BANK OF GREECE
EUROSYSTEM

BANKING AND CREDIT MATTERS COMMITTEE

Meeting 281/17.3.2009

Item 5: Prevention of the use of credit and financial institutions under Bank of Greece supervision for money laundering and terrorist financing

THE BANKING AND CREDIT COMMITTEE, having regard to:

(a) the provisions of the Statute of the Bank of Greece, in particular Article 55A, as currently in force;

(b) Article 1 of Law 1266/1982 "Bodies responsible for conducting monetary, credit and foreign exchange policies, and other provisions", as currently in force;

(c) Law 3601/2007 "Taking up and pursuit of the business of credit institutions, capital adequacy of credit institutions and investment firms, and other provisions";

(d) the provisions of Law 3691/2008 "Prevention and suppression of money laundering and terrorist financing, and other provisions" (hereinafter referred to as "the Law"), with respect to the obligations of the Bank of Greece as the competent authority, for the purposes of the Law, for supervising compliance of the credit and financial institutions referred to in Article 6(2) of the Law and the provisions of Article 6(3)-(5) of the Law;

(e) Bank of Greece Governor's Act 336/1984, as currently in force;

(f) the provisions of Bank of Greece Governor's Act 2577/2006 "Framework of operational principles and criteria for the evaluation of the organisation of Internal Control Systems of credit and financial institutions and relevant powers of their management bodies", as currently in force;

(g) Banking and Credit Matters Committee Decision 231/4/13.10.2006, as currently in force, supplementing Bank of Greece Governor's Act 2577/2006 by adding Annex 4 "Prevention of the use of the financial system for money laundering and terrorist financing";

(h) the provisions of Directive 2005/60/EC of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and

terrorist financing and of Directive 2006/70/EC laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of 'politically exposed person' and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis;

(i) Regulation 1781/2006 of the European Parliament and of the Council on information on the payer accompanying transfers of funds; and

j) the need to amend and supplement the current regulatory framework according to the provisions of Law 3691/2008,

HAS DECIDED:

to replace Banking and Credit Matters Committee Decision 231/4/13.10.2006 and revise the supervisory framework on the prevention of the use of institutions supervised by the Bank of Greece for money laundering (hereinafter referred to as "ML") and financing of terrorism (hereinafter referred to as "FT") as follows:

1. GENERAL PRINCIPLES

1.1 The Bank of Greece, as the supervisory authority responsible under Article 6(2) of Law 3691/2008 "Prevention and suppression of money laundering and terrorist financing, and other provisions" for compliance with the provisions of the Law by Credit Institutions (hereinafter referred to as "CIs") and Financial Institutions (hereinafter referred to as "FIs"), lays down, by authority of Article 6(3)-(5) of the Law, the following obligations for CIs, and corresponding obligations for FIs, on the basis of the principle of proportionality, as the latter obligations are specified in Chapter 12 of this decision.

1.2 In the context of an effective risk strategy management according to the provisions of Bank of Greece Governor's Act 2577/2006, as currently in force, each CI shall adopt an Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) policy, which shall be recorded, documented and approved by the CI's Board of Directors. To this end, each CI shall have a Compliance Officer pursuant to Article 44 of Law 3691/2008, a relevant unit, the resources required and adequate staff.

1.3 For the purposes of this Decision and in the context of its approved policy, each CI, through its Management (within the meaning of Chapter IVA, para. 3 of Bank of Greece Governor's Act 2577/2006), shall:

(i) Adopt and implement adequate and appropriate measures for specialising this policy and procedures relating to:

(a) due diligence, according to the provisions of Chapters C and D of Law 3691/2008, with respect to the customer and the beneficial owner, within the meaning of Article 4(16) of the Law;

(b) reporting of suspicious transactions in accordance with Article 26 of the Law;

(c) record-keeping in accordance with Article 35 of the Law;

(d) internal control of implementation of these procedures by both their central services and their network of outlets;

(e) continuous ML/FT risk assessment and continuous assessment of compliance with the regulatory framework, so that the CI may identify, prevent, avert and report transactions whereby the offences referred to in Article 2 of Law 3691/2008 are possibly committed.

CIs shall lay down and review on a regular basis their customer acceptance policy and unacceptable risk criteria after a thorough assessment of the risks from existing and new customers, transactions, the countries or jurisdictions where their business either originates or takes place, as well as from the launch of new products and services. Finally, they shall take special measures in the establishment of cross-border correspondent banking relationships, as well as in the duration of such relationships, according to the provisions of Article 21 of Law 3691/2008 and of this Decision.

(ii) Establish a full profile of the customer and the beneficial owner, according to the provisions of para. 5.4(iv) of this Decision, in order to classify them in terms of ML/FT risk and take the necessary due diligence measures.

(iii) Ensure that all KYC particulars of existing customers and beneficial owners are obtained and verified according to the provisions hereof and adopt updating and control procedures.

(iv) Establish appropriate IT systems for continuously monitoring and detecting suspicious or unusual transactions or activities, within the meaning of paras. 13 and 14, respectively, of Article 4 of Law 3691/2008, and examine very carefully any transaction that, due to its nature or to data concerning the person or identity of the customer, may be associated with ML or FT.

(v) Specify the role, responsibility and duties of the Compliance Officer referred to in Article 44 of Law 3691/2008 (hereinafter referred to as the “Compliance Officer”) and the unit he heads, in accordance with the provisions of the Law and this Decision.

(vi) Allocate clear responsibilities and duties to the persons and units involved in the CI's transactions and operations, in order to ensure effective implementation of AML/CFT policy, procedures and controls and achieve compliance with Law 3691/2008 and this Decision.

