may be of personal nature or which has hitherto never been called for. Such information can include documents evidencing source of funds/income tax returns/bank records etc. This can sometimes lead to raising of questions by the customer with regard to the motive and purpose of collecting such information. There is, therefore, a need for intermediaries to sensitize their customers about these requirements as the ones emanating from AML and CFT framework. Intermediaries should prepare specific literature/ pamphlets etc. so as to educate the customer of the objectives of the AML/CFT programme.