ATONLINE LIMITED

Anti-Money Laundering (AML) Policy

Relevant to:		
☑	**ALL DEPARTMENTS / EMPLOYEES**	
		Own Account Dealing
		Brokerage Department
		Investment Advice Department
		Corporate Finance Department
		Research Department
		Operations (Back Office)
		Accounting Department

Document Information					
Status:	FINAL	**Version:**	3	**Last Updated On:**	14 September 2017
Prepared By:	Pavels Mitins, AML Compliance Officer				
	Irina Grekova, Compliance Officer				
Approved By:	Board of Directors at a meeting that took place on 19th September 2017				
Submitted to CySEC:					

ATONLINE LIMITED

Anti-Money Laundering (AML) Policy

Table of Contents

Definitions

"**Beneficial Owner**": is defined as the natural person(s) who ultimately owns or controls the customer and / or the natural person on whose behalf a transaction or activity is being conducted.

"**Firm**": means Atonline Limited.

"**Money Laundering**": shall mean the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities and /or to legalize the possession and the use of such proceeds.

"**Politically Exposed Persons (PEPs)**": these are defined as natural persons who are or have been entrusted with prominent public functions* and immediate family members**, or persons known to be close associates***, of such persons. According to European Directive 2007/70/EC, where a person has ceased to be entrusted with a prominent public function for a period of at least one year, Investment Firms shall not be obliged to consider such a person as politically exposed.

* "prominent public functions" include:
  a. heads of State, heads of government, ministers and deputy or assistant ministers
  b. members of parliaments
  c. members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances
  d. members of courts of auditors or of the boards of central banks
  e. ambassadors, chargés d'affaires and high-ranking officers in the armed forces
  f. members of the administrative, management or supervisory bodies of State-owned enterprises

** "immediate family members" include:
  a. the spouse or the person with which cohabit for at least one year
  b. any partner considered by national law as equivalent to the spouse
  c. the children and their spouses or the persons with which cohabit for at least one year
  d. the parents

*** "persons known to be close associates" include:
  a. any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a Politically Exposed Person
  b. any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of a Politically Exposed Person

"**Predicate offences**": are defined as:
  a. Criminal offences punishable with terms of imprisonment exceeding one year
  b. Terrorist financing offences
  c. Offences associated with the trafficking of narcotics

"**Shell bank**": means a credit institution, or an institution engaged in equivalent activities, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group.

"**Suspicious transactions"**: any transactions that bear some of the traits of possible attempts to launder money or finance terrorist activities.

"**Terrorist financing**": it is defined as the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part any of the terrorist offences defined in Council Framework Decision 2002/475/JHA.

"**Unit for Combating Money Laundering**" / "MOKAS" (hereinafter – "UCML"): shall mean the department in the Office of the Attorney General of the Republic of Cyprus, taking measures of the preventing legalization of the criminal proceeds.

ATONLINE LIMITED

Anti-Money Laundering – Firm principles and policy

As part of our commitment to maintaining the highest ethical standards, and to adhering to all relevant regulations, it is the Firm's policy to prohibit and actively prevent money laundering and terrorist financing. This commitment includes not only the direct laundering of money, but any activity that facilitates money laundering as well as the funding of terrorist or criminal activities.

Legal Framework

a. Relevant Legislation

Our Anti-Money Laundering policy is underpinned and defined by the following Legislation:

- European Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing as transposed into National Law (L188(I)/2007)
- European Directive 2004/39/EC (known as Markets in Financial Instruments Directive "MiFID)
- European Directive 2006/73/EC implementing MiFID as regards organizational requirements and operating conditions for investment firms and defined terms of the purposes of that Directive
- Directive 144-2007-08 issued by the Cyprus Securities and Exchange Commission (CySEC), as amended from time to time
- Any other Directives and Circulars issued by CySEC, the Unit for Combating Money Laundering (UCML) and any other authority entrusted with the task of combating Money Laundering

b. Applicable Legislation for Branches

In the case of Branches situated in other European Economic Area jurisdictions, even though the Host Member State authorities do retain certain rights in respect of the prevention of Money Laundering, (the most prominent one being the obligation to appoint a Money Laundering Reporting Officer responsible for reporting any suspicions of money laundering or terrorist financing to the relevant competent authorities of the Host Member State), it is the Anti-Money Laundering legal regime of the Home Member State that applies.

c. Subject Matter of the Law, Scope, Definitions and Penalties

According to Article 4(1) of L188(I)/2007, it is a crime for any person who either knows or at the material time ought to have known that such property is derived from predicate offences or from an act of participation in such offences, and proceeds to:

Money Laundering Offences

a) the conversion or transfer of property for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action;
b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property;
c) the acquisition, possession or use of property;
d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counseling the commission of any of the actions mentioned in the foregoing points.

Money laundering is punishable with 14 years imprisonment and / or a fine of up to €500.000.

Tipping-Off

The provision of information in relation to money laundering investigations to enable the person who benefited from the commitment of predicate offences to keep the proceeds or control over the proceeds of such offences.

Tipping –off is punishable with up to 5 years imprisonment
It should be noted that:

- Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.
- Knowledge, intent or purpose required as an element of the activities mentioned hereabove may be inferred from objective factual circumstances, which reduces the onus of proof for the commitment of such offences.

Stages of Money Laundering

The main money laundering stages are:

1. **Placement**: cash are placed into the financial system or retail economy or are smuggled out of the country. The aims of the launderer are to remove the cash from the location of acquisition so as to avoid detection from the authorities and to then transform it into other asset forms for example: travellers cheques or postal orders
2. **Layering**: is the first attempt at concealment or disguise of the source of the ownership of the funds by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity
3. **Integration**: the money is integrated into the legitimate economic and financial system and is assimilated with all other assets in the system. Integration of the "cleaned" money into the economy is accomplished by the launderer making it appear to have been legally earned

Board of Directors responsibilities[1]

The Firm's Board of Directors (the "BoD") is responsible for determining, recording and approving the Firm's general policy principles in relation to the Prevention of Money Laundering and Terrorist Financing. The BoD is also responsible for the appointment of the Firm's Anti-Money Laundering Compliance Officer(s) and for establishing their duties and responsibilities, which should be clearly stated in the Firm's Operations Manual.

