International Capital Markets Brokers Limited
Suite 305, Griffith Corporate Centre, Beachmont |P.O. Box 1510, Kingstown
Saint Vincent & the Grenadines
Support@icmbrokers.com
www.icmbrokers.com

Customer Identification and Due Diligence Procedures

Application of customer identification and due diligence procedures

The Company is obliged to apply customer due diligence measures in the following cases:

1. When establishing a business relationship

2. When carrying out an occasional transaction which:

(a) amounts to an amount equal to or higher than fifteen thousand euros (€15,000) whether the transaction is carried out in a single operation or in several operations which appear to be linked

Additional Measures in Verification regarding High Net worth Clients

- EUR50,000+ or equivalent, additional document(s) is required, and source of funds is being requested. The documents which the Company approve as source of funds are the following:

a) bank reference letter issued in last 6 months;
b) complete tax returns forms;
c) Bank Statements – Include one bank statement for each of the last two years for any bank accounts in which client maintained a substantial balance;
d) Audited Financial Statements - submit any financial statements that have been prepared for the investor personally or for the investor's business by verified accountants or auditors. If available, audited financial statements are preferred for corporate clients – legal entities;
e) Payslips;
f) any other document which can prove that the client obtained/earned legally the money deposited in the Company's accounts

- When there is a suspicion of money laundering or terrorist financing, regardless of the amount or any derogation, exemption or minimum threshold pursuant to the provisions of the Law;

- When there are doubts about the veracity or adequacy of previously obtained customer identification data;

Ways of applying customer due diligence and identification procedures

- The identification procedures and the customer due diligence measures include the following:

1. Identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

2. identifying the beneficial owner's identity and taking reasonable measures to verify that person's identity so that the Company is satisfied that it knows who the beneficial owner

is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer;

3. assessing and, depending on the case, obtaining information on the purpose and intended nature of the business relationship;

4. Conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the information and data in the possession of the Company in relation to the customer, the business and risk profile of the customer, including where necessary, relating to the source of funds and ensuring that the documents, data or information held are kept up-to-date;

5. Provided that, in the application of the measures referred to in point 1 and point 2 above, the Company shall also verify that any third person purporting to act on behalf of the customer is duly authorised by the customer for this purpose and identifies and verifies the identity of that person.

a. The Company applies each of the customer due diligence measures and identification procedures set out in subsection above but may determine the extent of such measures on a risk-sensitive basis taking into account at least the variables included in the Joint Guidelines. The Company must be able to demonstrate that the extent of the measures it applies are appropriate and proportionate in view of the risks of money laundering and terrorist financing it is exposed to.

b. Proof of Identity is satisfactory if:

i. It is reasonable possible to establish that the customer is the person he claims to be; and

ii. The person who examines the customer's evidence is satisfied, in accordance with the procedures followed under this Law, that the customer is actually the person he claims to be.

When to apply customer due diligence and identification procedures.

- The verification of the identity of the customer and the beneficial owner is performed before the establishment of a business relationship or the carrying out of the transaction.

The verification of the identity of the customer and the beneficial owner may be completed during the establishment of a business relationship, if this is necessary so as not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing occurring: Provided that in such a case the customer and beneficial owner identity verification procedures shall be completed as soon as possible after the initial contact and before any transactions take place.

In such cases, the Company shall be under strict obligation to fully justify and document the reasons why:

i. The verification of the Client/Beneficial Owner prior to the establishment of the business relationship would disrupt the normal conduct of business, and

ii. The risk of money laundering or terrorist financing is low.

The Company will implement:

Where the Company is unable to comply with the customer due diligence requirements laid down in section 5 it shall not carry out a transaction through a bank account, establish a business relationship or carry out the transaction, according to the case, shall terminate the business relationship and examines the possibility submitting a suspicious transaction report to the Unit in relation to the customer, in accordance with the provisions of this Manual.

- Customer due diligence requirements and identification procedures must be applied not only to all new customers but also to existing customers at appropriate times, on a risk-sensitive basis, among others, at times when the relevant circumstances of the customer change.

