BROKER

AML POLICIES

Table of Contents

INTERNAL MANUAL AND PROCEDURES AGAINST MONEY LAUNDERING AND TERRORIST FINANCING

1. General provisions and definitions

Hereby AM Globe Services Ltd institutes an Anti-Money Laundering internal manual and procedures intended to detect, prevent, and report possible money laundering or terrorist financing activities in compliance with the International Money Laundering.

1.1. Abbreviations used:

"AML/CFT" – Anti-Money Laundering and Combating the Financing of Terrorism.

"FATF" – Financial Action Task Force. FATF is an inter-governmental body whose objectives are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.

"AMG" – AM Globe Services Ltd

"Manual" – this internal document that describes measures and principles applied by AM Globe Services Ltd in order to comply with requirements of MLTPA and international sanctions.

1.2. This Manual shall be observed and applied by all employees and managers of AMG, unless otherwise stipulated in this Manual. This Manual shall be applicable to all business relations and customer transactions of AMG, including any transactions intermediated by agents in cases where certain functions have been delegated to third parties. The obligations arising from this Manual shall be performed by using the information technological solutions implemented in AMG according to any relevant conditions and procedures.

1.3. This Manual shall be applied in conjunction with MLTPA and its subordinate and amending acts and guidelines issued by competent authorities.

1.4. Money laundering is:

(i) the concealment or maintenance of confidentiality of the true nature, origin, location, manner of disposal, relocation, right of ownership of assets deriving from crime or of other assets acquired in the place thereof, as well as of other rights relating to such assets;

the conversion, transfer, acquisition, possession or use of assets deriving

from crime or of assets acquired in the place thereof, the purpose of which is the concealment or maintenance of confidentiality of the illicit origin of the assets, or assisting a person who has participated in a criminal activity in order to enable such a person to avoid the legal consequences of his or her action.

If a criminal activity, which results in the acquirement of assets used in money laundering, takes place on the territory of another state, then this shall also be deemed to be money laundering.

1.5. Financing of acts of terrorism is financing or supporting an act of terrorism, incl. allocation or raising of funds to plan or perform acts, which are deemed to be acts of terrorism, or to finance the operations of terrorist organisations or in the knowledge that the funds allocated or raised will be used for the aforementioned purposes.

1.6. Politically exposed person is a natural person carrying out or having carried out significant duties of public authority, also family members and close colleagues of such person, except if the person has not carried out any significant duties of public authority for at least one year as of the date of transaction.

1.6.1. The following are persons carrying out significant duties of public authority (incl. respective officials of the European Union and international organisations):

(i) a head of state, a head of government, a minister, a deputy minister or an assistant minister;

(ii) a member of the parliament;

(iii) a judge of a supreme court, judgments of which can be appealed in exceptional cases only;

(iv) a member of the council of a state control authority or the council of a central bank;

(v) an ambassador, a charge d'affaires or a flag officer of the defence forces;

(vi) a member of the management body, supervisory body or administrative body of a state enterprise.

1.6.2. family member of a person carrying out significant duties of public authority is:

(i) his or her spouse;

(ii) his or her partner equivalent to a spouse under the law of the country of residence of the person or a person having a common household with him or her at least one year as of the date of signing the transaction;

(iii) his or her children and their spouses or partners in the meaning of clause (ii),

(iv) his or her parent.

1.6.3. Close colleague of a person carrying out significant duties of public authority is:

(i) a natural person having close business relations with the person carrying out significant duties of public authority or together with whom the person carrying out significant duties of public authority is a joint actual beneficiary in a legal person or a contractual legal entity;

(ii) a person who, as an actual beneficiary, has complete ownership of a legal person or a contractual legal entity that is known to have been established for the benefit of the person carrying out significant duties of public authority.

1.7. Compliance officer is an authorised employee, carrying out the duties specified in these This Manual and appointed by the director of AMG.

2. Due diligence measures

2.1. The goal of persons involved in money laundering or terrorist financing is to conceal their identity, the origin of funds, and the actual purpose of transactions. In order to prevent money laundering or terrorist financing through AMG, all managers and employees of AMG whose duties include establishment of business relations or conclusion of transactions shall implement the due diligence measures specified in these This Manual. The aim of said measures is to ensure, at all times, clarity with regard to the identity of any partners in legal relationships for the managers and employees of AMG. These measures are implemented for the purposes of transparency and reliability of the commerce of AMG and their implementation helps to reduce the counter-party and reputation risks and to increase credibility of the financial sector.

2.2. The managers and employees of AMG shall, in their economic activities, pay special attention to the operations of persons or clients participating in transactions or operations and to any circumstances, which could indicate money laundering or terrorist financing or which are likely to be related to money laundering or terrorist financing, including complex, high-value and unusual transactions without reasonable economic purpose.