Further responsibilities of the BoD include, among others:

a) the approval of the Risk Management Manual for the Prevention of Money Laundering and Terrorist Financing, which is dully communicated to all employees who are responsible for handling client financial instruments and funds
b) the positioning of appropriate and effective systems and processes in order to achieve compliance with any rules and regulations
c) in order to warrant that the Compliance Officer is in a position to perform the duties and responsibilities assigned to him / her effectively, the Board ensures that the compliance officer, has full access to all information and identification information of customers, transactions and other documents, records and information held by the Firm
d) the evaluation and approval of the Annual Report for the Prevention of Money Laundering and Terrorist Financing and the taking of all appropriate measures to correct any deficiencies identified within the Report

Internal Auditor's responsibilities

As an additional safeguard that appropriate AML measures are applied, article 6 of Directive 144-2007-08 provides that the internal audit department of the Firm reviews and evaluates, at least on an annual basis, the appropriateness, effectiveness and adequacy of the policy, practices, measures, procedures and control mechanisms applied for the prevention of money laundering and terrorist financing.

The findings and observations of the internal auditor are submitted, in a written report form, to the Board of Directors which decides the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies which have been detected. The minutes of the abovementioned decision of the board of directors and the internal auditor's report are submitted to the Commission at the same frequency and manner provided for the Compliance annual report.

[1] Paragraph 5 of Directive 144-2007-08

AML Compliance Officer Designation and Duties[2]

Main Duties

The Firm designates the Compliance Officer as its Anti-Money Laundering Compliance Officer (herewith the "AML Compliance Officer"). The individual must be qualified and possess any requisite certificates of professional competence, with experience, knowledge and training in order to be able to act as the Firm's AML Compliance Officer and will continue to enhance his or her training on a regular basis by participating in official training courses.

It is the responsibility of the Compliance Officer to monitor the Firm's compliance with AML obligations by continuously monitoring the activities of the Firm's clients, associated personnel and office employees to ensure that they are in compliance with the Firm's AML obligations. In addition, the AML Compliance Officer is responsible for developing and overseeing training for the Firm's personnel and oversees AML communications with clients, regulatory authorities, counterparties, the Firm's Senior Management, and the Board of Directors.

The AML Compliance Officer shall continuously monitor and update the Firm's written supervisory procedures relating to AML and the relevant Directive.

It is the responsibility of the Firm's AML Compliance Officer to ensure that proper AML records are kept and that any Compliance Officer's Reports to the Unit for Combating Money Laundering (herewith the "Suspicious Activity Report" or "SAR") are filed and appropriately communicated.

In the case of Branches, the Firm ensures that each branch has a designated Anti-Money Laundering Reporting Officer ("MLRO") approved by the relevant Supervising authority. All Compliance Officers are collectively responsible for ensuring that proper AML records are kept. When warranted, the AML Compliance Officers will ensure that Suspicious Activity Reports ("SAR") are filed.

The AML Compliance Officer makes himself available to answer any questions and offer assistance to employees in connection with any matter related to the prevention of money laundering and terrorist financing.

The responsibilities and duties of the Firm's AML Compliance Officer are described in more detail in Appendix I.

Compliance Officer's Annual Report for the Prevention of Money Laundering and Terrorist Financing

The Annual Report for the Prevention of Money Laundering and Terrorist Financing is an important tool for assessing the degree of conformity of the Company with its obligations under the AML Directive. The said report is prepared and submitted for approval to the Board of Directors within two months from the end of each calendar year.

The Annual Report, once approved by the Board of Directors, is submitted to the Commission together with the minutes of the BoD meeting during which the report was discussed and approved. Directive 144-2007-08 states that the BoD minutes must include all measures adopted to rectify any weaknesses and omissions identified within the Annual Report, as well as an implementation schedule of these measures. The Board minutes, accompanied by the Annual Report, must be submitted to the Commission within twenty days from the date the BoD meeting was held, and not later than three months after the end of the calendar year.

The compliance officer's annual report covers issues regarding Money Laundering and Terrorist Financing which occurred during the year under review, and contains at least the following:

a) Information for measures taken and/or procedures introduced for compliance with any amendments and/or new provisions of the Law and the AML Directive which took place during the year under review.

b) Information on the inspections and reviews performed by the compliance officer, reporting the material deficiencies and weaknesses identified in the policy, practices, measures, procedures and controls that the Firm applies for the prevention of money laundering and terrorist financing. In this regard, the report outlines

[2] Paragraph 9 of Directive 144-2007-08

the seriousness of the deficiencies and weaknesses, the risk implications and the actions taken and/or recommendations made for rectifying the situation.

c) The number of internal suspicion reports submitted by employees of the Firm to the compliance officer, and possible comments/observations thereon.
d) The number of Suspicious Activity Reports that the AML Compliance Officer has submitted to the UCML, and brief details and information on the reasons for suspicion and highlights of any particular trends.
e) Information and observations regarding communication with the Firm's employees regarding issues relating to Money Laundering and Terrorist Financing
f) Summary figures, on an annualised basis, of customers' total cash deposits in Euro and other currencies in excess of the set limit of 10.000 Euro (together with comparative figures for the previous year) as reported in the Monthly Prevention Statement. Any comments on material changes observed compared with the previous year shall also be reported
g) Information on the policy, measures, practices, procedures and controls applied by the Firm in relation to high risk customers as well as the number and country of origin of high risk customers with whom a business relationship is established or an occasional transaction has been executed.
h) Information on the systems and procedures applied by the Firm for the ongoing monitoring of customer accounts and transactions.
i) Information on the measures taken for the compliance of branches and subsidiaries of the Firm, that operate in countries outside the European Economic Area, with the requirements of the AML Directive in relation to customer identification, due diligence and record keeping procedures and comments/information on the level of their compliance with the said requirements.
j) Information on the training courses/seminars attended by the compliance officer and any other educational material received.
k) Information on training/education and any educational material provided to staff during the year, reporting, the number of courses/seminars organised, their duration, the number and the position of the employees attending, the names and qualifications of the instructors, and specifying whether the courses/seminars were developed in-house or by an external organisation or consultants.
l) Results of the assessment of the adequacy and effectiveness of staff training.
m) Information on the recommended next year's training program.
n) Information on the structure and staffing of the department of the compliance officer as well as recommendations and timeframe for their implementation, for any additional staff and technical resources which may be needed for reinforcing the measures and procedures against money laundering and terrorist financing.

Organizational Procedures

To ensure compliance with Anti-Money Laundering and Terrorist Financing legislation in force, it is essential to have appropriate and effective organisational procedures in place designed to address the key requirements and facilitate the smooth and at the same time controlled flow of information and interaction between the various departments.

The Firm has herein incorporated the following Customer Identification process as an integral part of the Firm's anti-money laundering compliance program. The Customer Identification process is in compliance with the Fifth Appendix of Directive 144-2007-08 (Specific Customer Identification Issues).

a. Customer Adoption - Customer Due Diligence

The main purpose of the Customer Adoption Policy is to protect the Firm's good reputation continuously and consistently, and to prevent the Firm from being used for fraudulent or criminal purposes. The underlying principle of the Customer Adoption Policy is that the Firm should "know its customers" (Know-your-Client process / "KYC"). The Firm's reputation can be harmed either by failing to act in accordance with regulators' principles or by dealing with counterparties whose business activities and reputation may cause harm to the Firm's reputation.

