

DELTASTOCK AD
ANTI MONEY LAUNDERING POLICY
June 2009

[Approved by the Directors, Procurator and MLRO]

CONTENTS

1. STATEMENT	1
2. SCOPE.....	2
3. AML POLICY.....	2
4. COMPLIANCE	3
5. PRODUCTS & SERVICES.....	4
6. MONEY LAUNDERING.....	4
7. RISK ASSESSMENT	5
8. CUSTOMER IDENTIFICATION	6
9. VERIFYING INFORMATION.....	6
10. GOVERNMENT LISTS CHECK.....	6
11. MONITORING & REPORTING	7
12. SUSPICIOUS ACTIVITY	7
13. ONLINE PAYMENTS & ELECTRONIC FUND TRANSFER	10
14. INVESTIGATION	11
15. RECORD KEEPING.....	11
16. TRAINING	11
17. POLICY TESTING AND REVIEW.....	12
18. ADMINISTRATION.....	12

1. STATEMENT

1.1 Deltastock AD and its wholly owned subsidiaries and branches ("Deltastock Group") in the regulated financial services business are committed to risk management and have adopted an Anti-Money Laundering (AML) compliance policy ("Policy") as set forth in the Board minutes of its respective financial services companies, updated June 2009, to prevent money laundering, fight crime and terrorist financing by incorporating compliance with the:

1.1.1 EU Third Money Laundering Directive 2006/70/EC;

1.1.2 Anti Money Laundering Act 1998 as amended, Law on the Measures against Money Laundering 2003, the Prevention of Terrorist Financing Act 2003 as amended, Law on the Measures against Terrorist Financing 2003 as amended and the Penal Code 1968 as amended under Bulgarian law, and

1.1.3 Money Laundering Regulations 2007 including the Terrorism Act 2000, as amended by the Anti-Terrorism Crime and Security Act 2001; the Proceeds of Crime Act 2002 as amended by the Serious Organised Crime and

Police Act 2005; and the Counter Terrorism Act 2008 under English law.

- 1.2 The AML Policy is to be read in conjunction with the current version of the AML Manual for each company within the Deltastock Group.

2. SCOPE

- 2.1 This policy applies to the Deltastock Group companies, wherever located within the European Community, its directors, MLRO, officers and employees who deal with customers in relation to Deltastock products and services.
- 2.2 Each company and branch within the Deltastock Group will implement risk sensitive approach procedures to identify customers, avoid, prevent, detect and report on transactions at first instance to their MLRO internally for review and who will be responsible, in appropriate cases, for making suspicious activity reports or other reports required to the law enforcement agencies and regulatory authorities.

3. AML POLICY

- 3.1 It is the policy of Deltastock Group to prohibit and actively pursue the prevention of money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities or such acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have been derived from legitimate origins or constitute legitimate assets.
- 3.2 Deltastock Group is committed to AML compliance in accordance with applicable law and aims to establish such procedures of internal control and communication as may be appropriate for the purpose of forestalling and preventing money laundering activity.
- 3.3 Its directors, MLRO, officers and employees dealing directly with customers are required to comply with internal systems and controls and procedures in their AML Manuals in the prevention of use of its products and services for money laundering or funding of terrorists or criminal activities.
- 3.4 It is the policy of Deltastock Group not to undertake:
 - 3.4.1 to enter into business relationships or execute transactions where details of the customer and/or beneficiary are unknown or cannot be identified or verified;
 - 3.4.2 cash transactions directly from its customers, with the exception of Romania and Bulgaria;
 - 3.4.3 transmissions of funds to any individuals or politically exposed persons (PEPs) and their family and close associates or political parties known to be supporting terrorism or suspected criminal organizations;

- 3.4.4 the opening of customer accounts or the establishment of customer relationships with shell banks incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial institution or group; and
- 3.4.5 transactions for customers who refuse to provide identification information and documents when requested or who produce misleading information.
- 3.5 Records of such reports and supporting documentation, as required by anti-money laundering law and regulations, will be retained and kept for a period of five years or in accordance with the provisions of the relevant law and regulation of the country in which the company within Deltastock Group operates.
- 3.6 All internal MLRO reports of suspicious activity and external reports to the governmental enforcement agencies and regulatory authorities will be documented in Deltastock Group records.