(vii) Take appropriate measures so that its management and staff are informed about the provisions of Law 3691/2008 and this Decision, as well as the CI's policy and procedures specifying them, and ensure their participation in specialised AML/CFT training courses.

(viii) Ensure the valuation of the customer's overall business portfolio maintained with the CI and, possibly, with other companies in its group, according to Article 13(2), taken together with Article 32(2) of Law 3691/2008, in order to confirm that the transaction examined as suspicious or unusual is consistent and compatible with such portfolio(s).

(ix) Take any appropriate measure, including refusing to execute the transaction or terminate the business relationship with the customer and the beneficial owner, in the event that (a) the identification and verification conditions have not been fulfilled; (b) the due diligence measures referred to in para. 5.4(iii) and (v) below have not been observed; or (c) reports on the customer in question have been repeatedly submitted to the AML/CFT Commission.

(x) Ensure that the above obligations, with respect to a parent CI, are performed by both its subsidiaries in Greece and abroad, and its branches and representative offices abroad, unless this is wholly or partly prohibited by the relevant foreign legislation, in which case they shall inform to this effect the AML/CFT Commission and the Bank of Greece.

1.4 The CI's Control Committee (failing which its Board of Directors), in the context of the annual monitoring and assessment of the adequacy and effectiveness of the AML/CFT policy, shall take into account the relevant data and information in the ML/FT Annual Report of the Compliance Officer (referred to in Chapter 3 below), the report of the Internal Audit Unit, the findings and observations of external auditors, as well as the findings of supervisory authorities.

1.5 For the uniform implementation of the provisions of this decision, the minimum procedures to be applied by CIs for duly performing their obligations are stated below.

1.6 The definitions in Article 4 of Law 3691/2008 for the time being in force shall apply to the provisions of this decision.

2. ROLE OF THE COMPLIANCE OFFICER

2.1 Appointment of the Compliance Officer referred to in Article 44 of Law 3691/ 2008

2.1.1 The CI's management officers and employees shall report to the Compliance Officer any transaction they consider as unusual or giving rise to suspicions of attempted or actual commission of the offences referred to in Article 2 of Law 3691/2008 and any event they become aware of due to their service that may be an indication of such acts.

2.1.2 The Compliance Officer shall be appointed by the CI's Board of Directors on the basis of his morality, integrity, status, scientific background, experience in the relevant field and familiarity with the CI's operations. If the Compliance Officer is unavailable, he shall be replaced by an alternate appointed together with him. His data shall be communicated to the Bank of Greece within not later than then days. The Compliance Officer and his alternate may not hold any other position in the CI in conflict with their obligations, and any of their activities outside the CI may not be in conflict with the role and duties of a Compliance Officer. The Bank of Greece shall have the right to request the replacement of these persons if it considers that they do not meet the requirements and qualifications for performing their duties.

2.1.3 CIs shall establish, within the Compliance Unit (in the event that the conditions for establishing it are met according to the provisions of Chapter Vc of Bank of Greece Governor's Act 2577/2006), a Special AML/CFT Service, headed by the Compliance Officer and staffed according to the size, structure, complexity of operations and the risks facing the CI and its group. In this case, the CI's Board of Directors shall ensure, mainly in relation to the Compliance Officer's obligation to report suspicious transactions to the AML/CFT Commission, his independence within the Compliance Function. If the CI is not obliged to establish a Compliance Function, it shall ensure that the Compliance Officer has adequate resources and the conditions for effective performance of his duties are in place. The Compliance Officer and the Head of the Compliance Function may be one and the same person.

2.1.4 In the case of a financial group, the largest company of the group shall appoint a Compliance Officer in charge of ensuring compliance with the provisions of the Law and this Decision by the other companies of the group. To this end, this Compliance Officer shall cooperate, coordinate and exchange information with the Compliance Officers of the companies of the group appointed according to the above provisions.

2.2 Duties of the Compliance Officer

CIs shall specify and record, in the context of their AML/CFT policy, the role, responsibilities and duties of the Compliance Officer. The Compliance Officer shall at least:

(i) Receive from the CI's employees reports of suspicious or unusual transactions, as well as information about any event they are aware of due to their service that could be an indication of ML or FT. All reports shall be archived in a separate file.

(ii) Recommend appropriate procedures for ensuring the receipt and processing of alerts of unusual or suspicious transactions produced by the CI's IT system. Such processing may be effected either by the branches or by the AML/CFT Special Service.

(iii) Examine and assess the aforementioned reports and alerts by collecting information from reliable sources, such as Tiresias S.A., ICAP and other recognised information banks. The assessment results shall be recorded and archived in the relevant file.

(iv) Submit a confidential report to the AML/CFT Commission in the event that, after the assessment referred to in the preceding paragraph, he judges that there are indications of ML/FT. Reports to the AML/CFT Commission shall be archived in a separate file.

(v) Contact directly the AML/CFT Commission both at the commencement and during the investigation of cases examined after the submission of a relevant report, and answer to questions about any clarifications.

(vi) Monitor very carefully on a continuous basis the transactions of persons about which a report has been submitted to the AML/CFT Commission and inform in this connection the coordinator in charge, if he is not the same person as the Compliance Officer, for companies of the group referred to in Article 44(2) of Law 3691/2008, under the conditions of Article 32 of the Law.

(vii) Compile statistics of internal reports to the Compliance Officer and reports of the latter to the AML/CFT Commission.