2.3. The managers and employees of AMG shall implement the following due diligence measures as specified in these This Manual:

2.3.1. identifying and verifying the identity of a client or a party of a transaction;

2.3.2. identifying and verifying the identity and right of representation of a representative of a natural or a legal person;

2.3.3 identifying the actual beneficiary;

2.3.4. identifying the purpose and nature of business relations and transactions;

2.3.5. constantly monitoring business relations, regularly verifying and updating the data used for identification and, if necessary, identifying the source and origin of the funds used in a transaction;

2.3.6 detecting suspicious accounts and report them to appropriate supervisory personnel;
2.3.7 Maintaining an adequate audit trail that would allow competent authorities to trace all transactions that pass through the Firm in case of an investigation;

2.4. The managers and employees of AMG shall implement due diligence measures at least:
2.4.1. upon establishing lasting business relations;
2.4.2. upon carrying out one-off transactions involving a sum of over 10,000 US dollars our equivalent in any other currency, irrespective of whether the financial obligation is fulfilled with one payment or with multiple connected payments. For that purpose, the managers and employees of AMG shall, in all instances, assess the limits of transactions concluded with respective persons or persons monitored by them, as well as the nature of such transactions;
2.4.3. upon suspicion of money laundering or terrorist financing, irrespective of any derogations, exceptions or thresholds provided for by law;
2.4.4. upon suspicion of insufficiency or falseness of any documents or data collected earlier during identification of a person and verification of presented information or updating the corresponding data.

2.5. Implementation of reinforced due diligence requirements shall be triggered, *inter alia*, by the following circumstances:

(i) the places of business or the place of residence and/or seat of the representative and the principal are located in different jurisdictions;
(ii) the authorisation (except for a statutory right to represent a legal person) has been issued for a term of over one year;
(iii) large transactions (transaction amount over 10,000 US Dollars) and complex transactions;
(iv) transactions that deviate significantly from the previous normal transaction history of the person;
(v) transactions involving large asset transfers to a country that is not the known home country of the person;
(vi) the social appearance and behaviour, personal financial situation or other circumstances surrounding the person are irregular considering the characteristic features of the transaction to be concluded or the business of the principal.

2.6 The country of origin and the names of all clients and their banks shall be checked against the following government-issued lists:

2.6.1 Sanctioned Countries:
The current list of sanctioned countries, as well as detailed descriptions of the sanctions may be found at:

FATF webpage: http://www.fatf-gafi.org/countries/
US Office of Foreign Assets Control (OFAC): http://www.treasury.gov/resource-center/sanctions/Pages/default.aspx

2.6.2 Specially Designated Nationals (SDN)

The List of Specially Designated Nationals and Blocked Persons contains the names of individual and corporate entities sanctioned against by the US. The list is maintained by OFAC. The current list of sanctioned entities may be found at: http://www.treasury.gov/resource-center/sanctions/Pages/default.aspx

2.7 Deposit and Withdrawal Screening

2.7.1 For all deposits and withdrawals, transfer of funds between AMG and client must always be between the accounts of the same beneficiary. All third party transfers are forbidden without the express approval of management board. Such permission may be given only in cases where management board believes that it has sufficient proof from the customer as to the legitimacy of the transfer.

2.7.2 Each withdrawal will be screened by Back Office if the customer is listed in the AMG's High Risk Accounts list. All transactions by a High Risk customer will be reported to the Compliance Officer to obtain approval for the transaction. The Compliance Officer will review the trading and transaction history of any such account before determining whether or not to approve the withdrawal as requested by client.

2.7.3 The bank used by the customer shall be checked against the Sanctions Lists as in Section 2.6. In transactions where the beneficiary bank is located in a region prohibited by the Sanctions List, Back Office will immediately notify the Compliance Officer. Compliance officer will review the instructions published in the Sanctions order and act accordingly. The bank used by the customer shall be checked against the list. In transactions where the beneficiary bank is positively matched, the funds being transferred will be diverted into a special blocked account and frozen. The Financial Intelligence Unit will immediately be notified of such action through its reporting process by the Compliance Officer.

2.7.4 SC will not process a withdrawal to a foreign bank account with no physical headquarters in any jurisdiction (Also known as "Shell Banks".)

2.7.5. Any single or a sequence of smaller deposits in total value of 10,000 US Dollars or greater (and equivalent size deposits foreign currencies) must be forwarded to Compliance Officer for review and approval prior to processing. When conducting reviews of such large-size deposits, the Compliance Officer reviewing the deposit

will consider factors such as the anticipated versus observed volume and activity in the account, as well as the known financial information of the customer. The Compliance Officer should obtain additional information as necessary in order to make a reasonable assessment of the deposit.

3. Extent of implementation of due diligence measures (risk analysis)

3.1. The extent of implementation of due diligence measures shall be determined by AMG in consideration of the nature of transaction or the risk level of the party to transaction/operation. A manager or employee of AMG shall pay special attention to circumstances that could indicate money laundering or terrorist financing and shall implement reinforced due diligence measures if the circumstances of a business relationship or transaction or the circumstances surrounding a person are associated with a high risk of money laundering or terrorist financing. A manager or an employee of AMG may implement simplified due diligence measures in connection with the risk level of a particular transaction or person if the circumstances surrounding such a transaction or person are associated with a lower risk of money laundering or terrorist financing.

3.2. If there is no requirement to implement reinforced due diligence measures or no grounds for implementing simplified due diligence measures, a manager or employee of AMG shall implement general due diligence measures.