The ultimate responsibility for KYC obligations, both during the process of adoption and thereafter throughout the life cycle of the relationship, rests with the Compliance function. The Compliance function is responsible for monitoring developments in the field, identifying required action and informing and training all relevant personnel. The Compliance function is also responsible for the general over-viewing of the application of the prescribed procedures and the improvement / amendment of these procedures if the need arises.

In compliance with the legal framework, the Firm applies a risk based approach to Customer Due diligence based on the principles outlined below:

i. Major Determinants of the Due Diligence Process

1. The Due Diligence Procedures are applied[3]:
   a. When establishing a business relationship
   b. When carrying out occasional transactions amounting to €15.000 or more, irrespective of whether the transaction is carried out in a single operation or in several operations which appear to be linked
   c. When there is suspicion of money laundering or terrorist financing, irrespective of the value of the envisaged transaction
   d. When there are doubts about the veracity or adequacy of previously obtained customer identification data
2. As a general rule, the verification of the identity of the customer and the beneficial owner takes place before the establishment of a business relationship or the carrying out of the transaction.

   By way of exemption to the general rule, and subject to the controls outlined here below, it is possible to allow the verification of the identity of the customer and the beneficial owner to be completed during the establishment of a business relationship, if this is necessary in order not to interrupt the normal contact of business, in which case, the procedures must be completed as soon as practicable after the initial contact. Exemptions can only be granted by the Compliance Function or the General Manager only for the following cases:

   a) Where the potential customer is classified as “Low Risk” or “Normal Risk”
   b) Following the “sign-off” by the Compliance Officer or the General Manager of a special form stating the grounds for the exemption, the items of missing information and the deadline for submission of the missing documents / information.
   c) If the deadline for delivery of the missing information is not met, the account officer notifies immediately the Compliance Officer or the General Manager accordingly, who decides on further steps.
3. The keeping of anonymous accounts is strictly prohibited.
4. No accounts are opened with "shell banks" as these are defined within EU Legislation.

ii. Customer Due Diligence Measures

Such measures comprise of:

a) Identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;
b) identifying, where applicable, the beneficial owner and taking risk-based and adequate measures to verify his identity so that we are satisfied that we know who the beneficial owner is, including, as regards legal persons, trusts and similar legal arrangements, taking risk-based and adequate measures to understand the ownership and control structure of the customer;
c) obtaining information on the purpose and intended nature of the business relationship
d) 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 our knowledge of the customer, the business and risk profile, including, where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date

.

iii. Definition of Beneficial Owner

Beneficial Owner is defined as the natural person(s) who ultimately owns or controls the customer and / or the natural person on whose behalf a transaction or activity is being conducted and includes at least the following for:

1. **Corporate entities (companies):**
   a) the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements

[3] Section 60 of Law N188(I)-2007

consistent with Community legislation or subject to equivalent international standards; a percentage of 10 %[4] plus one share shall be deemed sufficient to meet this criterion;

b) the natural person(s) who otherwise exercises control over the management of a legal entity.

2. **Foundations, and legal arrangements, such as trusts, which administer and distribute funds:**

a) where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of 10% or more of the property of a legal arrangement or entity

b) where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;

c) the natural person(s) who exercises control over 10% or more of the property of a legal arrangement or entity

3 **Special cases**

a) **Collective Investment Vehicles:** The definition refers to unit trusts, mutual funds and hedge funds. Because in such cases, the number of beneficial owners is potentially large and because the beneficial owners change continuously, the Customer Due Diligence process is performed for the Investment Manager or the Administrator of the fund.

In such cases, before we apply this exemption, we need to collect sufficient proof of the fact that the Customer belongs to this category. Such information might consist of:

i) Copy of the prospectus
ii) Articles and Memorandum of Association

In addition, the business relationship between the fund and the Fund Manager or the Administrator must also be established. This can be achieved by obtaining extracts[5] of the management agreement between the fund and the Fund Manager or the Administrator.

b) **Situations where the client specifies explicitly the counterparty to the transaction**: According to Circular 2007/12 issued by CySEC, if a client submits an order for execution and at the same time specifies explicitly who the counterparty in the transaction is going to be, we are obliged to carry-out the same Customer Due Diligence procedures that are applied for our Customers in respect of the specified counterparty in the transaction. The logic behind this requirement is that it would be a convenient way for a money launderer to blur the trail of the money by making transactions between a number of companies that are in effect controlled by the same, without losing beneficial ownership of the assets. It would also be a convenient way to abuse the markets by either creating plasmatic prices and/ or volumes.

c) **Transactions on behalf of a third party**: Investment Firms are obliged to take adequate measures for the collection of sufficient documents, information or data for the identification and verification of the identity of any third person on whose behalf the customer is acting.

In addition, for customers that are corporate entities or other legal entities such as foundations and legal arrangements such as trusts, it must be verified that the natural person(s) that purports to act on behalf of the customer is duly authorized for that purpose and the identity of such persons must be established and verified.

iv. Risk Categorisation

Depending on the information that is made available to us though the “Investor Questionnaire” and any other supplementary information, all potential and existing customers are categorized, into three categories: **Low** / **Medium** / **High Risk**.

Risks posed by some customers may only become evident only once the customer has commenced trading through his account, making monitoring of customer transactions a fundamental component of the Company’s AML Compliance process.

[4] European Directive 2005/60/EC sets the benchmark to 25%. However, Cypriot Authorities have exercised the discretion accorded by article 5 of the said Directive to adopt stricter provisions.

[5] The parts that relate to the remuneration of the Fund Manager or the Administrator can be omitted on the grounds that it represents sensitive information that may not be disclosed.

In measuring potential Money Laundering Risk, the Firm also considers and assesses the following factors:
a. Type of the customer and nature of business;
b. Type of product / service availed by the customer; and
c. Country where the Customer is domiciled.

The level of Money Laundering risks that the Firm is exposed to through a client relationship depends also on the following Risk Components:
a. Country risk;
b. Customer risk; and
c. Product and Service Risk.