4. COMPLIANCE

- 4.1 The Board of Directors, Procurator and MLRO of Deltastock Group (“Management”) shall have full responsibility for the AML Policy, the design, implementation and update of the Policy as required; its dissemination of updated information to its officers and employees who deal directly with customers within the Deltastock Group.
- 4.2 Each company and branch under the Deltastock Group will have its own MLRO who will report directly and be supervised where appropriate by Management.
- 4.3 The MLRO will be responsible for the upkeep and maintenance of the AML Manual and ensure they are kept abreast of guidance published by EC, domestic government and regulatory recognised sources of AML guidance for the financial services industry within their countries of operation such as the Financial Supervision Commission in Bulgaria and the Financial Services Authority and The Treasury in the UK.
- 4.4 Management will also be responsible for putting in place adequate systems and controls to enable due diligence checks be made on the identification and verification of customers before establishment of a business relationship, ongoing monitoring of customers and transactions on a risk sensitive basis, filing of suspicious activities reports and implementation, maintenance and safe keeping of records and the testing of the adequacy of its own systems and controls and compliance by Deltastock Group officers and employees.
- 4.5 AML training will be arranged by Management for its members, officers and employees who deal directly with customers to the standards, if any, required by law and/or the regulatory authorities.

5. PRODUCTS & SERVICES

- 5.1 The AML Policy and compliance procedures will apply to transactions of all financial services products and services including those relating to securities investments and financial instruments offered by Deltastock Group falling under the Markets in Financial Instruments Directive 2004/39/EC.
- 5.2 A list of current products and services offered by Deltastock Group can be viewed at www.deltastock.com.
- 5.3 Transactions will include any deposit, withdrawal, currency exchange or transfer of funds involving Deltastock Group's products and services.

6. MONEY LAUNDERING

- 6.1 For the purposes of the Policy, money laundering includes the proceeds of all criminal conduct and activity, no matter how minor the conduct or benefit arising from such criminal activity.
- 6.2 The definition of criminal activity includes, but is not limited, for example, terrorism financing, corruption, bribery payments to politicians, drug trafficking, human trafficking, evasion of taxes, obtaining money by fraud or deception or organised crime activities generating proceeds of crime.
- 6.3 The process by which criminals attempt to conceal the true origin and ownership of property or proceeds from criminal activity and turning 'dirty' money (the proceeds from criminal activity) into clean money by a transaction or a series of transactions.
- 6.4 Criminal property includes money, securities, property and it includes, but is not limited to property which either constitutes a person's benefit from criminal conduct or activity or represents (in whole or in part and whether directly or indirectly) a person's benefit from criminal conduct or activity; and is known or suspected by the alleged offender to constitute or represent such a benefit.
- 6.5 Money laundering occurs generally in three stages.
 - 6.5.1 placement stage where cash enters the financial system as, for example, investments, where the cash generated from criminal activities is converted into financial instruments;
 - 6.5.2 layering stage, where the funds are transferred or moved into other accounts or other financial institutions or into property, locally or cross border and usually a number of times, to further separate the money from its criminal origins; and
 - 6.5.3 integration stage, where the funds are reintroduced into the economy and used to purchase legitimate property, assets or to fund legitimate businesses.

- 6.6 Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which may be subsequently used for criminal purposes.
- 6.7 Terrorism is the use or threat of action designed to influence government, or to intimidate any section of the public, or to advance a political, religious or ideological cause where the action would involve violence, threats to health and safety, damage to property or disruption of electronic systems.
- 6.8 Dealing with funds or property which are likely to be used for the purposes of terrorism, even if these funds are “clean funds” in origin, will amount to a terrorist financing offence.
- 6.9 It is an offence to enter into or become concerned in an arrangement which facilitates the retention or control of terrorist property by or on behalf of another person by concealment, removal from the jurisdiction, transfer to nominees or in any other way.