(viii) Monitor and assess the proper and effective implementation of the CI's AML/ CFT policy and the relevant implementation measures. To this end, the Compliance Officer shall apply appropriate control mechanisms, as described in paras. 9.2 and 9.3 below, in units or branches of the CI, in order to verify their compliance with the arrangements in force (regulatory framework, AML/CFT manual, customer acceptance policy etc.). In the event that the Compliance Officer identifies any failures or weaknesses or risks from existing customers, new customers, products and services, he shall recommend appropriate corrective measures in writing.

(ix) Participate with other units of the CI in the development of the AML/CFT manual. This manual, after being approved by the Management or the Board of Directors, shall be

communicated to the officers and all employees who handle, monitor or control in any manner transactions of customers and are responsible for the implementation of the policy, procedures and controls that have been decided. The manual shall be periodically assessed and revised where any defects are identified or it is necessary to adapt the CI's procedures with a view to tackling ML/FT risks more effectively.

(x) Ensure the maintenance of lists of low- and high-risk customers, including each customer's name, account number, branch where the account is kept and date of establishment of the business relationship. In addition, he shall ensure that these lists are updated regularly (on an at least annual basis) with information on all new customers or additional information on old customers.

(xi) Submit to the CI's Management an annual report assessing high-risk customers, broken down by risk category. This report shall include aggregated data on these customers, drawn from the CI's units' summary reports, and recommend the termination of the CI's relationship with customers of this category that exceed the limits of unacceptable risk.

(xii) Respond to written questions asked by the Bank of Greece, and provide in a secure manner any data required on matters within the Bank's scope of authority.

(xiii) Provide guidance to the CI's employees on AML/CFT issues.

(xiv) Prepare and implement, in cooperation with other competent sections of the CI, the annual staff further training and education programme approved by the Management. The Compliance Officer shall recommend the services, branches and employees of the CI that need further training in AML/CFT issues and shall organise appropriate educational meetings or courses. Finally, he shall receive from the competent sections detailed data on training courses provided to the CI's employees and shall jointly assess the adequacy of the training provided.

(xv) Assess the adequacy, within the scope of the CI's responsibility for concluding correspondent banking relationships under para. 1.3(i) above, of the AML/CFT policy, procedures, systems and controls applied by the CIs that request the conclusion or that have concluded correspondent banking relationships according to the criteria of para. 5.15.9 below, and submit a relevant recommendation to the competent unit.

(xvi) In the event that the CI has outsourced the customer identification and verification procedure, assess the procedures applied by them and submit a relevant recommendation to the CI's Management.

(xvii) Take or recommend, as appropriate, corrective AML/CFT measures according to the findings of examinations conducted by the Bank of Greece.

(xviii) Assess the findings of the Internal Audit Unit in order to take corrective AML/ CFT measures.

(xix) Ensure that the CI's branches and subsidiaries abroad take all the measures required for full compliance with the requirements of the law and this Decision.

3. ANNUAL REPORT OF THE COMPLIANCE OFFICER

3.1 The Compliance Officer shall prepare an annual report, which shall be a considerable input for the assessment of the CI's compliance with the AML/CFT provisions. The annual report shall be assessed by the Board of Directors, through the Audit Committee referred to in Bank of Greece Governor's Act 2577/2006, as currently in force, and shall be approved and submitted within March to the Bank of Greece (Department for the Supervision of Credit and Financial Institutions – Money Laundering Prevention Sector) **in electronic form or in a hard copy**, accompanied by the results of the annual assessment of the adequacy and efficiency of the AML/CFT policy carried out by the Audit Committee (failing which by the Board of Directors).

3.2 The annual report shall include at least the following **information**:

(i) (a) The full name, post and data of the decision appointing the Compliance Officer, his alternate and the coordinator, in the case of financial groups.

(b) The organic structure and staff of the Compliance Officer's Special Service, as well as recommendations on any additional staff and technical equipment requirements, with a view to enhancing the AML/CFT measures and procedures.

(ii) The AML/CFT policy and manual established in writing by the CI. It should be noted that, in the event of important changes in the relevant procedures during a year, the Bank of Greece shall be informed in writing.

(iii) Brief information on important measures taken and procedures adopted during the year.

(iv) Examinations, as described in paras. 9.2, 9.3 and 9.4 below, of units or branches of the CI, including the number of examinations and the serious defects and weaknesses identified in the CI's AML/CFT policy and procedures, the seriousness of failures or weaknesses, the risks entailed and the actions or recommendations for corrective measures.

(v) The AML/CFT IT systems installed by the CI, including a description of their operations and any weaknesses that have arose. It should be noted that any important upgrading of these systems shall be communicated in writing to the Bank of Greece.

(vi) (a) The number of reports of unusual or suspicious transactions submitted to the Compliance Officer, classified by case/customer.

(b) The number of reports of unusual or suspicious transactions submitted by the Compliance Officer to the AML/CFT Commission, classified by case/customer, including brief information on the categories of suspicious or unusual transactions that were identified.

(c) The AML/CFT measures taken on the cases reported to the AML/CFT Commission.

(vii) The number of high-risk customers with which the CI maintains business relationships, the number of those it terminated its relationship with, their home countries and a brief annual assessment.

(viii) Measures taken for the compliance of the CI's branches/subsidiaries abroad with the requirements of this Decision, as well as comments or information on the degree of their compliance therewith.

(ix) Training courses attended by the Compliance Officer and his alternate.

(x) Information on the staff's training during the year, with details of:

- the number of presentations/courses organised;
- their duration;
- the number of employees that attended;
- the subject areas of presentations /courses; and
- the general conclusion from participants' assessments.