AML Compliance procedures provide guidance on the way of identification of the customer's money laundering risk, including the proportional weight of each of the risk components in the overall risk assessment and on the way of measuring thereof.

a. Low risk clients - criteria

Low Risk Customers, according to legislation[6] are:

1. Credit or financial institutions covered by the EU Directive
2. Credit or financial institutions carrying out one or more of the financial business activities as these are defined in section 2 of the EU Directive and which are situated in a country outside the European Economic Area, which:
   i. in accordance with a decision of the Advisory Authority for Combating Money Laundering and Terrorist Financing, imposes requirements equivalent to those laid down by the EU Directive and
   ii. it is under supervision for compliance with those requirements
3. Listed companies whose securities are admitted to trading on a regulated market in a country of the European Economic Area or in a third country which is subject to disclosure requirements consistent with community legislation
4. Domestic public authorities of countries of the European Economic Area

No other Entity can be considered as a Low Risk.

b. High risk clients - criteria

Customers are classified as high risk according to the following criteria:

1. **High Risk Countries & Deficient Jurisdictions:** Even though literally all countries have enacted anti-money laundering legislation, the tenacity and effectiveness of implementation varies widely across jurisdictions. Deficient jurisdictions have been defined as all those countries and territories identified by the Financial Action Task Force (FATF) as non-cooperative countries and territories (NCCT) in the fight against money laundering or as having material deficiencies in their anti-money laundering procedures.
2. **Politically Exposed Persons (PEPs)**
3. **Bearer Shares:** The ownership structure contains legal entities that have either issued bearer shares, their Articles and Memorandum of Association allow the issue of bearer shares and / or the switch from registered to bearer shares and / or companies shares are in bearer form.
4. **The Customer has not been physically present for identification purposes (non face to face transactions)**
5. **The Corporate Customer opts for an excessively complex structure that favours anonymity;**
6. **Trusts Accounts**
7. **There are multiple accounts which have the same person(s) as beneficial owner(s):** This does not necessarily imply that the accounts are used to launder money, but, it does make it easier to churn assets through accounts that are controlled by the same person, which also increases the risk of market manipulation. This criterion should be used alongside the presence of any of the other criteria mentioned hereabove.
8. **Clients involved in electronic gambling / gaming through the internet.**

[6] Section 63(1) of L188(I)-2007

The above list is indicative and it is not exhaustive. The Compliance Officer examining the case, can classify a Customer (potential or existing) as high risk if there are any circumstances that would warrant so such as the industry in which the customer operates, reputational factors and other risk presented from a potential cooperation.

c. Normal Risk Clients - Criteria

Normal Risk Customers are customers that generally do not fall in the Low or High Risk Categories.

v. Simplified Due Diligence[7]

According to section 63 of Law L188(I)/2007, in the case of Customers who are classified as "low risk" the Firm may not apply customer due diligence measures subject to the provisions of paragraph 18 of Directive 144-2007-08.

However, it is provided that the Firm will collect sufficient information so as to decide whether the customer can be exempted from the standard of due diligence process. Such information shall include:

a) Evidence to be obtained from the Customer regulator's website of authorisation credentials, including, where applicable, details of the Investment and/or ancillary services that the customer is authorised to provide, in order to assess whether these are compatible with the envisaged business relationship
b) Copy of the authorisation license of the client
c) Proof of listing from the web-site of the regulated market where the financial instruments issued by the Customer are listed

Applying simplified customer due diligence procedures does not absolve from the need to collect information about the natural persons who can commit the Customer in any agreement. Such information includes:

a) Certificate of Directors, issued by a reliable and independent authority
b) In the case of large financial institutions where other persons, apart from the Directors, can commit the Customer in its dealings with our Firm, a Signatory List
c) Any Power of Attorneys that may have been issued by the Customer to third parties representing the Customer

vi. Enhanced Due Diligence[8]

Under Law L188(I)/2007 and Directive 144-2007-08, the Firm is required to have in place enhanced procedures where money laundering risk is high. The Firm, in order to comply with the mentioned legislation, applies enhanced customer identification and due diligence methods, in respect to high risk customers, as these are defined in the Fourth Appendix of the Directive 144-2007-08.

The Firm recognizes that there is a heightened risk of not knowing the customer's true identity for certain types of accounts, such as an account opened in the name of an entity that is created, or conducts substantial business in, a jurisdiction that has been designated by relevant authorities as of primary money laundering concern or has been designated as non-cooperative by an international body such as the Financial Action Task Force (FATF), the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), etc.

Additional measures may be used to obtain information about the identity of customers that pose a heightened risk, as standard documentary methods may prove to be insufficient. Such additional procedures for verifying the identity of certain customers would include obtaining information about individuals with authority or control over such accounts.

Customers categorized as "High Risk" are subject to certain additional measures and controls. These include:

1. In cases where the Customer has not been physically present for identification purposes or the customer is requesting to establish a business relationship or an occasional transaction by mail, telephone or through the internet (**non face to face transactions**), at least one of the following measures, or a combination of them, must be applied:

[7] Paragraph 23 of Directive 144-2007-08
[8] Paragraph 24 of Directive 144-2007-08

a) Obtain additional documents, data or information for verifying customer's identity.
To that end, through Directive DI144-2007-08(A), CySEC provides some guidance as to the nature of such additional documents, data and information, and provides suggestions as to the means of obtaining the said information. In particular, the following measures are stipulated:

(i) a personal interview is recommended during which all information for customer identification should be obtained
(ii) ***At least one*** of the following measures should be applied:

1. The first payment of the operations is carried out through an account opened in the customer's name with a credit institution operating and licensed in a third country, which, according to the Advisory Authority's decision, imposes requirements on combating money laundering equivalent to those of the EU Directive.
2. A direct confirmation of the establishment of a business relationship is obtained through direct personal contact, as well as, the true name, address and passport/identity card number of the customer, from a credit institution or a financial institution with which the customer cooperates, operating in a Member State or in a Third Country, which, according to the Advisory Authority's decision, imposes requirements on combating money laundering equivalent to those of the EU Directive (or a true copy of the confirmation).
3. Telephone contact with the customer at his home or office, on a telephone number which has been verified from independent and reliable sources. During the telephone contact, the Firm shall confirm additional aspects of the identity information submitted by the customer during the procedure of opening his account.
4. Communication via video call with the customer, provided that:
   - the video recording and screen shot safeguards apply to the communication.
   - The said customer cannot deposit an amount over €2.000 per annum, irrespective of the number of accounts that he keeps with the Financial Organization,