Obligation for customer identification and due diligence procedures

- The Company ensures that the customer identification records remain completely updated with all relevant identification data and information throughout the business relationship. The Company examines and checks, on a regular basis, the validity and adequacy of the customer identification data and information it maintains, especially those concerning high risk customers. The procedures and controls of our "Customer Acceptance Policy" also determine the timeframe during which the regular review, examination and update of the customer identification is conducted. The outcome of the said review is recorded in a separate note/form which should be kept in the respective customer file.

- Despite the provisions of section 5 and taking into consideration the level of risk, if at any time during the business relationship, the Company becomes aware that reliable or adequate data and information are missing from the identity and the economic profile of the customer, then takes all necessary action, by applying the customer identification and due diligence procedures according to the Law, to collect the missing data and information, the soonest possible, so as to identify the customer and update and complete the customer's economic profile.

- In additional to the section 5, the Company checks the adequacy of the data and information of the customer's identity and economic profile, whenever one of the following events or incidents occurs:

(a) an important transaction takes place which appears to be unusual and/or significant compared to the normal pattern of transactions and the economic profile of the customer;
(b) a material change in the customer's legal status and situation, such as:
   i. change of directors/secretary,
   ii. change of registered shareholders and/or beneficial owners,
   iii. change of registered office,
   iv. change of trustees,

v. change of corporate name and/or trading name,
vi. change of the principal trading partners and/or undertake new major business activities;

(c) a material change in the way and the rules the customer's account operates, such as:
i. change in the persons that are authorised to operate the account,
ii. application for the opening of new account for the provision of new investment services and/or financial instruments.

c. Transactions that favour anonymity

The Company shall pay special attention to every threat or danger for money laundering or terrorist financing which may result from products or transactions which may favour anonymity, and shall take measures, if needed, to prevent their use for such activities and to apply to the extent possible reasonable measures and procedures to face the dangers arising from technological developments and new financial products.
In the case of customers' transactions via the internet, phone, fax or other electronic means where the customer is not present so as to verify the authenticity of his signature or that he is the real owner of the account or that he has been properly authorised to operate the account, the Company applies reliable methods, procedures and control mechanisms over the access to the electronic means so as to ensure that it deals with the true owner or the authorised signatory to the account. Among other the following will be used:

- Customers' transactions via the phone: Personal questions like ID and/or passport number, client code, etc will be asked by responsible employee.

- Customers' transactions via Email/fax: Signature will be compared with sample signature provided by the customer

d. Failure or refusal to submit information for the verification of customers' identity

- Failure or refusal by a customer to submit, before the establishment of a business relationship or the execution of an occasional transaction, the requisite data and information for the verification of his identity and the creation of his economic profile, without adequate justification, constitutes elements that may lead to the creation of a suspicion that the customer is involved in money laundering or terrorist financing activities. In such an event, the Company does not proceed with the establishment of the business relationship or the execution of the occasional transaction while at the same time the AMLCO considers whether it is justified under the circumstances to submit a report to MOKAS
- If, during the business relationship, a customer fails or refuses to submit, within a reasonable timeframe, the required verification data and information according to section 5, the Company terminates the business relationship and closes all the accounts of the customer while at the same time examines whether it is justified under the circumstances to submit a report to MOKAS

Transaction examination for vulnerable and/or complex and/or unusually large transactions and/or all other unusual patterns of transactions which have no apparent economic or visible lawful purpose.

Taking into consideration the risks involved in cash transactions (deposits/withdrawals), the Company applies procedures and controls for preventing and monitoring of any such cases either for transactions involving the Company or transactions related with Company's clients.

In case of identification of a cash transaction the Company has in place procedures and controls to investigate and evaluate it.

Company's policy is not to accept cash deposits/withdrawals, apart from exceptional cases where no other method is available and same is approved by Company's Senior Management and/or the AMLCO. In addition, the Company shall return deposited funds, when the customer requests a withdrawal, in the same bank account / using the same method from which they originated.

In case of any cash transaction of more than EURO 10.000, this is reported to the AMLCO for further handling.