(xi) Information on the actions scheduled to be taken in the next year for improving the CI's AML/CFT system.

4. RISK-BASED APPROACH OF MONEY LAUNDERING

4.1 CIs shall adopt a policy and procedures for assessing and managing effectively the risk of their services being used for ML and FT purposes. What follows is a description of the general principles of application of a risk-based approach. In determining their policy and procedures, CIs shall take into account the FATF's document entitled Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing – High Level Principles and Procedures (www.fatf-gafi.org/dataoecd/43/46/38960576.pdf).

4.2 CIs shall conduct **customer due diligence** (CDD) according to the provisions of Chapter 5 below and shall be able to justify to the Bank of Greece that the scope of the relevant measures is proportional to the ML/FT risk and that they apply these measures consistently and effectively.

4.3 The appropriate procedures and measures applied for managing ML/FT risk shall be determined on the basis of the size, structure and complexity of each CI's operations. To identify and assess the overall risk facing it, each CI shall take into account at least:

- the risk from CI's customers' business or professional activities (e.g. complex ownership structure of legal persons, companies with bearer shares, offshore companies, politically exposed persons, customers with large cash transactions etc.);
- the risk from the customer's transaction behaviour (e.g. transactions with no obvious legitimate financial/commercial purpose, difficulties in verifying the source and origin of the customer's assets, customer's unwillingness to disclose the real owners of a legal person etc.);
- the risk from transactions favouring customer anonymity (e.g. distance customers);
- the risk from the products and services provided to the customer (e.g. remittances, private banking services, investment products etc.); and
- the risk from the country or region of origin or destination of the funds, or the customer's home country.

4.4 CIs shall classify customers in at least three different risk categories:

- low
- moderate
- high,

associated with appropriate CDD, periodic monitoring and control measures. The customer categories referred to in paras. 5.15.1-5.15.10 shall be compulsorily included in high-risk customers, to which enhanced CDD shall apply.

Parameters of a risk assessment and classification system shall include, without limitation:

- professional activity of a natural person;
- the customer's home country or country of business;
- transactions with the use of new technologies;
- complexity of transactions;
- countries of origin and destination of funds;
- legal status and country of incorporation of a legal person;
- ultimate or beneficial owner of a legal person;
- deviations from the customer's profile;
- volume, size and kind of business transactions; and
- area of activity of a legal person.

4.5 CIs, according to the risk management policy they apply, shall adopt unacceptable risk criteria for classifying customers with whom they do not conclude or terminate business relationships and transactions they do not carry out (e.g. exclusion of countries and jurisdictions, non-documented cash transactions of a considerable amount, activities giving rise to suspicions of association with organised crime).

4.6 CIs shall install **adequate IT systems** and effective procedures for continuously monitoring accounts and transactions, in order to detect, monitor and assess high-risk transactions and customers. IT systems shall be capable of providing timely, reliable and necessary information for detecting, analysing and effectively monitoring customers' accounts and transactions. Accounts and transactions shall be monitored in relation to the typology of transactions, the customer's profile, as defined in para. 5.4(iv) below, and the anticipated operation of the account in relation to the operation of other accounts in the same customer category. Material deviations shall be further investigated. Procedures shall also apply to inactive accounts that are reactivated. IT systems shall be used for obtaining information on defective customer identification, the customer's profile and overall data on the CI's business relationship with the customer.

The **operations** of a risk management IT system shall include, without limitation:

- Assessing and classifying customers on the basis of their profile into risk categories according to the criteria laid down by the CI, which shall include at least the requirements of Chapter 5 below.
- Controlling the CI's clientele and transactions on the basis of lists of persons or entities subject to sanctions under EU Regulations and Resolutions of the UN Security Council. Control shall be carried out on a real-time basis at the commencement of the business relationship or during the conduct of the transaction. By entering every new list, the IT system shall check all the clientele of the CI in order to verify whether the CI maintains or maintained a business relationship with the listed persons or entities, the kind of relationship and any relevant transaction.
- Controlling the clientele and transactions on the basis of local lists of persons or entities that have committed criminal offences, prepared by the competent police and judicial authorities. Control shall be carried out on a real-time basis at the commencement of the business relationship or during the conduct of the transaction. By entering every new list, the IT system shall check all the clientele of the CI.

- Controlling all transactions on the basis of the international typology of suspicious transactions communicated regularly by the Bank of Greece.
- Revising and further developing preventive measures, taking into account the results of risk analysis.
- Issuing alerts of unusual or suspicious transactions according to the criteria laid down hereinabove. CIs shall lay down a procedure for receiving and processing alerts, which may be undertaken by either a central unit of the CI or local branches and services. Regarding inadequately justified alerts, the procedure of Chapter 8 below on detection, handling and reporting of unusual transactions shall apply.

4.7 ML/FT risk management is an ongoing and dynamic procedure, as both customers' activities and CIs' products/services change. As a result, procedures, systems and controls are revised regularly with a view to effective management of the risks from changes in the characteristics of existing customers, new customers, products and services.

5. CUSTOMER IDENTIFICATION AND VERIFICATION PROCEDURES AND CUSTOMER DUE DILIGENCE

5.1 Collection and maintenance of adequate information on a customer, the use of such information for identification purposes and the assessment of his overall profile form the basis of AML/CFT procedures and the most effective protection against negative effects on CIs' solvency and goodwill. CIs shall apply at least the CDD measures provided for hereunder.

5.2 CIs shall not open and keep secret, anonymous or identified-by-number accounts or accounts in fictitious names or accounts without the full name of their holder, in accordance with the identity certification documents.