     Unless

     - an additional measure out of the list of measures enumerated under this section is taken

     or

     - any of the supplementary measures of paragraph (b) here below is taken in order to verify his identity.
   - During the internet communication, the Financial Organization shall confirm additional aspects of the identity details submitted by the customer when opening his account.
   - The Firm shall apply appropriate measures and procedures in order to:
     - confirm and monitor both the amount of the customer's deposit and the risk for money laundering or terrorist financing and take additional measures to verify the customer's identity depending on the degree of the risk;
     - ensure the normal conduct of business is not interrupted where the amount of the deposit exceeds the amount of €2.000 per annum;
     - warn the customer appropriately and in due time for the above procedure in order to obtain the customer's express consent prior to its commencement.
5. Communication with the customer through at an address that the Firm has previously verified from independent and reliable sources, in the form of a registered letter (For example, such communication may take the form of a direct mailing of account opening documentation to him, which the customer shall return to the Firm or the Firm may send security codes required by the customer to access the accounts opened through the internet).
6. Performing an electronic verification:
   - In such cases, electronic identity verification is carried out either directly by Firm or through a third party. Both the Firm and the said third parties must cumulatively satisfy the following conditions:
     - the electronic databases kept by the third party or to which the third party or the Firm has access are registered to and/or approved by the Data Protection Commissioner in order to safeguard personal data (or the corresponding competent authority in the country the said databases are kept).
     - electronic databases provide access to information referred to both present and past situations showing that the person really exists and providing both positive information (at least the customer's full name, address and date of birth) and negative information (e.g. committing of

offences such as identity theft, inclusion in deceased persons records, inclusion in sanctions and restrictive measures' list by the Council of the European Union and the UN Security Council).
- electronic databases include a wide range of sources with information from different time periods with real-time update and trigger alerts when important data alter.
- transparent procedures have been established allowing the Financial Organization to know which information was searched, the result of such search and its significance in relation to the level of assurance as to the customer's identity verification.
- procedures have been established allowing the Firm to record and save the information used and the result in relation to identity verification.

- The Firm evaluates the results of electronic verification in order to assess that the conditions of Article 61(3) of Law L188(I)/2007 are satisfied, namely that the proof of identity is satisfactory, in the sense that:
  - It is reasonable possible to establish that the customer is the person he claims to be; and
  - The person who examines the evidence is satisfied, in accordance with the procedures followed under the said law and this policy, that the customer is actually the person he claims to be.

  The Firm shall, in such cases, establish mechanisms for the carrying out of quality controls in order to assess the quality of the information on which it intends to rely upon.
- Information must come from two or more sources. The electronic verification procedure shall at least satisfy the following correlation standard:
  - identification of the customer's full name and current address from one source, and
  - identification of the customer's full name and either his current address or date of birth from a second source.
- For purposes of carrying out the electronic verification, the Firm shall:
  - establish procedures in order to satisfy the completeness, validity and reliability of the information to which it has access.
  - Ensure that the verification procedure includes a search of both positive and negative information.

b) take supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution covered by the EU Unit for Combating Money Laundering – UCML

Directive DI144-2007-08(A) provides some additional guidance as to the form of verification of such documents, and states that they shall be in any of the following forms:

(i) Original, or
(ii) True copy of the original, where the certification is made by the Firm in cases where it establishes the customer's identity itself, once the original is presented thereto, or
(iii) True copy of the original, where the certification is made by third parties, in cases where the customer's identity is establish by relying on the performance by third parties of the customer due diligence process
(iv) True copy of the original, where the certification is made by a competent authority or person that, pursuant to the relevant provisions of the laws of their country, is responsible to certify the authenticity of documents or information, in cases where they establish the customer's identity themselves, or
(v) Copy of the original, provided that at least one of the procedures referred to in paragraph (b) below is followed.

c) Ensure that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution which operates in a country within the European Economic Area.

Directive DI144-2007-08(A) stipulates also that the Firm shall take additional measures to ensure that the companies or other legal persons operate from the address of their main offices and carry out legitimate activities in all respects.

2. In respect of Politically Exposed Persons (**PEPs**), at least one of the following measures, or a combination of them, must be applied:
   a) The approval of the General Manager is required for establishing business relationships with PEPs
   b) The source of wealth and source of funds that are involved in the business relationship or the transaction must be established
   c) Such accounts are subjected to continuous monitoring

3. Companies the capital of which consists of **bearer shares**

As a general rule, no account should be opened for legal entities the ownership structure of which includes at least one company who has either issued bearer shares or the Articles and Memorandum of Association allows the issue of bearer shares and / or the switch from registered to bearer shares, unless at least one of the following conditions is satisfied:

a) The shares are listed on a recognized stock exchange
b) The company acts as an approved collective investment fund, incorporated in a country that exercises effective regulation and supervision of the operations of such funds
c) The stocks or the control of the company are in the hands of a government or a governmental organization
d) The beneficial shareholder is a multinational company of good repute and financial strength

In case none of the conditions outlined above is met, an account is opened provided that all of the following procedures are applied:

a) The true identity and the background of the beneficial shareholders / directors of the company is verified prior to the execution of any transaction
b) At the stage of examining the application for the establishment of a business relationship, it is requested from the directors or the lawyer or the accountants/auditors who acted for the incorporation of the company to provide an estimate of the frequency and value of the orders to be submitted for execution. The higher the expected frequency of submitting orders, the more cautious we must be.
c) The certificates of the bearer stocks must be placed under our own physical custody for all the time the business relationship is in effect, or we must obtain a certificate from a European bank that the bearer stock certificates (titles) are under its custody and that it will duly notify us in case the certificates are released from their custody and transfer to another person.
d) If it is finally decided that we will proceed to the establishment of the business relationship, the account is subjected to close scrutiny and surveillance. At least twice a year, an overview of this relationship is undertaken and a review of the accounts' transactions and turnover is carries out, and a note is prepared summarising the results of the review which must be kept in the customer's file.

   As part of the review process, a comparison is carried-out between the actual vs the expected frequency and value of transactions. Any substantial deviations are investigated for the purpose of assessing the trustworthiness of the lawyer, or the accountant/auditor who has recommended the establishment of the business relationship with the said client.
e) At least once every year, it is verified through the lawyer or the accountant/auditor who acted for the incorporation of the said customer, that the capital structure of the company or of its subsidiaries/holding company, depending on the case, has not been altered by the issue of new bearer stocks or the cancellation of existing ones.
f) When there is a change in the true beneficial owners of the company, we must reassess whether it is appropriate to continue the business relationship.

For all other clients who are categorized as "high risk" and do not fall into one of the two cases stated above, at least one of the additional measures stated hereabove is applied.

vii. Non Documentary Methods for Client Verification

The Firm may use the following non-documentary methods of verifying a customer's identity:

a. Contacting the customer
b. Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from public sources
c. Checking references with other financial institutions, authorities, and/or approved third parties
d. Checking for information from www.worldcompliance.com or any other commercial source of information

Non-documentary methods of verification will be used in the following situations:

a. When the Firm is unfamiliar with the documents the customer presents for identification verification (i.e. first time received government corporate documentation)
b. When the customer and the Firm do not have face-to-face contact (subject also to the special conditions for non-face-to-face customers)
c. When there are other circumstances that increase the risk that the Firm will be unable to verify the true identity of the customer through documentary means

Information will be verified within a reasonable time before or after the account is opened. Depending on the nature of the account and requested transactions, the Firm may refuse to complete a transaction before it has verified the information. Approval by General Manager must be obtained prior to completing a transaction when the verification of information has not been completed.