3.3. The assessment of the risk of money laundering and terrorist financing shall include assessment of geographic risk, client risk and risk associated with the transaction or operation.

3.4. Assessment of geographic risk

3.4.1. Geographic risk and the risk of money laundering or terrorist financing shall be assessed as high if the client or transaction or operation is associated with the following countries or territories:

(i) countries or territories subject to United Nations, United States Treasury and the Office of Foreign Assets Control (OFAC), European Union sanctions, embargoes or other similar measures;
(ii) countries identified by the Financial Action Task Force (FATF) as having insufficient requirements for prevention of money laundering and terrorist financing;
(iii) countries that have been reliably linked to supporting terrorism or have a high level of corruption.

3.5. Customer risk assessment

3.5.1. The level of customer risk shall be assessed as high if:

(i) a legal person's structure, legal form or relations with other persons do not enable a

manager or an employee of AMG to identify the actual beneficiary with sufficient degree of confidence;
(ii) the majority of the share capital of a legal person is made up of bearer shares;
(iii) a person has a foreign state background;
(iv) a person is entered in a United Nations, United States Treasury, European Union list of persons who are subject to international financial sanctions or a person is registered in a low-tax area;
(v) the business area of a person is associated with a higher risk of money laundering or terrorist financing;
(vi) a manager or an employee of AMG is previously aware of a suspicion of money laundering or terrorist financing associated with the person.

3.5.2. The business areas associated with a higher risk of money laundering or terrorist financing, referred to in point (v) of clause 3.5.1, shall be defined in writing by the Compliance Officer and shall be immediately notified to the employees of SC. For the purposes of defining such business areas, the Compliance Officer shall communicate with competent supervisory authorities and shall consider measures frequently used for money laundering, including the money laundering trends discovered and disclosed by the Financial Intelligence Unit.

3.6. Assessment of transaction or operation risk

3.6.1. Risk associated with a transaction or an operation shall be assessed as high if:

(i) the purpose of a transaction could be concealment of the actual parties to or actual objects or rights of the transaction;
(ii) a transaction lacks a reasonably comprehensible commercial, financial, legal or other purpose (the transaction deviates from regular economic activities of the person or differs significantly from payment and behaviour patterns of other similar clients);
(iii) a manager of employee of AMG suspects for any reason that a transaction or operation can be associated with money laundering or terrorist financing;
(iv) large transactions of over 10,000 US Dollars in value are concluded in cash;
(v) a transaction is paid for by a person not associated with the party to transaction.

3.6.2. Risk associated with a transaction or operation is assessed as low if the transaction does not enable the person to remain anonymous and, if necessary, a manager or an employee of SC is immediately able to implement all due diligence measures in case of suspicion of money laundering or terrorist financing. Risk level shall be deemed as low if:

(i) a transaction or operation is concluded in the framework of a long-term contract (lasting business relationship) with the client;
(ii) profit from a transaction is not realised as a third-party profit, except in case of death, incapacity for work, reaching of a previously established old age limit or a similar event;

(iii) a payment is made via the account of the person participating in the transaction or the client and the account has been opened in a credit institution in a country where requirements equivalent to those specified in the Money Laundering and Terrorist Financing Prevention Act are in force;
(iv) the total annual value of fulfilling monetary obligations resulting from transactions of this type will not exceed 10,000 US Dollars;
(v) in case of transactions with shares in investment funds, the profit from the transaction cannot be realised by the client before one year from the transactions, the shares in the investment fund being the object of transaction cannot be used as a security for other transaction, the transaction is not concluded via payment in due course, and the contract does not include a client's redemption clause.

3.8. Assessment of risks associated with a client and/or a transaction should always be performed in consideration of characteristic features of persons or transactions as specified in legislation or guidelines of competent authorities for the purpose of establishing higher or lower risk level, as well as of typical cases encountered by managers and employees of AMG in the performance of duties arising from these This Manual, which should result in a map of sample cases for employees and managers to determine the risk level associated with clients and transactions or operations.

DUE DILIGENCE MEASURES IN PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

4. Identification of natural persons

4.1. If a person, who does not have a lasting business relationship with AMG, is provided a service for the first time or any other transaction is concluded with such a person for the first time, he or she shall be identified by being in the same location with the person or a representative to be identified.

4.2. Presentation of one of the following documents shall be requested from the natural person or a representative of a legal person for the purposes of identification:

(i) ID card;
(ii) passport;
(iii) a valid driving licence, including the name, photograph or facial image, signature or image of signature, and date of birth or personal identification code of the holder;

(iv) a valid travel document (passport) issued in a foreign country;
(v) a diplomatic passport;
(vi) a seafarer's discharge book;
(vii) an alien's passport;

4.3. If a document referred to in clause 4.2 cannot be presented for identification, the identity of the person can be determined and verified by using notarised or officially authenticated documents and AMG shall only perform the transaction if there are no doubts regarding the identity of the other party.