7. RISK ASSESSMENT

- 7.1 Deltastock Group adopts a risk sensitive based approach to money laundering and terrorist financing which includes:
 - 7.1.1 identification and management of the money laundering and terrorist financing risks that are relevant to its business;
 - 7.1.2 assessing the risks presented by the particular customer type and behaviour, Deltastock Group products and services, delivery channels and payments, ownership and beneficial interests, source and destination of customer's funds;
 - 7.1.3 the implementation of controls, management and monitoring of customers and transactions and maintenance of records and documentation;
- 7.2 A policy of enhanced customer due diligence and ongoing monitoring is also adopted by Deltastock Group:
 - 7.2.1 where the customer is not physically present for identification purposes - no face to face dealings;
 - 7.2.2 a credit institution (“correspondent”) which has or proposes to have a correspondent banking relationship with a respondent institution from a non EU State;
 - 7.2.3 business relationship or occasional transaction with a politically exposed person or PEP, his family and close associates; and
 - 7.2.4 any other situation which can present a higher risk of money laundering or terrorist financing.

8. CUSTOMER IDENTIFICATION

- 8.1 Deltastock Group has adopted as part of its customer due diligence, a Customer Due Diligence Identification and Verification Policy.
- 8.2 It will provide notice to its potential and existing customers that it will seek identification information; collect certain minimum customer identification information from each customer, record such information and the verification methods and results; and compare these with the information supplied by the customer and if necessary, take follow up action.
- 8.3 The following customer notice will be used, with modifications as required by applicable law:
 - 8.3.1 The law requires us to fight the funding of terrorism and money-laundering activities. Financial services businesses such as ours are required to obtain, verify, register and record information that identifies persons who engage in financial services transactions with or through our businesses. This means that we will verify your name, residential address, nationality, date of birth and occupation on the account opening application. We may also ask to see your passport, identification card, photo driver's licence or other documents of identification.

9. VERIFYING INFORMATION

- 9.1 Adopting a risk sensitive based approach, and as far as reasonably practicable, Deltastock Group will endeavour to verify the identity of its customers through independent identification service providers. It will note and record any inconsistencies from the information provided by the customers against verification from independent sources.
- 9.2 Such verification will be stored in documentary or electronic file form for a period of five years from the date of the transaction concerned or the date the customer relationship has been terminated.
- 9.3 Deltastock Group will not however attempt to determine, as it is not qualified to do so, that the documents its customers provide for identification have been validly issued. For verification purposes, it will rely on at least two or three independent sources to establish a customer's identity.
- 9.4 Deltastock Group will document and record its verification, including all identifying information provided by its customers, the methods used and results of the verification. All such identification and verification matches will be signed by the person conducting the customer due diligence.

10. GOVERNMENT LISTS CHECK

- 10.1 Before establishing a business relationship with any new customers and thereafter on an ongoing basis with new and existing customers,

Deltastock Group will check to ensure that a person or entity does not appear on:

- 10.1.1 the United States Department of The Treasury's OFAC "Specifically Designated Nationals and Blocked Persons" List (SDN List) and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC website at www.treas.gov/offices/enforcement/ofac/sdn/index.shtml.
 - 10.1.2 the United Kingdom Her Majesty's Treasury Financial Services Consolidated List of Financial Sanctions Targets at www.hm-treasury.gov.uk/fin_sanctions_index.htm.
 - 10.1.3 the Bulgarian Government Council of Ministers published decisions on SDN List.
- 10.2 Deltastock Group will also review existing customers, agents, business producers and employees against the lists in paragraph 10.1 on a periodic basis. The frequency of the reviews will be documented and retained.

11. MONITORING & REPORTING

- 11.1 All companies within the Deltastock Group will monitor and maintain such monitoring as required of transactions and customers as required under AML regulations and policies.
- 11.2 Monitoring of specific transactions will include, but is not limited to, transactions aggregating government thresholds or Deltastock Group cash thresholds of BGN 10,000, or its equivalent in Romania, or more and those transactions which the companies within Deltastock Group have reason to suspect amount to suspicious activity.
- 11.3 It is the duty of the employees of Deltastock Group to record and report to their MLRO any transaction which they believe to amount to suspicious activity.
- 11.4 All reports will be documented and retained in accordance with its AML Policy.