5.3 CIs shall apply, pursuant to Article 12 of Law 3691/2008, CDD measures in the following cases:

(a) when establishing a business relationship;

(b) when carrying out any transaction amounting to at least €15.000, whether the transaction is carried out in a single operation or in several operations which appear to be linked; CIs shall in any case be able to detect whether a transaction has been carried out in several operations;

(c) when there is a suspicion of money ML or FT, regardless of any derogation, exemption or threshold; and

(d) when there are doubts about the veracity, completeness or adequacy of previously obtained identification and verification data about the customer, other persons on behalf of whom the customer is acting and the beneficial owner of the customer.

5.4 CDD measures, both at the commencement and in the duration of a business relationship, shall comprise:

(i) Identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from reliable and independent sources.

(ii) Identifying the beneficial owner(s) of legal persons and entities, continuously updating the information and taking reasonable, risk-based measures to verify their identity so that the CI is satisfied that it knows who the beneficial owner(s) is (are). As regards other legal persons, trusts and similar legal arrangements, CIs shall take reasonable, risk-based measures to understand the ownership and control structure of the customer.

(iii) Obtaining information on the purpose and intended nature of the business relationship or of important transactions or activities of the customer or the beneficial owner.

(iv) Establishing the profiles of their customers (both individual and corporate), including at least:

- the purpose for which an account is opened or a business relationship is concluded;
- the anticipated operation of the account;
- the kinds of transactions that may be carried out;
- the anticipated source of the funds credited to the account;
- the anticipated destination of outgoing remittances or payments;
- the size and sources of the customer's assets and revenue; and
- a description of the customer's professional or business activity.

(v) Conducting ongoing oversight of the business relationship, including scrutiny of transactions and activities undertaken by customers and beneficial owners throughout the course of the relationship, to ensure that such transactions and activities are consistent with the CIs' knowledge of these persons, their business and risk profile, including, where necessary, the source of funds. CIs shall also ensure that documents, data or information are kept up-to-date.

(vi) Examining with special attention any transaction or activity which, by its nature or by virtue of the customer's personal circumstances or capacity, could be associated with ML or FT. These transactions include in particular complex or unusually large transactions and any unusual kind of transaction that is conducted with no apparent economic or lawful purpose.

The results of the examination shall be recorded and kept on file for at least five years, including the evidence.

(v) Taking any appropriate measure, including refraining from conducting the transaction and refusing to provide services or carry out activities, unless the customer identification and verification requirements are met or the CI ensures compliance with CDD measures, and in the event that reports on the customer in question are repeatedly submitted to the AML/CFT Commission.

(viii) Refraining from conducting the transaction, refusing to provide services or carry out activities and promptly informing the AML/CFT Commission and the Bank of Greece when the name of the CI's customer is included in lists of persons or entities subject to sanctions under EU Regulations and Resolutions of the UN Security Council.

5.5 Without prejudice to any additional information required for higher risk customers, the following customer identification and verification procedures shall apply to natural and legal persons.

5.5.1 Minimum information required for the identification of natural persons:

Natural persons
1. Full name and father's name
2. Identity card or passport number
3. Issuing authority
4. Date and place of birth
5. Current residence address
6. Contact phone number
7. Occupation and current occupational address
8. Taxpayer's Identification Number
9. Specimen of customer's signature

The above particulars of natural persons shall be verified on the basis of original documents issued by reliable and independent sources and recorded in the CI's AML/CFT manual. Specifically, the particulars referred to in Nos. (1)-(4) in the table above shall be verified on the basis of a valid identity card or passport (or equivalent document) or a special identity card of persons serving in law enforcement agencies and the armed forces. The particulars referred to in Nos. (5)-(8) in the table above shall be verified on the basis of documents that are difficult to forge or obtain illegally, including, but not limited to, recent utility bills, dwelling or occupational premises lease agreements certified by internal revenue

offices, certificates issued by internal revenue offices, employers' certificates, copy of the last payroll slip, self-employment startup declarations, occupational identity cards or certificates issued by social security funds.

Copies of the above identity verification documents shall be kept, according to the provisions of Article 35(1b) of Law 3691/2008, for a time period of at least five years from the end of the business relationship or transaction, in a manner ensuring the confidentiality of the data received.

5.5.2 Minimum information required for the identification of legal persons:

S/N	**Legal entities**
1.	***Sociétés anonymes and limited liability companies, including branches of foreign companies with the same legal form***: A. The Société Anonyme & Limited Liability Companies Issue of the Government Gazette where a summary of the statutes of the société anonyme or limited liability company was published, including: • the name, registered office, objects, number of directors (for Société Anonyme) and names of administrators (for limited liability companies); • the names and identity particulars of the company's representatives and their powers; • the number and date of the decision of the authority that approved the formation of the société anonyme, or the registration number referred to in Article 8(1) of Law 3190/1955 "Limited Liability Companies"; • Government Gazette issues in which any amendments to the statutes in connection with the above particulars were published, accompanied by certificates of changes in/amendments to the statutes issued recently by the competent authorities (the court of first instance having territorial jurisdiction on a limited liability company and the prefecture having territorial jurisdiction on a société anonyme); and • identification and verification of the particulars of the beneficial owners, where required, the legal representatives and all persons authorised to operate the company's account, as described in para. 5.5.1 above (unless verified by their official authorisations). B. Regarding society anonym, in addition to the above data, minutes of the general assembly of a Société Anonyme certifying the election of the board of directors and minutes of the board of directors authorising the persons that bind the company with their signatures, as well as a certificate from the Register of Society Anonym on the

	registration of the above minutes, or the Government Gazette Issue in which this certificate was published.
2.	***Partnerships***: • certified copy of the original statutes that have been filed to the court of first instance, including any amendments thereto; • a certificate of amendments to the original statutes issued recently by the court of first instance having territorial jurisdiction on the partnership; and • identification and verification of the particulars of the partners, the legal representatives and all persons authorised to operate the company's account, as described in para. 5.5.1 above (unless verified by their official authorisations).
3.	***Other legal persons or trusts***: • establishing documents, as appropriate, whether originals or copies certified by a public authority; and • identification and verification of the particulars of the legal representatives and all persons authorised to operate the company's account, as described in para. 5.5.1 above (unless verified by their official authorisations).