4.6. To identify a natural person, a manager or an employee of AMG shall record the following details of the natural person:
(i) name of the person and name of the representative (if any);
(ii) personal identification code or, if unavailable, time and place of birth;
(iii) address of the person's actual place of residence;
(iv) the person's profession or area of activity;
(v) name and number, date of issue, and name of the issuing authority of the document presented for identification and verification of identity;
(vi) in case of a foreign resident, the fact whether he or she is a person having a state background by asking the client to provide relevant information and, if necessary, verifying it via available databases (e.g., Internet search engines);
(vii) telephone number and email address.

4.7. In terms of profession or area of activity, AMG shall assess the usual business transactions and operations of the person and, if necessary, shall ask for additional information on the client's planned economic behaviour to enable subsequent assessment of whether any particular transactions are beyond the person's ordinary course of business or not.

4.8. If all personal data cannot be determined on the basis of presented documents, additional data or documents shall be requested for identification.

5. Identification of legal persons

5.1. Legal persons shall be identified by identifying the legal form, objectives of activities, profile, legal capacity, members of management bodies of the legal person, using the procedure specified in this section, as well as any representatives and the basis, extent and term of their authorisation.

5.2. To identify a legal person, a manager or employee of AMG shall record the following information regarding that legal person, based on the submitted identification document or, if necessary, additional requests for information:

(i) name of the manager or names of the members of the management board or other body substituting for a management board, and their authority in representing the legal person;
(ii) area of activities and principle place of business;
(iii) numbers of communication means;
(iv) data of the actual beneficiaries of the legal person identified according to This Manual;
(v) in case a person having a foreign state background is associated with the legal person, the information on that person having a state background shall be recorded by asking the client to provide relevant information and, if necessary, verifying it via public databases (e.g., Internet search engines).
(vi) Articles of Incorporation

5.4. In terms of area of activities, AMG shall assess the usual business transactions and operations of the person and, if necessary, shall ask for additional information on the client's planned economic behaviour to enable subsequent assessment of whether any particular transactions are beyond the person's ordinary course of business or not.

5.5. If the required information or documents cannot be obtained, the person shall be identified by using notarised or notarial or officially authenticated documents and AMG shall only perform the transaction if there are no doubts regarding the identity of the other party.

5.6. If all personal data cannot be determined on the basis of presented documents, additional data or documents shall be requested, in particular, to determine legal capacity of a foreign legal person, and in doing so AMG shall be guided by, *inter alia*, the guidelines issued by the competent authorities. When determining the right of representation, the managers and employees of AMG shall pay special attention to companies founded in low-tax countries or areas where existence of legal capacity is not always unambiguous.

6. Identifying and verifying the identity and right of representative

6.1. A manager or an employee of AMG shall determine, whether the person acts on his or her own behalf or as a representative on behalf and/or on account of another person.

6.2. If the person acts as a representative, the manager or employee of AMG shall identify both the principal and the representative. This shall be done according to the

procedure established for identifying natural persons or legal persons, respectively.

6.3. The basis, extent and term of the right of representation shall be verified in addition to identification and verification of the identity of the representative. For that purpose, the manager or employee of AMG shall request, in addition to the documents required for identification, also a proof of the right of representation (if the right of representation does not arise from the document presented for identification).

6.4. The proof of the rights of a representative shall indicate at least the name of the document, date of issue and the name of the issuer. A document certifying the right of representation shall be notarised or equivalently authenticated and properly legalised, unless otherwise stipulated in an international agreement. If additional requirements for the proof of the right of representation are set out in legislation, the proof of the right of representation shall also comply with the requirements of legislation.

6.5. The manager or employee of AMG shall verify the validity and extent of authorisation. The manager or employee of AMG may not conclude a transaction or operation with a representative if the right of representation is not properly formalised, has lapsed, or does not cover conclusion of this particular transaction or operation.

6.6. If a manager or employee of AMG suspects that the person is not an actual representative of the company, he or she shall carry out an interview to clarify whether the person is familiar with the principal, understands the circumstances associated with the transaction or the business of the principal, and is able to provide adequate clarifications and assessments regarding those (incl. regarding the place of business, areas of activity, turnover and transaction partners, other associated persons and final beneficiaries of the principal). The representative must be able to demonstrate convincingly the legal origin of assets of the principal used in the transaction.

7. Identifying the actual beneficiary

7.1. The actual beneficiary shall be identified during identification of a legal person. Identification of the actual beneficiary shall not be required if the securities of the respective company have been accepted for trade in a regulated market.

7.2. An actual beneficiary is a natural person who exercises final control over a transaction and in the interest of whom the transaction is carried out. An actual beneficiary is also a natural person who:

7.2.1. holds more than 25 per cent of shares or voting rights through direct or indirect holding or control, including in the form of bearer shares; or

7.2.2. controls the management of a legal person in another manner; or

7.2.3. is, to a previously determined extent of at least 25 per cent, a beneficiary with regard to the assets of a legal person, civil law partnership or another similar contractual legal entity engaged in the administration or distribution of assets, or who significantly controls the assets of the legal person, civil law partnership or another similar contractual entity to an extent of at least 25 per cent; or

7.2.4. is, to an extent previously not determined, a beneficiary with regard to the assets of a legal person, civil law partnership or another similar contractual legal entity engaged in the administration or distribution of assets, and in whose interests primarily the legal person, civil law partnership or another similar contractual entity was founded or is operating.