In addition, the Firm may, pending verification, restrict the types of transactions or quantity of transactions as to number and/or amount invested in, until the verification of information has been fully completed.

viii. Transactions that favour anonymity[9]

In cases where customer is not present (transactions via internet, phone, fax) Investment Firms have the obligation to verify the authenticity of his signature, and/or that his is the real owner of the account and/or that he has been properly authorized to operate the account. In order to do that the Firm is checking the information saved in internal systems, such as beneficial owner identity and signatory list.

ix. Customers who refuse to provide information[10]

In cases where a potential or existing customer either refuses to provide the information described above, or appears to have intentionally provided misleading information, the Firm will not open a new account and, after considering the risks involved, consider withholding activity of any existing account(s) for the said customer. In either case, the Firm's AML Compliance Officer must be notified by the Firm's staff through an Internal Suspicion Report so that he/she can determine if the situation should be reported to UCML by filing a Suspicious Activity Report.

b. Customer Adoption – Performance by third parties[11]

Subject to certain conditions pertaining, the Firm may rely on the performance by third parties[12] (including affiliated entities) for some or all of the elements of its Customer Identification process. The implementation of customer identification and due diligence procedures, as these are prescribed in sections 61(1)(a),(b) and (c) of Law L188(I)/2007, provide that the third person makes immediately available to the Firm all data and information that was collected for the performance of the Customer Due Diligence process, which must be certified as true copies of the originals.

The Firm shall obtain data and information so as to verify that the third party is subjected to professional registration and in accordance with relevant laws 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 Firm 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 its customers. Any additional data and information, according to the degree of risk, for the purpose of updating the customer's economic profile or for the purpose of examining unusual transactions executed through the account, shall be obtained directly 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 the customer's funds and assets.

Where the third party is an accountant, an independent legal professional, or a trust and company services provider from a country which is a member of the European Economic Area or a third country that the Advisory Authority for Combating Money Laundering and Terrorist Financing has determined to be applying procedures and measures for the prevention of money laundering and terrorist financing equivalent to the European Union Directive, then the Firm, before accepting the customer identification data verified by the said third party, shall apply the following additional measures/procedures:

a. Assessment and evaluation of the systems and procedures for the prevention of money laundering and terrorist financing applied by the third party

[9] Paragraph 19 of Directive 144-2007-08
[10] Paragraph 20 of Directive 144-2007-08
[11] Paragraph 25 of Directive 144-2007-08
[12] L188(I)/2007 section 67,(2)(a)(b)

b. The commencement of the cooperation with the third party and the acceptance of customer identification data verified by the third party is subject to approval by the compliance officer.

c. Customer Adoption - Investor Questionnaire - Risk Categorisation

i. Scope of the Investor Questionnaire

Potential Customers have to submit a duly completed and signed "Investor Questionnaire" form. This is a multi-faceted document, that apart from being used for the collection of information for AML purposes, it is also used to collect information about the investment objectives, the financial status and the knowledge and experience of the applicant (concepts of appropriateness and suitability).

In this section, we will concentrate on those parts of the questionnaire that are relevant for AML purposes and that are used to enhance the "Know Your Client" principle. In this respect, the additional information collected relates, among other things, to:

1. the structure of the entity
2. the countries that represent the entity's interests
3. the bank accounts to be used by the client in the business relationship
4. the estimated volume of transactions
5. the nature of the customer's business
6. the source of funds
7. the existence of a KYC policy on the part of the customer
8. information as to whether there are other related / affiliated accounts held with the Firm

ii. Checking the Investor Questionnaire - Risk categorisation / Recording and communicating the decisions taken

The first task performed by the Back Office person pre-checking the Investor Questionnaire form is to verify the validity of the document by checking the signature of the person signing the questionnaire against the list of signatories that have the power to commit the customer.

All the answers provided on the form and which relate to AML, are entered by the Compliance Officer in the specially designed database of the Firm, ATDPMain (the database has full access controls and audit trail functionality).

The Compliance Officer examining the case applies the Risk Categorisation principles after examining all the available information and after reviewing the documents that have been submitted as regards the identity of the customer or the beneficial owner.

Upon completing the process, the Compliance Officer asks from the Head of Back Office to open the account and notifies to the same:

- The Risk Classification of the customer (Low / Medium / High)
- The Customer Due Diligence method (Simplified, Standard, Enhanced)
- The MiFID category (Professional or Eligible Counterparty)

d. Retention and updating of records

i. Creation of the Customer Folder / Retention period

A folder is created for each new customer that contains all relevant KYC information in hard copy and the Compliance Function is responsible for the keeping and updating of the folder. In addition, all documents submitted by the Customer are scanned and stored in electronic format on a designated directory on the Firm's servers.

The Customer's file is frequently updated throughout the operation of the account and all the information contained therein, and other information related to the operation of the account that is kept in electronic form is retained for a period of five years after the business relationship with the Customer has ended or the last transaction was carried-out.

ii. Updating of records

The Firm applies a review process that involves the following steps:

1. The following information are kept in the system for enabling monitoring and control:
   Expiration date for:
   - Certificate of Good Standing
   - Power of Attorney
   - Certificate of Directors

   Review Date for counterparties

The above mentioned information are used by the system in order to create alerts.

Additionally prior to the execution of any transaction, Client Service Desk, in close cooperation with the Compliance Function, is responsible for checking whether any information of the client is due to review or update.

2. The review process has two distinctive forms, namely:
   - **Full Review:** in this case, clients and counterparties are asked to submit recent copies of all the documents that are required for the performance of the Customer Due Diligence process, and also the duly completed and updated Investor Questionnaire according to the following frequency, depending of their risk categorisation:
     - Low Risk accounts: Once every five (5) years
     - Medium Risk accounts: Once every two (2) years
     - High Risk accounts: Every year
   - **Soft Review:** in this case, a letter is sent to clients and counterparties asking them to either confirm that the information that the Firm has on record is still valid and true or otherwise to notify the Firm if any of the said information has changed. In the latter scenario, the affected client / counterrparty shall submit all the necessary documents that confirm the changes. The soft reviews are performed according to the following frequency, depending on the risk categorisation of each account:
     - Low and Medium Risk accounts: Every year
     - High Risk accounts: Twice per year (included in both the March and September batches)

     The Full and Soft Review processes interact with each other in the sense that, if during any of the two schedules, it is time for an account to undergo a Full Review, the Soft Review will be substituted by the Full Review and from there on, the Soft Review process will run at the frequency that applies for the particular client.