12. SUSPICIOUS ACTIVITY

- 12.1 Signs that suggest suspicious activity that may amount to money laundering may be referred to as "alarms bells" If an alarm bell is detected, additional and enhanced due diligence will be performed before proceeding with the transaction.
- 12.2 If the prospective or existing customer is unable to provide a reasonable explanation, the suspicious activity shall be reported internally to the MLRO who will evaluate and make a decision as to whether there are grounds to make a suspicious activity report (SAR) externally to the appropriate enforcement and regulatory authorities.

- 12.3 A non-exhaustive list of examples of alarm bells include new and/or existing customers:
- 12.3.1 having unusual concern regarding Deltastock Group's compliance with government reporting requirements and its AML policies, particularly with respect to his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspect identification or business documents;
 - 12.3.2 refusing to identify or failing to indicate any legitimate source for his or her funds and other assets;
 - 12.3.3 whose signature in the identification documents differ from the signature affixed by the customer in connection with the customer's account and/or commercial transaction;
 - 12.3.4 requesting a wire transfer of funds after they have been deposited via credit card payment;
 - 12.3.5 funding transactions from money transferred in from accounts in financial institutions outside the EC which belong to third parties that have no relation with the customer;
 - 12.3.6 performing multi transactions or deals of small amounts, within a short period of time, which when aggregated would trigger reporting requirements;
 - 12.3.7 who enter into large transactions to buy securities or forex by depositing funds and then closing the deals for no apparent commercial benefit or reason and withdrawing funds;
 - 12.3.8 who instruct funds from sale of their investments, securities and foreign exchange to be paid into "mailbox" or shell company bank accounts;
 - 12.3.9 performing frequent transactions which are not related to the main business of the customer in the purchase of securities and foreign exchange;
 - 12.3.10 funding transactions to purchase securities and forex from their own funds and selling the acquired investments with instructions to pay a third party other than the customer;
 - 12.3.11 wishing to engage in transactions that lack business or commercial sense or apparent investment strategy, or are inconsistent with the customer's stated business strategy;
 - 12.3.12 providing information seeking to identify a legitimate source for funds which is found to be false, misleading, or substantially incorrect;

- 12.3.13 entering into transactions for securities under usual circumstances which raises a reasonable suspicion that the source of funds originated from other than the customer;
- 12.3.14 or a person publicly associated with the customer, has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations;
- 12.3.15 exhibiting a lack of concern regarding risks, commissions, or other transaction costs;
- 12.3.16 appearing 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;
- 12.3.17 having difficulty describing the nature of his or her occupation, business or lacks general knowledge of his or her industry;
- 12.3.18 attempting to make frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies relating to the deposit of cash and cash equivalents;
- 12.3.19 engaging in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds;
- 12.3.20 who for no apparent reason, has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers;
- 12.3.21 from or has accounts in a country identified as a non-cooperative country or territory by the Financial Action Task Force or jurisdictions identified and listed by the OECD as being not committed to internationally agreed tax standard;
- 12.3.22 has unexplained or sudden extensive wire activity in their accounts, especially in accounts that had little or no previous activity;
- 12.3.23 with accounts showing numerous currency or cashiers cheque transactions aggregating to threshold sums;
- 12.3.24 whose account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business;
- 12.3.25 whose account has wire transfers that have no apparent business purpose to or from a country identified as a

- money laundering risk or an offshore tax haven or which promotes banking secrecy (see also paragraph 12.3.21);
- 12.3.26 whose account indicates large or frequent wire transfers, immediately withdrawn by cheque or debit card without any apparent business purpose;
- 12.3.27 making funds deposits followed by an immediate request that those funds be wired out or transferred to a third party, or to another firm, without any apparent business purpose, thus using Deltastock Group as if it were a bank;
- 12.3.28 requesting transactions to be processed in such a manner to avoid the firm's normal documentation requirements; and
- 12.3.29 whose account shows an unexplained high level of account activity with very low levels of securities transactions.