7.3. The managers and employees of AMG shall record and preserve in a collated manner all descriptions of typical cases of identifying actual beneficiaries, thereby establishing a map of sample cases for employees and managers to identify actual beneficiaries.

7.4. Identification of the actual beneficiary shall be based on the company register documents if they specify the structure of ownership of the company.

7.5. If the register data do not enable identification of an actual beneficiary or there are doubts about the identity of the actual beneficiary (e.g., if the legal person specified as the owner has been registered in a low-tax area or jurisdiction where identification of persons controlling the company is complicated), a manager or an employee of AMG shall, as required and on the basis of performed risk analysis, request suitable documents of proof (e.g., tax returns or confirmation of a taxation authority, account statements of the actual beneficiary, etc.) to verify any statements of a representative of the legal person. Any documents issued by foreign institutions or companies have to be legalised according to the established procedure.

7.6. If an actual beneficiary cannot be identified with a sufficient degree of confidence, AMG shall refuse the conclusion of transaction or operation and shall, according to the procedures specified herein, notify the Financial Intelligence Unit of the person's intent to perform the transaction.

8. Due diligence measures in conclusion of transactions

8.1. In order to implement due diligence measures, a manager or an employee of AMG shall collect information on the business activities of the client and on the purpose and nature of the particular planned transaction or operation.

8.2. The client's activity profile shall be determined during establishment of the client relationship considering, *inter alia*, the nature, regularity, volume and other relevant factors pertaining to the transactions of the client. This shall be done, as required, by requesting from the client additional information and/or documents, using other legal options for obtaining information on the client, analysing the client's previous payment patterns, and implementing other suitable and reasonable measures depending on circumstances. In case of a legal person, the objectives of its activities and, if possible, the main business partners shall be identified.

8.3. The managers and employees of AMG shall pay special attention to transactions beyond a client's ordinary course of business, as well as complex and unusually large transactions or unconventional transaction schemes without an obvious or discernible economic or legal purpose, as well as transactions associated with persons from countries where obtaining information on the person is complicated, or transactions with persons from countries that do not make sufficient efforts to prevent money laundering[1].

8.4. Reinforced due diligence measures shall be implemented in case of unusual transactions where the assessed risk of money laundering or terrorist financing is high and also in case of a suspicion of criminal background of the funds.

8.5. Electronic orders may not be executed automatically, without a prior analysis according to the procedure specified herein.

8.6. When concluding a transaction, a manager or an employee of AMG shall record the following details of the transaction with a person:

(i) date or period of transaction;
(ii) description of the content of transaction;
(iii) amount of transaction;
(iv) payment currency and account number;
(v) type of security, monetary value of transaction, currency and account number in case of redemption of fund units or shares or payments associated with other securities;
(vi) information and documents submitted by the client for the provision of the service.

[1] See Non-Cooperative Countries and Territories (http://www.fatf-gafi.org)

9. Monitoring of client relationships and updating of personal data

9.1. The managers and employees of AMG shall continuously monitor the circumstances associated with the business activities of a client, including transactions

concluded, regularly verify the details used for identification, update any relevant documents and data and, if necessary, identify the source and origin of the funds used for transaction.

9.2. Clients shall be classified into low-risk and high-risk clients according to current relevant data on the nature and prevalence of measures and methods used for money laundering and terrorist financing and any potential changing trends in such circumstances. High-risk clients shall be clients requiring implementation of reinforced due diligence measures. High-risk clients, their transactions and details shall be verified after shorter intervals and in a more thorough manner, at least once a year. Low-risk clients shall be clients with regard to whom simplified due diligence measures may be implemented. Low-risk clients, their transactions and details shall be verified at least once every two years. A client's details shall always be verified and updated in case of suspicion or knowledge that a significant change has occurred in the client's details.

9.3. The due diligence requirement shall be fulfilled by conducting an analysis of client transactions to detect any anomalies in the client's transactions, which deviate from the client's profile of operations and could be indicative of characteristics of money laundering or terrorist financing in the client's behaviour.

9.4. Any suspicious transactions shall be assessed separately to determine any possible links of the transactions or funds used to money laundering or terrorist financing.

9.5. Detection and assessment of suspicious transactions shall be based, *inter alia*, on the Financial Intelligence Unit regarding transactions with a money laundering or terrorist financing suspicion.

9.6. In case of an unusual transaction, a transaction significantly deviating from the past profile of operations or a suspicious transaction, it shall be determined whether it is associated with any circumstances that are different in terms of the client's past behaviour but have a reasonable explanation, a special transaction caused by a significant change of circumstances surrounding the client, or a transaction with a suspicion of money laundering/terrorist financing. Any circumstances that cannot be reasonably explained and/or certified shall be interpreted as suspicious in terms of money laundering.

9.7. The following actions are also required to perform the operation specified in clause 9.6:

9.7.1. analyse and compare the discovered circumstances of transaction with the characteristics of transactions with a money laundering suspicion;

9.7.2. verify the origin of assets;

9.7.3. investigate the contents of previously received information with regard to the client's previous payment patterns and other known information;

9.7.4. submit inquiries in a form allowing reproduction in writing to obtain additional information on the client and to preserve the responses to such inquiries.