Notwithstanding the procedure outlined here above, clients have a contractual obligation to notify us in cases where there is any change in the capital structure or any other development that would bring about a change in effective control as soon as such an event occurs or becomes known to the management of the customer. The customer is also expected to notify us immediately of any termination of the authorization granted to any of the signatories / attorneys.

In the case of customers who are classified as High Risk, by decision of the Compliance Function and in the application of the Enhanced Due Diligence concept, additional information might be required from the customer, like a copy of the latest audited financial results of the client.

In the case of Customers that were classified as “Low Risk”, the updating of records is carried-out in the same manner as the at the adoption process – for example, if proof of authorisation was obtained through the internet for the set-up of an account for a European regulated Investment Firm, the same will apply for the update process.

e. Prohibition of third party transfers

As a general rule, and except from duly justified cases, the Firm does not accept any instructions for the transfer of funds or financial instruments to any bank or custody account where the beneficiary is any third party and not the Firm’s Client.

This measure has a two-fold purpose:

1. To prevent a client from creating a complicated money trail and thus using the Firm as an intermediary, accessory or conduit to the Client's money laundering efforts. This in itself can act as an important deterrent to money launderers approaching our Firm to establish a business relationship.
2. To avert the threat of fraud and embezzlement of property belonging to our clients

In duly justified cases, by decision of the AML Compliance Officer, the Firm might allow 3rd party transfers, upon presentation by the client of authentic documents supporting a valid and legal reason for the transfer.

f. Prohibition of dealing in cash

As a matter of policy, our Firm does not accept cash or cash equivalents (for example 'travellers cheques') from Clients.

g. On-going monitoring – Identifying and Reporting Suspicious Activity

i. Identifying and Reporting Suspicious Activity

Suspicious activity may include identifying patterns of unusual size, volume, or type of transaction, geographic factors such as the choice of banks that are located very far away from the place of incorporation / operations, or any of the «red flags»

The Compliance Officer is responsible for such monitoring, which is done during the normal daily review of trades. Among the information that will be used to determine if a Suspicious Activity Report should be filed are exception reports that include transaction size, location, type, number, and nature of the activity.

The Company's AML Compliance Officer issues employee guidelines with examples of suspicious money laundering activity and lists of high-risk clients whose accounts may warrant further scrutiny.

A list of warnings that may signal possible money laundering or terrorist financing ("Red Flags") is attached in Appendix II. The list attached in Appendix II is not exhaustive nor does it include all types of transactions that may be used. Nevertheless it can assist the Firm and staff in recognising the main methods used for money laundering and terrorist financing.

The Firm and staff may also refer to the list provided in the Sixth Appendix of the Directive 144-2007-08 containing further examples of what might constitute suspicious transactions and activities related to money laundering and terrorist financing.

ii. Responding to "Red Flags" and Suspicious Activity

The detection by any member of staff of any of the traits of a "red flag" mentioned in Appendix II and the Sixth Appendix of the AML Directive prompts further investigation and constitutes a valid cause for seeking additional information as to the source and origin of the funds, the nature and business purpose of the client's transaction, as well as the circumstances surrounding a particular activity performed by the customer.

When a member of staff detects any "red flag", he/she will alert the Compliance Officer through an Internal Suspicions Report who will, in turn, conduct further investigations. This may include gathering additional information internally or from third-party sources, contacting the relevant government authorities, freezing the account, or filing a Suspicious Activity Report to the UCML. The Compliance Officer receiving the report must remind the person submitting the report about the obligation to avoid the "tipping-off" of the Customer or any other third party and the ramifications of such an act.

The Compliance Officer will issue an Internal Evaluation Report his / her evaluation and examination of the information received by the Firm's employees and stating the Compliance Officer's final decision on the matter. Irrespective of the outcome of the process, the internal report containing the facts originally submitted and the actions and justification of the decision of the AML Compliance Officer is archived for future reference.

iii. Prohibition of Dealing prior to the submission of a SAR

Investment Firms and their employees shall refrain from carrying-out transactions which they know or suspect to be related to money laundering or terrorist financing, until a SAR is submitted to the UCML.

However, the Law recognizes that in certain cases, refraining from carrying-out the transaction is impossible or not carrying-out the transaction would in itself "tip-off" the Customer. In such cases, the Law allows for the reporting to be performed immediately after the transaction is carried-out.

It is important that any suspicions are notified to the Compliance Officer immediately when they are raised. The Compliance Officer will offer advice as to whether it is preferable to carry-out the transaction or refrain from doing so, imploring, if deemed necessary, the advice of the UCML.

iv. Suspicious Transactions Reporting - Filing a SAR

It is a requirement of the Cyprus Securities and Exchange Commission that suspicious activity reports be filed. According to the requirement, the Firm shall file SARs for any account activity conducted or attempted through our Firm when we know, suspect, or have reason to suspect that:

1. The transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from any illegal activity as part of a plan to violate or evade any governmental law or regulation,

2. The transaction has no apparent business or purportedly lawful purpose, or is not the sort in which such a customer would normally be expected to engage in, and we are unable to determine, after examining the background, possible purpose and/or other facts relating to such transaction, no reasonable explanation for it.

3. The transaction involves the Firm in facilitating criminal activity.

We will not base our decision on whether to file a SAR solely on whether the transaction falls above a set threshold. We will file a SAR and notify law enforcement of all transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities.

Notification will not be provided to any person involved in the transaction reported and especially to the suspected customer except as permitted by UCML regulations. The fact that a SAR has been submitted or any information related to the case will not be disclosed to any party, except where disclosure is requested by UCML, or another appropriate law enforcement or regulatory authority (always upon instructions by the UCML). If the Firm receives such a request, the AML Compliance Officer will be immediately notified, and, in turn, he/she will notify UCML of the disclosure request.

v. Submission of Monthly reports

Over and above the measures and procedures outlined above, the Cyprus Securities and Exchange Commission requires all Investment Firms authorised by it to report, within fifteen days from the end of each month, all transactions in cash above a certain predetermined limit, currently set at 10.000 Euros.

h. AML record keeping

i. Suspicious Activity Report Maintenance and Confidentiality

The Firm will keep all Suspicious Activity Reports and any supporting documentation confidential. It will not inform anyone besides UCML or other regulatory authorities approved by UCML about the Suspicious Activity Report. The Compliance Officer will segregate SAR filings and copies of supporting documentation from other Firm books and records.

ii. Responsibility for AML Records and Suspicious Activity Reports

The Firm's Compliance Officer will be responsible for ensuring that AML records are properly maintained and that Suspicious Activity Reports and other supporting documentation are filed as required.

i. Confidentiality and Prohibition of Disclosure

Given the duty of confidentiality that is owed to our Customers and the general prohibition of disclosure, it becomes imperative to analyse in detail our responsibilities in respect of these principles.

i. Confidentiality

a) Informing authorities about suspicions of money laundering or terrorist financing does not in any way breach any confidentiality duties owed to our Customers. It is a crime not to disclose such suspicions.
b) There is no breach of confidentiality in the application of the concept of performance of the Customer Due Diligence Process by third parties. However, in order to ensure that the concept is not abused, we will always seek the approval of our Customer before submitting to any third party information about the Customer and the ultimate beneficial owners.

ii. Prohibition of Disclosure

"Tipping-off" is a criminal offence punishable with up to 5 years imprisonment. The Law states that Investment Firms, their directors and employees shall not disclose to the customer concerned or to other third persons the fact that a SAR has been submitted or that a money laundering or terrorist financing investigation is being or may be carried-out.