The Company has in place procedures and controls to ensure on a timely basis that no cash deposits/withdrawals have been contacted (both for own account and for client's bank accounts (i.e. management of client's bank accounts).More precisely:

(a) Cash Bank Transaction requests are duly evaluated from the Back-Office Department and where necessary the AMLCO;
(b) Client's Bank accounts are duly monitored through several accounting tools i.e. bank reconciliation, accounting services, management accounts, to ensure on a timely basis that no cash deposits/withdrawals have been contacted, and/or to identify cash transactions and take relevant action.
(c) The AMLCO monitors/examines regularly and on a sample basis (proportionate to clientele) bank statements and bank reconciliation reports to ensure that the above measures are duly implemented;
(d) AMLCO is responsible for the training of all staff in relation to Company's measures to cash transactions;
(e) AMLCO ensures that all relevant measures for monitoring and preventing cash transactions are known and implemented by all employees and same are reviewed periodically.
(f) In case of identification of a cash transaction the AMLCO is the person responsible to investigate and evaluate it:
    i. The AMLCO will assess whether the cash transaction is in line with client economic profile;
    ii. If needed the AMLCO will communicate with the client;
(g) The AMLCO shall investigate and evaluate the cash deposit/withdrawal and analyse the cash transaction by completing the relevant "Cash Transaction evaluation Form", which shall include the following data:
    - Date of notification of the cash transaction from the Back office or Accounting department
    - client name
    - client code/number
    - client country of origin and/or residency or incorporation (for legal entities)
    - date of establishment of business relationship
    - bank account number
    - name and location of the bank

- date of the cash deposit/withdrawal
- amount of the cash deposit/withdrawal
- means of cash transaction
- source and origin of cash transaction
- client's business activities
- client risk categorisation
- description (purpose of deposit/withdrawal)
- assess whether the cash transaction in line with client's economic profile
- decision whether the cash transaction is in line with client's economic profile and justification of the legality of the cash transaction
- decision whether to report or not to MOKAS in case the cash transaction is not in line with client's economic profile.

Construction of an economic profile

- Irrespective of the customer's type (e.g. natural or legal person, sole trader or partnership), the Company requests and obtains sufficient data and information regarding the customer's business activities and the expected pattern and level of transactions.

However, it is noted that no single form of identification can be fully guaranteed as genuine or representing correct identity and, consequently, the identification process will generally need to be cumulative.

- The verification of the customers' identification is based on reliable data and information issued or obtained from independent and reliable sources, meaning those data, and information that are the most difficult to be amended or obtained illicitly.

- A person's residential and business address is an essential part of his identity and, thus, a separate procedure for its verification

- It is never acceptable to use the same verification data or information for verifying the customer's identity and verifying its home address.

- The data and information that are collected before the establishment of the business relationship, with the aim of constructing the customer's economic profile and, as a minimum, include the following.

(a) the purpose and the reason for requesting the establishment of a business relationship;

(b) the anticipated account turnover, the nature of the transactions, the expected origin of incoming funds to be credited in the account and the expected destination of outgoing transfers/payments;

(c) the customer's size of wealth and annual income and the clear description of the main business/professional activities/operations.

- The data and information that are used for the construction of the customer's-legal person's economic profile include, *inter alia*, the name

of the company, the country of its incorporation, the head offices address, the names and the identification information of the beneficial owners, directors and authorised signatories, financial information, ownership structure of the group that the company may be a part of (country of incorporation of the parent company, subsidiary companies and associate companies, main activities and financial information). The said data and information are recorded in a separate form designed for this purpose which is retained in the customer's file along with all other documents as well as all internal records of meetings with the respective customer. The said form is updated regularly or whenever new information emerges that needs to be added to the economic profile of the customer or alters existing information that makes up the economic profile of the customer.

Identical data and information with the above mentioned are obtained in the case of a customer-natural person, and in general, the same procedures with the above mentioned are followed.

- Transactions executed for the customer are compared and evaluated against the anticipated account's turnover, the usual turnover of the activities/operations of the customer and the data and information kept for the customer's economic profile. Significant deviations are investigated, and the findings are recorded in the respective customer's file. Transactions that are not justified by the available information on the customer, are thoroughly examined so as to determine whether suspicions over money laundering or terrorist financing arise for the purposes of submitting an internal report to the AMLCO.