With respect to companies, a "beneficial owner" shall be understood as:

(i) the natural person(s) who ultimately own(s) or control(s) a company through direct or indirect ownership of or control over a sufficient percentage of the shares or voting rights in the company, including through bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards; a percentage of at least 25% shall be deemed sufficient to meet this criterion;

(ii) the natural person(s) who otherwise exercise(s) control over the management of the company.

With respect to the certification of the identity of legal persons or entities, the completeness of the required authorisations and certificates shall be certified by CIs' legal departments. Regarding société anonyme and limited liability companies, the relevant database of the National Printing Office shall be consulted (on its website, www.et.gr).

Copies of the above documents shall be kept for a time period of at least five years from the end of the business relationship or transaction, in a manner ensuring the confidentiality of the data received.

5.6 With respect to legal persons or entities incorporated outside Greece and having no establishment in Greece, CIs shall request documents bearing an Apostille under the Hague Convention of 5 October 1961, officially translated into Greek if considered necessary by CIs for better comprehending their contents, as well as data similar to those referred to in para. 5.5.2 above. In any case, a CI shall obtain through the documents produced the following information: full name, lawful incorporation of the legal person according to the laws of its country of establishment, nature and objects, country of incorporation and establishment, address, identity particulars of beneficial owners, where required, legal representatives and all persons authorised to operate the company's account, as described in para. 5.5.1 above. The identity of the legal person or entity shall be verified by using reliable and independent documents, data or other information. The CI shall take appropriate measures to verify the ownership structure and control of the legal person or entity.

5.7 CIs shall require counterparties or customers acting on behalf of another natural person, in addition to identifying themselves, to disclose and prove the identity particulars of the other natural or legal person on behalf of whom they act. In any case, CIs shall also verify these particulars where the counterparty or customer has not made such disclosure, but there are doubts whether he is acting on his own behalf. If during the business relationship a CI doubts whether a counterparty or customer is acting in his own behalf, it shall take the measures required for collecting information on the real identity of the person on behalf of which they are acting.

5.8 CIs shall apply, at appropriate times and on a risk-sensitive basis, CDD procedures not only to new, but also to existing customers, and shall ensure that their customers' identity particulars are continuously updated throughout the business relationship. Specifically, CIs shall review, on a regular basis or whenever there are doubts about their validity, the data in their possession and, at least on an annual basis, the data on high-risk customers. The results of such examination shall be recorded and kept in the customer's file. If the updating of the customer's identity particulars is not achieved, the CI shall terminate the business relationship and consider submitting a report to the AML/CFT Commission.

5.9 CIs shall ensure the assessment of the customer's overall portfolio with the CI and possibly other companies of the group, according to Article 32(2) of Law 3691/ 2008, in order to verify the relevance and compatibility of the examined unusual or suspicious transaction with this portfolio(s).

5.10 In the case of joint accounts of savings, securities or other financial products, all the co-owners of these accounts shall be considered as customers and CDD shall apply to them.

5.11 In the cases of a transaction or a series of linked transactions in which more than two obligated persons participate, according to Article 5 of Law 3691/2008, CDD shall apply to each one of them. This shall apply in particular to insurance polices, sales of shares, contracts on derivatives, bonds or other financial products and transactions through cards of any nature.

5.12 CIs shall treat with caution applications for renting of safe deposit boxes by persons who do not keep accounts with the CI concerned, following the envisaged identification procedures.

5.13 CIs shall request all CIs abroad with which they have established or are going to establish correspondent banking relationships to complete and sign a questionnaire stating their AML/CFT policies and procedures. If correspondent banking relationships are established with CIs from third countries, the additional CDD measures referred to in para. 5.15.9 below shall apply.

5.14 The identity particulars of the customer, any other person on behalf of which the customer is acting and the beneficial owner shall be certified and verified before the establishment of a business relationship or the conduct of a transaction. By way of derogation, the verification of the above persons' identity particulars may be completed during the establishment of the business relationship if required in order not to interrupt the smooth conduct of transactions and provided that the risk of commission of the offences referred to in Article 2 of Law 3691/2008 is low. In these cases, the verification procedures shall be completed as soon as possible after the initial contact. If the verification of the customer's identity particulars is not achieved, the CI shall terminate the business relationship and consider submitting a report to the AML/CFT Commission.

5.15 Enhanced CDD

In the event that CIs consider that there is increased risk, they shall conduct enhanced CDD, according to the provisions of Chapter 4 above, reassessing customers and business relationships on an at least annual basis. To this end, the branch or unit shall prepare a brief report with aggregated data on the reassessment of high-risk customers, which shall be sent to the Compliance Officer. The reports shall be processed by the Compliance Officer, who shall submit an overall report, recommending the termination of some business relationships, to the CI's Board of Directors, which shall decide thereon. Follows a list of minimum required high-risk categories.