Training Program

The Firm has developed ongoing employee training under the leadership of the Firm's Compliance Function. Training will occur on at least an annual basis or whenever there is a material change in the AML laws and regulations or when the Firm's policies and procedures may change. The Compliance Officer will maintain records of the persons who received training, the date of training, the subject matter of the training and a copy of the materials used to conduct the training.

In cases there are major developments in the field of Anti-Money Laundering, depending on how critical these developments are, the Compliance Function may opt to organize a seminar to be attended by all affected parties. If this option is attained, a signed list of the people participating will be kept. Arrangements will be made for the people who were not able to attend the seminar to get a copy of the taught material and have any queries answered.

As part of the initiation process of new employees, all new employees receive a copy of the Company's Operations Manual that incorporates the AML policy.

As part of the wider training program, the Firm fosters a "train-the-trainer" approach. Compliance Officers frequently attend AML seminars and forums to keep up to date with current developments in the field. The pool of knowledge acquired is shared with the rest of the colleagues and one-on-one meetings are conducted, as needed, with individual employees.

Appendix I

Responsibilities of the AML Compliance Officer

The main responsibilities of the AML Compliance Officer within the Firm are the following:

a) Plans the Firm's procedures and controls for the Prevention of Money Laundering and Terrorist Financing
b) Develops the Customer Acceptance Policy which is approved by the Board of Directors
c) Prepares the Risk Management Manual for the Prevention of Money Laundering and Terrorist Financing
d) Monitors and evaluates the sound and effective implementation of the Firm's general policy principles in relation to the Prevention of Money Laundering and Terrorist Financing
e) Applies adequate monitoring mechanisms such as spot checks, for the collection of necessary information on the degree of compliance of all departments within the Firm. Any results from evaluations are kept in writing. In identifying omissions and weaknesses in the implementation of required practices, measures, procedures and controls, he provides appropriate guidance for corrective measures and, where necessary, informs the Board of Directors.
f) Receives information from all personnel regarding suspicious client transactions and activities, which they believe that a client may be associated with Money Laundering or Terrorist Financing. The information is obtained through the Internal Suspicion Report
g) Evaluates the information received regarding suspicious client transactions and activities, and discusses the facts about the case with the reporting employee and, where necessary, with the Head of Department of the reporting employee.
h) If the compliance officer decides to disclose the information received in point (f) to the UCML, he prepares a written Suspicious Activity Report (SAR) submitted to the unit the soonest possible.
i) Evaluates the systems and procedures implemented by a third person to whom the financial institution is based on the implementation procedures for determining identity and customer due diligence measures.
j) Prepares and submits to the Cyprus Securities & Exchange Commission the Monthly Preliminary Statement for the Prevention of Money Laundering and Terrorist Financing as this has been posted in the Commission's website.
k) Prepares and submits to the Board of Directors the Annual Report for the Prevention of Money Laundering and Terrorist Financing.

ATONLINE LIMITED

Appendix II

Red Flags

The following are a number of warnings that may signal possible money laundering or terrorist financing:

1. The customer or potential customer exhibits unusual concern about the Firm's compliance with reporting requirements and the Firm's AML policies (particularly concerning his/her identity, type of business and/or assets), or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspicious identification or business documents.
2. The customer provides non-verifiable references or is reluctant or refuses to provide financial information or information concerning his/her financial relationships and business activities.
3. A customer questions if conducting certain asset movements either these are funds or financial instruments would prompt reporting to the Cyprus authorities (i.e. the UCML, CySEC, the Police).
4. The customer repeatedly requests exceptions to policies and procedures set up to deter money-laundering activities (i.e. banking secrecy rules existing in third countries allowing him/her to withhold information).
5. The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated investment objectives.
6. The information provided by the customer that identifies a legitimate source for funds is false, misleading or substantially incorrect.
7. Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
8. The customer (or a person publicly associated with the customer) has a questionable background or is the subject of investigations indicating possible criminal, civil, or regulatory violations.
9. The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
10. The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
11. The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
12. The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash, or asks for exemptions from the Firm's policies relating to the deposit of cash.
13. The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the €10,000 CySEC reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
14. For no apparent reason, the customer requests multiple accounts under a single name, with a large number of inter-account or third party transfers.
15. The customer is from a country identified as a non-cooperative country or territory (NCCT) by the FATF.
16. The customer's account has unexplained or sudden extensive fund activity, especially in accounts that had little or no previous activity.
17. The customer's account has a large number of outgoing money transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
18. The customer's account has incoming and/or outgoing money transfers that have no apparent business purpose to or from a country identified as money laundering risk or a bank secrecy haven.
19. The customer's account indicates large or frequent incoming money transfers, immediately withdrawn to another account without any apparent business purpose.
20. The customer makes a funds deposit followed by an immediate request that the money be transferred out or transferred to a third party, or to another Firm, without any apparent business purpose.
21. The customer requests that a transaction be processed immediately with primary cause the avoidance the Firm's normal documentation process requirements.
22. The customer, for no apparent reason or in conjunction with other warnings, engages in transactions involving securities, which although legitimate, have been used in connection with fraudulent schemes and money laundering activities. (Such transaction may warrant enhanced due diligence to ensure the legitimacy of the customer's activities.)
23. The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.
24. The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose.
25. The customer's account has inflows of funds or financial instruments well beyond the known income or resources of the customer.

26. An account develops a pattern of journaling funds and/or securities to other accounts.
27. The customer may request Firm codes or passwords to facilitate the transfer of cash or securities from or in his account through the Firm's counterparties.
28. The customer requests the disbursement of funds from an account versus un-cleared funds.
29. The customer frequently advises that money transfers have been sent in error and requests immediate return of funds or that the transfer to be forwarded in another account involving another counterparty.