- The information regarding the Client's Economic Profile and Identification is collected by the Client Account opening Questionnaire

Simplified Customer Identification and Due Diligence Procedures

- The Company, may apply simplified customer due diligence measures if the business relationship or the transaction presents a lower degree of risk. It is provided that the Company collects sufficient information, so as to assess and to ascertain whether a business relationship or transaction presents a lower degree of risk. The Company when assessing the abovementioned pays special attention to any activity of those customers or to any type of transactions, which may be regarded as particularly likely, by its nature, to be used or abused for money laundering or terrorist financing purposes.

- SDD is not an exemption from any of the CDD measures. However, the Company may adjust the amount, timing or type of each or all of the CDD measures in a way that is commensurate to the low risk it has identified.

- SDD does not exempt the Company from reporting suspicious transactions to the Unit. It is provided that the Company shall carry out

sufficient
monitoring of the transactions and the business relationships to enable the detection of unusual or suspicious transactions.

- Where there are indications that the risk may not be low, for example where there are grounds to suspect that ML/TF is being attempted or where the Company has doubts about the veracity of the information obtained, SDD must not be applied. Equally, where specific high-risk scenarios apply and there is an obligation to conduct EDD, SDD shall not be applied.

- When assessing the risks of money laundering or terrorist financing which relate to types of customers, geographical areas and particular products, services, transactions or delivery channels, the Company shall take into account at least the factors of potentially lower risk situations

- The Company considers that the following factors (the list is not exhaustive) may decrease risk:

a) Involvement of financial institutions or other obliged entities which are regulated in their home jurisdiction and subject to appropriate AML/CFT regulation.

b) Role or oversight of a regulator or multiple regulators (e.g. regulating obliged entities, trustees or any other person exercising effective control).

c) The regularity or duration of the client relationship. Long-standing relationships involving frequent client contact throughout the relationship may present less risk. In addition, a relationship may present less risk where, for example, the Company provides an integrated service, including acting as or providing trustees or directors of the trust, company or other legal entity and responsibility for preparation of accounts or maintaining the books and financial records of such trust, company or other legal entity.

d) Trusts, companies or other legal entities that are transparent and well-known in the public domain.

e) Listed entities and other business arrangements, such as pension trusts and employee benefit trusts and other trusts used for commercial purposes.

f) Company's familiarity with a particular country, including knowledge of local laws and regulations as well as the structure and extent of regulatory oversight.

- SDD measures the Company may apply include but are not limited to adjusting the timing of CDD, for example where the product or transaction sought has features that limit its use for ML/TF purposes, for example by:

i. verifying the customer's or beneficial owner's identity during the establishment of the business relationship; or

ii. verifying the customer's or beneficial owner's identity once transactions exceed a defined threshold or once a reasonable time limit has lapsed. The Company shall make sure that:

a. this does not result in a de facto exemption from CDD, that is, the Company shall ensure that the customer's or beneficial owner's identity will ultimately be verified;
b. the threshold or time limit is set at a reasonably low level (although, with regard to terrorist financing, the Company shall note that a low threshold alone may not be enough to reduce risk);
c. it has systems in place to detect when the threshold or time limit has been reached; and
d. it does not defer CDD or delay obtaining relevant information about the customer where applicable legislation, require that this information be obtained at the outset.

iii. adjusting the quantity of information obtained for identification, verification or monitoring purposes, for example by:

a. verifying identity on the basis of information obtained from one reliable, credible and independent document or data source only; or

b. assuming the nature and purpose of the business relationship because the product is designed for one particular use only, such as a company pension scheme or a shopping centre gift card, or based on the type of transaction carried out.

iv. adjusting the quality or source of information obtained for identification, verification or monitoring purposes, for example by:

a. accepting information obtained from the customer rather than an independent source when verifying the beneficial owner's identity (note that this is not permitted in relation to the verification of the customer's identity); or

b. where the risk associated with all aspects of the relationship is very low, relying on the source of funds to meet some of the CDD requirements, for example where the funds are state benefit payments or where the funds have been transferred from an account in the customer's name at an EEA firm.

v. adjusting the frequency of CDD updates and reviews of the business relationship, for example carrying these out only when trigger events occur such as the customer looking to take out a new product or service or when a certain transaction threshold is reached. The Company shall make sure that this does not result in a de facto exemption from keeping CDD information up-to-date

vi. adjusting the frequency and intensity of transaction monitoring, for example by monitoring transactions above a certain threshold only. Where the Company choose to do this, it shall ensure that the threshold is set at a reasonable level and that it has systems in place to identify linked transactions that, together, would exceed that threshold.

e. Enhanced customer identification and due diligence procedures

- The Company applies enhanced customer identification and due diligence procedures in respect of the customers referred to in section 64 of the Law, situations referred to in subsections 5.1, 5.2, 5.3 and 5.4 of the Manual, as well as in other situations, that pose a high level of risk for money laundering or terrorist financing and are classified by the Company as high risk on the basis of its section 6 "Customer Acceptance Policy" .