5.15.1 Non-residents' accounts

Customers having their residence abroad shall be subject to the same information requirements and identity verification procedures as those who live permanently in Greece.

Specifically, non-residents shall be requested to produce their passports (or identity cards, for those coming from EU Member States) issued by their home country, plus (for non-EU residents) a temporary stay permit or other equivalent document, entry visa or seal, where required. Furthermore, when there is any doubt concerning the identity of a person, the CI shall seek verification and authentication of these documents by the embassy or consulate of the issuing country in Greece, or by reliable CIs in the customer's home country.

The above information is also necessary for compliance with the sanctions imposed on countries or persons by the United Nations or the European Union. In this connection, the number, date and country of issuance of the customer's passport shall always be recorded.

5.15.2 Politically Exposed Persons

I. Politically Exposed Persons (PEPs) are natural persons that are or have been entrusted with a prominent public function, including their immediate family members or the persons known to be their close associates.

According to Article 22 of Law 3691/2008, natural persons entrusted with a prominent public function include:

(a) heads of state, heads of government, ministers, alternate and deputy ministers;

(b) MPs;

(c) judges of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, other than in exceptional circumstances;

(d) judges of courts of auditors;

(e) members of the boards of central banks;

(f) ambassadors and chargés d' affaires;

(g) high-ranking officers in the armed forces; and

(h) members of the administrative, management or supervisory bodies of state-owned enterprises.

None of the categories in (c) to (h) above shall be understood as covering middle-ranking or junior officials. The categories in (b) to (g) above include functions exercised at the EU and international levels.

Immediate family members of the persons referred to in the above paragraph shall include:

(a) the spouse;

(b) any partner considered by national law as equivalent to a spouse;

(c) natural or adopted children and their spouses or partners; and

(d) the parents.

Persons known to be close associates shall include:

(a) any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relationships, with a person referred to in the above paragraph; and

(b) any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been established for the benefit of a person referred to in the above paragraph.

Without prejudice to the application, on a risk-sensitive basis, of enhanced CDD measures, where a person has ceased to be entrusted with a prominent public function for a period of at least one year, CIs shall not be obliged to consider such a person as politically exposed.

II. CIs shall adopt the following additional CDD measures when establishing a business relationship with a PEP:

They shall:

(a) apply the appropriate procedures, on a risk-sensitive basis, to determine whether the customer is a PEP;

(b) obtain senior management's approval of the establishment of business relationships with such customers;

(c) take adequate measures to verify the origin of the wealth and funds that the business relationship or transaction concerns; and

(d) monitor the business relationship on a continuous and enhanced basis.

III. In the case of accounts of legal persons and other entities, the procedures applied shall aim at verifying whether the beneficial owners, legal representatives and persons authorised to operate the relevant account are PEPs. If any of the above persons is identified as a PEP, these legal persons' and other entities' accounts shall automatically be subject to the enhanced CDD measures referred to in the Law and this Decision.

IV. Usual CDD measures shall apply to PEPs established in Greece.

5.15.3 Accounts of companies with bearer shares

CIs shall apply at least the following CDD measures to companies with bearer shares that do not fall within the scope of para. 5.17:

(i) Before opening the account, they shall certify and verify the identity of the beneficial owners, legal representatives and the persons authorised to operate the bank accounts of the company on the basis of reliable and independent sources and/or by visiting the company's offices for this purpose.

(ii) They shall compare regularly the actual transactions through the account with those expected on the basis of the company's profile. Any significant divergences shall be scrutinised and the findings shall be entered in the company's file.

(iii) They shall obtain from the legal representative of the company a declaration in writing to the effect that, if the shares of the beneficial owners are transferred to a third party or there is any material change in the company's status, he shall immediately inform the CI, unless the same commitment is made in an agreement with the company. If there is any change in the beneficial owners of the company, CIs shall consider whether or not to continue the business relationship.

(iv) They shall consult the database of the National Printing Office (on its website, www.et.gr) in order to verify any changes in the ownership of the company or any other material changes (such as dissolution, liquidation etc.).

(v) They shall examine whether the company asking to open an account has established its central management, branches or subsidiaries or is otherwise active in any other countries.

5.15.4 Accounts of offshore companies and special purpose vehicles (SPVs)

Where the customer is a company that has no commercial or productive activity in the place of its establishment, such as an ***offshore company*** or a company referred to in Emergency Law 89/67, as currently in force, or an SPV, CIs shall conduct enhanced CDD.

To determine the countries where offshore companies operate, decision No. 1108437/2565/DOS of the Deputy Minister of Finance (Government Gazette B.1590/ 16.11.2005) or any regulatory act amending or replacing it shall be taken into account.

CIs shall apply at least the following CDD measures to the above companies:

- They shall take appropriate measures to fully verify the ownership structure and control of the company and to identify the beneficial owners. In order to identify the beneficial owners, CIs shall require either (i) a declaration in writing by the legal representative of the company together with certified copies of certifications and verifications of the beneficial owners' identities; or (ii) certification and verification of their identity by a lending officer of the CI, following approval by a member of senior management, on the basis of documents, data or information from a reliable and independent source. In the latter case, CIs shall keep a file of the offshore company, in which all relevant documents shall be kept, which shall be updated and communicated, if officially requested, to the Bank of Greece.