9.8. The Compliance Officer shall systematically and regularly verify the data used for identification, based on the nature of each client relationship and the client's risk profile. For that purpose, a manager or an employee of AMG shall ask the client to confirm the accuracy of previously submitted data or, if necessary, to re-submit the required identification documents; this shall be done in any case if the previously submitted documents are older than three years or there are suspicions regarding the accuracy of the information.

9.9. When providing services to a customer via electronic means of communication, SC shall implement electronic measures to verify the client's personal data by asking the person to submit an electronic confirmation of the accuracy of the personal data previously submitted to AMG.

9.10. When verifying a client's details, the Compliance Officer shall, as required and based on the principle of reasonableness, submit queries on legal grounds to registers, ask for confirmations from clients and/or supervision authorities, and shall implement other legal measures to obtain the necessary data.

10. Simplified and reinforced procedure for implementing due diligence measures

10.1. If there are grounds for implementing simplified due diligence measures as specified in these This Manual (see section 3), a manager or an employee of AMG shall have the right, after identification of the representative and verification of authorisation, to implement other due diligence measures at his or her own discretion if the manager or employee of AMG has collected sufficient information and documents to establish that the client meets the criteria of low risk of money laundering and terrorist financing. The extent of due diligence measures shall be based

on the nature of the business relationship or transaction or the risk level of the person or client participating in transaction or operation. When implementing simplified measures, the relevant employee or manager shall record this fact, the extent of measures implemented and a justification of sufficiency of limited implementation of due diligence measures in a form allowing reproduction in writing.

10.2. Simplified due diligence measures shall not be implemented in case of suspicion of money laundering or terrorist financing.

10.3. If a person or transaction has a high risk of money laundering or terrorist financing and, consequently, there are grounds specified in this Manual for implementing reinforced due diligence measures (see section 3), a manager or an employee of AMG shall, in addition to general due diligence measures, implement one or several of the following measures as necessary:

10.3.1. additional identification of the person and verification of identity on the basis of data obtained from an official national register or other reliable and independent sources;

10.3.2. request notarisation or official authentication of the documents submitted by the person or confirmation of the accuracy of a document issued by a credit institution by that credit institution;

10.4. Reinforced due diligence measures shall be implemented in case of establishing business relations and concluding transactions or operations with a person having a political exposure. If an employee of AMG identifies a politically exposed person, he or she shall immediately notify the management board of AMG. Only the management board of AMG shall decide a transaction or operation with a politically exposed person if there is sufficient proof of the origin of the money or other assets used for establishing the business relationship or concluding the transaction. The decision on concluding the transaction or operation shall be formalised in writing. Persons having political exposure shall be subject to continuous implementation of due diligence measures to monitor the business relationship, verify and update the documents and data used for identification, and to identify the source and origin of the funds of such persons.

10.5. If a correspondent account is opened in a credit institution of a third country, AMG shall implement reinforced due diligence measures, which shall include continuous assessment, based on publicly available information, of reliability and reputation of the credit institution, efficiency of supervision over that institution, as well as the internal control systems of the credit institution for preventing money laundering and terrorist financing.

10.6. AMG shall not open a correspondent account in a credit institution that meets at least one of the following criteria:

10.6.1. the actual place of management or operations of the credit institution is located outside its location country and the credit institution is not a part of a consolidated group or corporation of credit or financial institutions subject to sufficient supervision

(shell bank);

10.6.2. an assessment of the reliability of the credit institution's managers and measures for prevention of money laundering and terrorist financing results in shortcomings being discovered according to the standards applicable to and applied by AMG or on the basis of the circumstances used as a basis for the assessment specified in this section.

10.7. In case of establishing correspondent relations, the parties shall conclude a binding agreement in a form allowing reproduction in writing, which shall also set out the obligations and liability of both parties in connection with implementation of the measures for prevention of money laundering and terrorist financing, including expanded usage rights in case of implementation of due diligence measures in relation to the accounts.

11. Actions in case of a suspicion of money laundering or terrorist financing

11.1. The manager of AMG shall appoint a Compliance Officer, charged with the task of coordinating and controlling compliance with the requirements for prevention of money laundering, forwarding information on suspicions of money laundering to the Financial Intelligence Unit, organising collection and analysis of information indicative of unusual transactions or transactions with a money laundering or terrorist financing suspicion, reporting to the management board and supervisory board of AMG on the progress and shortcomings in internal implementation of This Manual, as well as performing other duties arising from This Manual, the employment contract and the job description.

11.2. The Compliance Officer shall be subordinated to and shall report to the director of AMG. The Compliance Officer shall, at least once a year, submit to the management board and supervisory board a report on the progress and shortcomings in internal implementation of This Manual during the reporting period, as well as on the measures applied to eliminate the shortcomings and the efficiency of said measures. The management board of AMG shall, at any time, have the right to request from the Compliance Officer information on implementation of measures for prevention of

money laundering and terrorist financing in the company.