- The Company examines, as far as reasonably possible, the background and purpose of all complex and unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. In particular, the Company shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear suspicious.

- Examples of Enhance Due Diligence include:

1. Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.
2. Obtaining additional information on the intended nature of the business relationship.
3. Obtaining information on the source of funds or source of wealth of the customer.
4. Obtaining information on the reasons for intended or performed transactions.
5. Obtaining the approval of senior management to commence or continue the business relationship.
6. Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
7. Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards

f. Reliance on third parties for customer identification and due diligence purposes

Without prejudice to the provisions of section 67 of the Law, the Company may rely on third parties for the implementation of customer identification and due diligence procedures, as these are prescribed in section 61(1)(a),(b) and (c) of the Law, provided that the third person (a) makes immediately available all data and information, which must be certified true copies of the originals, that were collected in the course of applying customer identification and due diligence procedures and (b) forward immediately to the Company, copies of these documents and relevant data and information on the identity of customer or the beneficial owner which the third party collected when applying the above procedures and measures.

It is provided that, the ultimate responsibility for meeting the above-mentioned measures and procedures shall remain with the Company

- The Company obtains data and information so as to verify that the third person is subject to professional registration in accordance with the competent law of its country of incorporation and/or operation as well as supervision for the purposes of compliance with the measures for the prevention of money laundering and terrorist financing.

- The Company may rely on third parties only at the outset of establishing a business relationship or the execution of an occasional transaction for the purpose of verifying the identity of their customers. According to the degree of risk any additional data and information for the purpose of updating the customer's economic profile or for the purpose of examining unusual transactions executed through the account, is obtained from the natural persons (directors, beneficial owners) who control and manage

the activities
of the customer and have the ultimate responsibility of decision making as regards to the management of funds and assets.

- In the case where the Company relies on a third party, applies the following measures/procedures:

(a) before the establishment of the business relationship or the carrying out of the occasional transaction applies due diligence measures to the third party;

(b) sign an agreement with the third party specifying the obligations of each party;

(c) maintains a separate file for every third party of the present paragraph, where it stores the relevant information.

The commencement of the cooperation with the third person and the acceptance of customer identification data verified by the third person is subject to approval by the AMLCO, according to subsection 3.2, point (l) above.

Note: The Company should not rely on third parties established in high-risk third countries.

g. Ongoing monitoring of accounts and transactions

Risk Assessment is not a static event of a limited duration or an event that happens only once. An effective risk assessment has to be dynamic and on-going. The Company has to ensure that it revises the existing procedures when there are significant developments within the environment it is operate in and within its business structures/activities. Such changes may lead to exposure to new ML/TF risks for the Company. Frequent revision of the risk assessment allows Company to take action to ensure that its measures, policies, controls and procedures are robust enough to cater for these.

The Company shall monitor and evaluate, on an ongoing basis, the effectiveness of the measures and procedures that have been introduced, with the aim of ensuring that the evaluations and assessments made remain current and that the procedures put in place remain suitable and appropriate for the assessed level of ML/TF risk. Any changes in the client's pattern of activity must be assessed to determine whether an update of the client's profile or risk categorisation is necessary.

In cases where the substance of a business relationship changes significantly, the Company should perform additional CDD procedures to identify and subsequently mitigate the money laundering and terrorist financing risks involved. If the revised risk is not in line with Company's Client Acceptance, then consideration should be made to terminate the business relationship.