13. ONLINE PAYMENTS & ELECTRONIC FUND TRANSFER

- 13.1 Deltastock Group operates a proprietary electronic trading platform which accepts online card payment.
- 13.2 Its payment service providers will, as regulated financial institutions or money service businesses, have their own AML Policy and customer due diligence procedures upon which Deltastock Group may seek to rely to supplement its customer due diligence but not as a substitute to their own customer due diligence under AML procedures.
- 13.3 Where possible, it will seek to have electronic transfer payments from customers to be made from the customer's own bank account within the EU, since these banks as regulated financial institutions are subject to and required by money laundering regulations to identify and verify their customers.
- 13.4 In instances where the customer is not present, the following policy is to be adopted as far as practicable by Deltastock Group:
- 13.4.1 inspect and evaluate all customer presented documents;
- 13.4.2 request by way of enhanced due diligence, provision of additional documents from the customer relating to identification;
- 13.4.3 request the first payment of funds for the transaction to be effected from an account opened by the customer in his name with an EU bank; and
- 13.4.4 in the case of a non EU bank, such payment of funds is to be evidenced in copy of the bank remittance advice with that bank's official stamp and date.

14. INVESTIGATION

- 14.1 In the event of a match to the SDN List, other OFAC List, the Financial Sanctions Targets List and the published decisions of the Bulgarian Government decisions on the SDN List, Deltastock Group will conduct a review of the circumstances and the relevant MLRO and Management will be notified. A suspicious activity report will be made to the relevant enforcement and regulatory authorities.
- 14.2 The investigation will include, but not be limited to, a review of all available information such as payment history, birth dates, and address. If the findings of the investigation warrant, a recommendation will be made to Management to file a blocked assets and/or a SAR with the appropriate law enforcement or regulatory agency.
- 14.3 The MLRO of the relevant company within Deltastock Group is responsible for any notice or filing with law enforcement or regulatory agency.
- 14.4 Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. Under no circumstances shall Management, MLRO, any officer or employee disclose or discuss any AML concern, investigation, notice or SAR filing with the customer concerned or any other person, including members of the officer's, employee's or appointed agent's family.
- 14.5 Disclosure of such is strictly prohibited by law and tipping off a money launderer or prejudicing an investigation into money laundering is a criminal offence.

15. RECORD KEEPING

- 15.1 The Management and the individual MLRO within the Deltastock Group will be responsible to ensure that AML records are maintained properly and that suspicious activity reports are filed in the required format and communicated as required. Deltastock Group will maintain AML records for at least five years.
- 15.2 The five-year retention period will start to run from the completion of the transaction or termination of the customer account, for whatever reason, whichever is later.

16. TRAINING

- 16.1 Deltastock Group has a programme of training courses arranged for its MLROs to ensure they are kept up to date with developments in AML law and regulations. The MLROs of the companies within Deltastock Group will have the function to ensure relevant staff receives AML training to ensure awareness of legal and regulatory requirements in their respective countries of operations.
- 16.2 The training will include, at a minimum: how to identify alarm bell situations and other signs of money laundering; what roles Management, the MLRO, officers and employees have in the Deltastock Group compliance efforts and how to perform such duties

and responsibilities; what to do once an alarm bell or suspicious activity is detected.

- 16.3 Deltastock Group will in compliance with its regulatory requirements under its record keeping policy, keep and maintain a record of disciplinary consequences for non-compliance with money laundering legislation and its AML Policy.
- 16.4 Training will be conducted on an annual basis. Management will, with participation of the MLRO, determine ongoing training requirements and ensure written procedures are updated to reflect any changes required in such training. Deltastock Group will maintain records to document that training has occurred.

17. POLICY TESTING AND REVIEW

- 17.1 The testing and review of the AML Policy will be conducted internally by Management every six months starting from February 2009 and annually thereafter.
- 17.2 Any findings will be reported to Management for evaluation, consideration and action required taken by the MLRO of the company within the Deltastock Group, as necessary.

18. ADMINISTRATION

- 18.1 Management is responsible for the administration, revision, interpretation and application of this Policy.
- 18.2 The Policy will be reviewed annually and revised as needed and a Board resolution passed to update any major changes that are necessary.
- 18.3 The Customer Due Diligence Identification and Verification Policy and Customer Notice shall be implemented by 30 June 2009.
- 18.4 Initial training shall be completed by 30 June 2009 and annually thereafter.