11.3. The Compliance Officer shall be independent in the performance of his or her duties. The management board of AMG shall provide the Compliance Officer with competence and resources required for the performance of duties, in particular internal access to all relevant information, especially information on clients and identification of clients and information on transactions.

11.4. All employees of AMG shall notify the Compliance Officer of any unusual clients and transactions, as well as clients and/or transactions where a suspicion of money laundering or terrorist financing has emerged. In addition, the employees of AMG shall immediately notify the Compliance Officer of any known failures to comply with the requirements for prevention of money laundering and terrorist financing. Such circumstances may also be reported directly to the management board of AMG. The Compliance Officer shall analyse the received information and shall decide whether the circumstances require notifying the Financial Intelligence Unit.

11.5. The Compliance Officer shall have the right to receive from the managers and employees of AMG additional information on suspicious or unusual transactions, operations or circumstances and the managers and employees of AMG shall immediately submit the relevant information at the request of the Compliance Officer.

11.6. If the Compliance Officer has discovered or has been informed of circumstances indicative of money laundering and/or terrorist financing or with a suspicion or knowledge of money laundering or terrorist financing, the Compliance Officer shall immediately notify the Financial Intelligence Unit as well as the management board and supervisory board of AMG. At the same time the Compliance Officer shall decide on postponement of the relevant transaction in case of a suspicion of money laundering and/or terrorist financing by submitting a respective instruction to the relevant manager or employee of AMG. If postponement of the transaction could cause significant damage to the parties, it is impossible to cancel the transaction or it could prevent capturing the person who allegedly committed money laundering or terrorist financing, the relevant transaction or operation shall be concluded and the Financial Intelligence Unit shall be notified immediately thereafter.

11.7. If, after analysing the information received, the Compliance Officer concludes that a circumstance or transaction does not warrant a notification to the Financial Intelligence Unit, the Compliance Officer shall make a separate decision on the need to take the respective person under increased surveillance, in which case the Compliance Officer shall notify the managers and employees of AMG of the requirement to implement reinforced due diligence measures with regard to said person.

11.8 If reporting suspicious activity to Financial Intelligence Unit, the Compliance Officer shall use the reporting form provided on the Financial Intelligence Unit website. The Suspicious Activity Report (“SAR”) must be filed immediately upon noticing the

suspicious incident. Upon filing, a copy of the SAR report and any supporting documentation must be retained for a period of 5 years from the date of the filing of the SAR. The Firm shall identify supporting documentation at the time the SAR is filed, but will not attach it to the SAR. Copies of all supporting documentation for a particular SAR will be maintained in a single file folder bearing the name and account number of the account holder, or scanned and maintained in a data file bearing the same identifying information.

11.9 if AMG has reason to suspect that a customer's transactions may be linked to terrorist activity, the Compliance Officer must immediately call Financial Intelligence Unit;

11.10. A manager or an employee of AMG shall not notify the person, his or he representative, the actual beneficiary or any third parties of the notification submitted to the Financial Intelligence Unit, suspension of transaction or any other implemented measures or initiation of criminal procedure, except in cases where such a right arises from law. A person may be notified of any sanctions taken in relation to that person only after the sanction has been implemented.

11.11. AMG shall refuse to create a business relationship or to conclude a transaction if the person or client participating in the transaction or operation, despite a respective request, fails to submit the documents and relevant information required for implementation of due diligence measures or if any submitted documents lead even to a slightest suspicion of money laundering or terrorist financing. In such a case, the employee of AMG shall immediately notify the Compliance Officer thereof and shall follow any subsequent instructions of the Compliance Officer. The employee shall also record as much details on the suspicious transaction and the person intending to conclude such a transaction. AMG shall also refuse to establish business relations and/or conclude a transaction if the client uses a mailbox number or demand address as his or her address.

11.12. AMG shall ensure existence of legal grounds for extraordinary termination of a client relationship without the advance notice period in case of a suspicion of money laundering or terrorist financing in connection with the client's transactions or if the client, despite a respective request, fails to submit a proof of legal origin of the money or other assets, which are the object of the transaction. The aforementioned circumstances shall be immediately notified to the Compliance Officer and management of AMG who shall decide on extraordinary termination of the client relationship.

11.13. Notification on the circumstances associated with the suspicion of money laundering or terrorist financing shall be transmitted to the Financial Intelligence Unit in writing or another manner agreed with the Financial Intelligence Unit.

11.14. The notification shall be submitted in a format established by Financial Intelligence Unit and Combating the Financing of Terrorism (AML/CFT) Guidelines for Banks, Financial Institutions, Credit Unions and Money Transfer Services Providers.

12. Data storage

12.1. AMG shall store all the data below in a form allowing reproduction in writing (in writing as files or electronically in the servers of AMG):

(i) documents required for identification of natural and legal person and registered data;
(ii) documents and data collected for verifying a representative's right of representation and for identifying and verifying the actual beneficiary;
(iii) data collected and compiled in connection with a transaction;
(iv) notifications received from the managers and employees of AMG regarding suspicious and unusual transactions, as well as information collected for analysing such notifications and other related documents;
(v) information on the circumstances of withdrawing from business relationships or refusing to conclude a transaction and circumstances of terminating the business relationship;
(vi) notification submitted to the Financial Intelligence Unit together with the time of submission and details of the submitting employee.