Changes in the terms of a business relationship with clients may include amongst others, the following:

a. Changes in the shareholding structure
b. Changes in the activities or turnover of a client that do not have commercial rationale
c. Enquiries and provision of new higher risk services
d. Changes in the nature of transactions of a client that cannot be explained
e. Set up of new corporate structures

Additionally, the Company shall periodically assess information obtained as part of its ongoing monitoring of a business relationship and consider whether this information affects the risk assessment.

The Company shall keep its assessments of the ML/TF risk associated with individual business relationships and occasional transactions as well as of the underlying factors under review to ensure its assessment of ML/TF risk remains up to date and relevant. The Company shall assess information obtained as part of its ongoing monitoring of a business relationship and consider whether this affects the risk assessment.

The Company shall conduct ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the information and data in the possession of the Company in relation to the customer, the business and risk profile of the customer, including where necessary, relating to the source of funds and ensuring that the documents, data or information held are kept up-to-date with a view to understanding whether the risk associated with the business relationship has changed;

The Company shall conduct detailed examination of each transaction which by its nature may be considered to be particularly vulnerable to be associated with money laundering offences or terrorist financing and in particular complex or unusually large transactions and all other unusual patterns of transactions which have no apparent economic or visible lawful purpose.

When examining transactions, the Company shall consider the following factors (the list is not exhaustive):

a. Geographical source/destination of funds
b. High or inconsistent amounts
c. Numerous small transactions that when combined they exceed anticipated threshold
d. Nature or type of individual transactions or series of transactions
e. Clients' usual pattern of activities or size of turnover
f. Changes in the usual method of communication with client
g. STRs or SARs

The Company has a full understanding of normal and reasonable account activity of their customers as well as of their economic profile and have the means of identifying transactions which fall outside the regular pattern of an account's activity or to identify complex or unusual transactions or transactions without obvious economic purpose or clear legitimate reason. Without such knowledge, the Company is not able to discharge its legal obligation to identify and report suspicious transactions to MOKAS, according to subsection 3.2 point (5) and section 7 of this Manual.

The Company shall record and document its risk assessments of business relationships, as well as any changes made to risk assessments as part of its reviews and monitoring, to ensure that it can demonstrate to the competent authorities that its risk assessments and associated risk management measures are adequate.

The Company shall ensure that it has systems and controls in place to identify emerging ML/TF risks and that it can assess these risks and, where appropriate, incorporate them into its business-wide and individual risk assessments in a timely manner.

Examples of systems and controls the Company shall put in place to identify emerging risks include:

a. Processes to ensure that internal information is reviewed regularly to identify trends and emerging issues, in relation to both individual business relationships and the Company's business.

b. Processes to ensure that the Company regularly reviews relevant information sources such as those specified in Company's Customer Acceptance Policy. This should involve, in particular:
   i. regularly reviewing media reports that are relevant to the sectors or jurisdictions in which the Company is active;
   ii. regularly reviewing law enforcement alerts and reports;
   iii. ensuring that the Company becomes aware of changes to terror alerts and sanctions regimes as soon as they occur, for example by regularly reviewing terror alerts and looking for sanctions' regime updates; and
   iv. regularly reviewing thematic reviews and similar publications issued by competent authorities.

c. Processes to capture and review information on risks relating to new products.#

d. Engagement with other industry representatives and competent authorities (e.g. round tables, conferences and training providers), and processes to feed back any findings to relevant staff.

e. Establishing a culture of information sharing within the Company and strong company ethics. Examples of systems and controls the Company shall put in place to ensure its individual and business-wide risk assessments remains up to date may include:

   i. Setting a date on which the next risk assessment update will take place, for example on 1 March every year, to ensure new or emerging risks are included in risk assessments. Where the Company is aware that a new risk has emerged, or an existing one has increased, this should be reflected in risk assessments as soon as possible.
   ii. Carefully recording issues throughout the year that could have a bearing on risk assessments, such as internal suspicious transaction reports, compliance failures and intelligence from front office staff.
   iii. Subscribe to receive alerts on changes of the EU/US/UN Sanctions lists.
   iv. Subscribe to a reputable database and screen clients at regular intervals.
   v. Reviewing media reports that are relevant to the sectors or jurisdictions in which the Company operates/has clients.
   vi. Monitor papers issued by the regulation and other competent authorities.
   vii. Participate in relevant seminars and trainings.
   viii. Review the National and the Supranational Risk Assessment Reports.

Like the original risk assessments, any update to a risk assessment and adjustment of accompanying CDD measures should be proportionate and commensurate to the ML/TF risk.

The Company shall take steps to ensure that its risk management systems and controls, in particular those relating to the application of the right level of CDD measures, are effective and proportionate.

Ongoing monitoring shall be proportional to the risk profile of the client. The higher the risk of a client the more frequent and more rigorous the monitoring procedures should be. Particular attention on ongoing monitoring procedures must be paid in client relationships where a PEP is involved or where a client has any links or relationships with high risk countries. By adopting a proportional to risk approach, the Company can utilise its resources more effectively.

Despite the proportionality principle mentioned above, it must be noted that ongoing monitoring should take place for all client relationships including low risk clients and clients for which Simplified

Due Diligence measures were adopted.
What can be altered accordingly is the frequency and extent of the ongoing monitoring.

The procedures and intensity of monitoring accounts and examining transactions are based on the level of risk and, as a minimum, achieve the following:

(a) identifying all high-risk customers according to subsection 2.3 of this Manual. Therefore, the systems or the measures and procedures of the Company are able to produce detailed lists of high-risk customers so as to facilitate enhanced monitoring of accounts and transactions;

(b) detecting of unusual or suspicious transactions that are inconsistent with the economic profile of the customer for the purposes of further investigation;

(c) the investigation of unusual or suspicious transactions from the employees who have been appointed for that purpose; the results of the investigations are recorded in a separate memo and kept in the file of the customer concerned;

(d) detecting transactions which fall outside the regular pattern of an account's activity;

(e) detecting complex transactions;

(f) detecting transactions without obvious economic purpose or clear legitimate reason;

(g) identify cash transactions.

(h) all necessary measures and actions must be taken, based on the investigation findings of point (c), including any internal reporting of suspicious transactions/activities to the AMLCO, according to subsection 3.2 point (5);

(i) ascertaining the source and origin of the funds credited to accounts

Transactions executed for the customer shall be compared and evaluated against:

- The anticipated account's turnover
- The usual turnover of the activities/operations of the customer
- The data and information kept for the customer's economic profile.

Significant deviations shall be investigated, and the findings shall be recorded in the respective customer's file. Transactions that are not justified by the available information on the customer, shall be thoroughly examined so as to determine whether suspicions over money laundering or terrorist financing arise for the purposes of submitting an internal report to the AMLCO and then by the latter to MOKAS, if required.

The AMLCO shall examine and check, on a regular basis the validity and adequacy of the customer identification data and information it maintains (especially for high risk customers). The frequency of the checks is as follows:

- Every 1 years for High risk customers
- Every 2 years for Normal risk customers
- Every 3 years for Low risk customers

The Company will consider to introduce and implement, where appropriate and proportionate, in view of the nature, scale and complexity of its business and the nature and range of the investment services

and activities undertaken in the course of
that business, adequate automated electronic management information systems which will be capable of supplying the board of directors and the AMLCO, on a timely basis, all the valid and necessary information for the identification, analysis and effective monitoring of customer accounts and transactions based on the assessed risk for money laundering or terrorist financing purposes.

The monitoring of accounts and transactions shall be carried out in relation to specific types of transactions and economic profile, as well as by comparing periodically the actual movement of the account with the expected turnover as declared at the establishment of the business relationship. Furthermore, the monitoring shall cover customers who do not have a contact with the Company as well as dormant accounts exhibiting unexpected movements.

The automated electronic management information systems may be also used to extract data and information that is missing regarding the customer identification and the construction of a customer's economic profile.

For all accounts, automated electronic management information systems shall be able to add up the movement of all related accounts on a consolidated basis and detect unusual or suspicious activities and types of transactions. This can be done by setting limits for a particular type, or category of accounts (e.g. high risk accounts) or transactions (e.g. deposits and withdrawals in cash, transactions that do not seem reasonable based on usual business or commercial terms, significant movement of the account incompatible with the size of the account balance), taking into account the economic profile of the customer, the country of his origin, the source of the funds, the type of transaction or other risk factors. The Company gives particular attention to transactions exceeding the abovementioned limits, which may indicate that a customer might be involved in unusual or suspicious activities.