12.2. In case of data collected in the course of implementing due diligence measures, the relevant employee of AMG shall record in a form allowing reproduction in writing the time and place of data submission, the reason for identification of a person (use of a service, updating client's details) and details of the employee who performed the identification.

12.3. In case of a change in personal data, the identification document used as a basis for amendment of personal data, the time and place of amendment of personal data and the details of the employee who amended the client's data or verified the submitted data or documents shall be registered in a form allowing reproduction in writing.

12.4. Any data collected in the course of implementing due diligence measures for prevention of money laundering and terrorist financing (incl. data collected for identification and verification of identity, transaction data and data on transmitted notifications) shall be stored for at least five years after termination of the contractual relationship with the respective client or conclusion of the transaction/operation in a systematic form and in a manner that enables quick finding of such data and submissions to competent authorities.

13. Training of employees

13.1. During hiring procedure, AMG shall provide all its employees with information on the obligations arising from the MLTPA and this Manual and any other internal

procedures for the performance of such obligations and shall arrange for additional training as required. The Compliance Officer shall assess the need for additional training and shall make respective proposals.

13.2. Notifications and information provided to employees shall also be based on the following:

13.2.1 the employees shall be given an overview of the legislation on prevention of money laundering and terrorist financing and of relevant guidelines, corresponding international regulations and the objectives thereof;

13.2.2. a uniform interpretation of the objectives established by legislation on prevention of money laundering and terrorist financing and by other relevant documents shall be developed among the employees;

13.2.3. the employees shall be notified of the sanctions applicable in case of failure to comply with the requirements of the MLTPA

14. Delegation of duties

14.1. AMG shall have the right, for better performance of its obligations related to business activities, to delegate a part of the obligations arising from legislation and This Manual to third parties. Delegation of obligations shall not relieve AMG from liability for inadequate performance of such obligations.

14.2. If obligations are delegated to third parties, the training requirements specified in This Manual shall be applicable to such third parties and the third parties shall, in performing the duties associated with prevention of money laundering and terrorist finance, comply with the requirements arising from these This Manual.

14.3. When selecting the third parties, establishing legal relationships with them and monitoring their activities, AMG shall rely on relevant legislation and the internal rules of procedure for delegation of activities.

Annex 1. Examples of suspicious activity – "Red Flags"

There are a myriad of ways in which money laundering or terrorism financing may occur. Below is a non–exhaustive list of "Red Flags" that may warrant closer attention.

General

If the Client:
• Does not want correspondence sent to home address.
• Shows uncommon curiosity about internal systems, controls and policies.
• Over justifies or explains the transaction.
• Is involved in activity out-of-keeping for that individual or business.
• Produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
• Provides insufficient, false, or suspicious information, or information that is difficult or expensive to verify.

Economic Purpose

• Transaction is unnecessarily complex for its stated purpose.
• Activity is inconsistent with what would be expected from declared business.
• Transaction involves non-profit or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.
• Accounts that show virtually no trading activity but are used to receive or pay significant amounts not clearly related to the Customer.

If the Client:
• Starts conducting frequent cash transactions in large amounts when this has not been a normal activity in the past.
• Deposits small amounts of cash on different successive occasions in such a way that on each occasion the amount is not significant, but combined, total a very large amount. (i.e. "smurfing").
• Consistently makes cash transactions that are just under the reporting threshold amount in an apparent attempt to avoid the reporting threshold.
• Stated occupation is not in keeping with the level or type of activity (e.g. a student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area).

• Unusually large deposits or withdrawals of cash by an individual or a legal entity whose apparent business activities are normally carried out using cheques and ohter monetary instruments.

Deposit Activity

• Funds are being deposited into several accounts, consolidated into one and transferred outside the country.

• Account with a large number of small cash deposits and a small number of large cash withdrawals.
• Establishment of multiple accounts, some of which appear to remain dormant for extended periods.
• Account that was reactivated from inactive or dormant status suddenly exhibits significant activity.
• Reactivated dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by frequent cash withdrawals until the transferred sum has been removed.

Cross-border Transactions

• Deposits followed within a short time by wire transfers to or through locations of concern, such as countries known or suspected to facilitate money laundering activities.
• Transaction involves a country where illicit drug production or exporting may be prevalent, or where there is no effective anti-money laundering system.
• Immediate conversion of funds transfers into monetary instruments in the name of third parties.
• Frequent sending and receiving of wire transfers, especially to or from countries considered high risk for money laundering or terrorist financing, or with strict secrecy laws. Added attention should be paid if such operations occur through small or family-run banks, shell banks or unknown banks.
• Large incoming or outgoing transfers, with instructions for payment in cash.
• Client instructs you to transfer funds abroad and to expect an equal incoming transfer.
• Client sends frequent wire transfers to foreign countries, but business does not seem to have connection to destination country.
• Client is not employed but makes frequent large transactions or maintains a large account balance.
• Transactions are with persons in jurisdictions that do not have adequate systems in place to prevent money laundering/terrorist financing.