- They shall obtain from the legal representative of the company a declaration in writing to the effect that, if the shares of the beneficial owners are transferred to a third party or there is any material change in the company's status, he shall immediately inform the CI. If there is any change in the beneficial owners of the company, CIs shall consider whether or not to continue the business relationship.
- They shall compare regularly the actual transactions through the account with those expected on the basis of the company's profile. Any significant divergences shall be scrutinised and the findings shall be entered in the company's file.

5.15.5 Trusts

Trusts are not separate legal entities and, therefore, business relationships are established through trustees acting on behalf of the trust. CIs shall take reasonable measures, on a risk-sensitive basis, to comprehend the ownership and control structure of trusts.

When they establish such relationships, CIs shall verify the name and date of establishment, the identities of trustors, trustees and beneficial owners, the nature, objects and activities of the trust, as well as the source of its funds. CIs shall obtain copies of the establishing documents of the trust and any other necessary information on the beneficial owners, and shall keep the relevant data and information in the customer's file.

For the purposes of this paragraph, a beneficial owner shall be:

(i) the natural person(s) entitled to at least 25% of the assets of the legal entity or arrangement, provided that the future beneficiaries have already been determined;

(ii) the class of persons in favour of which the legal entity or arrangement has been established and operates, provided that the beneficiaries of the legal entity or arrangement have not been determined yet; or

(iii) the natural person(s) exercising a control over at least 25% of the assets of the legal entity or arrangement.

5.15.6 Accounts of non-profit organisations

With respect to accounts of non-profit or public benefit agencies, organisations, associations, societies and other unions, CIs shall verify the legitimacy of their incorporation and objects, requiring the submission of a certified copy of their establishing deed (charter, private agreement etc.), their certificate of incorporation, certificate of registration and the number of their registration by the competent public authority. When such an entity has appointed more than one authorised signatories to operate its account, the identities of all authorised

signatories shall be verified, according to the identity verification procedures for natural persons provided for hereunder.

5.15.7 Portfolio management accounts of important clients

CIs shall take the following additional CDD measures where they undertake the management of portfolios of important clients:

- A member of senior management in charge of accepting new important customers that open portfolio management accounts shall grant his approval.
- CIs shall verify the identity of all the beneficial owners of such accounts.
- CIs shall verify whether the owner of the account is a PEP.
- CIs shall establish the source of the assets managed and the expected use of the account by the owners.
- CIs shall examine whether the operation of the account is consistent with its purpose and the owners' profiles.

5.15.8 Non-face-to-face transactions

CIs that provide their customers with the possibility of carrying out non-face-to-face transactions, notably opening accounts (phone banking, e-banking etc.), shall adopt specific and appropriate organisational, operational and technological procedures that ensure their compliance with the requirements of Law 3691/2008 and this Decision, in relation to the verification of customers' identity, in order to tackle the higher risk from such transactions, and shall in particular implement all or any of the following measures:

(i) ensure that the customer's identity is verified through additional evidence, data or information;

(ii) take supplementary measures to control or certify the documents submitted or require confirmation by a CI or FI established in an EU Member State or a state with an equivalent supervisory regime;

(iii) ensure that the first payment in the context of the business relationship or individual transactions be made through an account in the name of the customer kept with a CI operating in an EU Member State or a state with an equivalent supervisory regime;

(iv) obtain verification of the customer's full name, address and signature from a CI operating in his home country;

(v) obtain a letter of recommendation from a third obligated person applying the certification procedures referred to in Law 3691/2008; and

(vi) require the customer to send to the CI certified photocopies of identification documents, e.g. passport, identity card.

The requirements for natural persons set forth hereinabove shall also apply to companies or organisations requesting the opening of an account by mail or e-banking.

5.15.9 Cross-border correspondent banking relationships

With respect to cross-border correspondent banking relationships with banking institutions from third countries, CIs shall:

(a) gather sufficient information about the correspondent banking institution to fully understand the nature of the correspondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision;

(b) assess the correspondent institution's AML/CFT controls;

(c) take into account the country assessment reports of FATF, the IMF and the World Bank, as well as other independent and reliable sources, to evaluate the adequacy of the AML/CFT system in place in the correspondent institution's country of establishment;

(d) obtain from the correspondent institution a completed and signed questionnaire, such as, indicatively, the Wolfsberg Group questionnaire, describing the CI's AML/CFT policies and procedures;

(e) obtain approval from senior management before establishing new corresponding banking relationships;

(f) specify clearly their own responsibilities and those of the correspondent institution under the banking correspondence agreement; and

(g) with respect to payable-through accounts, be satisfied that the correspondent institution has verified the identity and performed ongoing monitoring of the customers having direct access to accounts of the correspondent, and that it is able to provide relevant CDD data upon request by the CI.

CIs shall not establish or continue correspondent banking relationships with shell banks or continue correspondent banking relationships with banks that are known to allow their accounts to be used by shell banks.

5.15.10 Countries that do not comply adequately with the FATF recommendations

CIs shall examine with particular attention transactions and conduct additional ongoing monitoring of business relationships and transactions with natural persons or legal entities, including CIs and FIs, from non-cooperative or non-compliant countries.

All transactions with natural persons or legal entities from these countries shall be examined with particular attention and, if such examination gives rise to doubts about the legitimate

origin of funds, a report shall be submitted to the AML/CFT Commission. The results of the examination shall be recorded and kept on file for at least five years, including all the documentation.

To assess country risk for AML/CFT purposes, CIs may use the following criteria:

- announcements by FATF concerning countries or territories that do not comply or comply inadequately with its recommendations;
- country assessment reports issued by FATF, regional bodies that have been established and operate according to its standards (e.g. Council of Europe Moneyval Committee), the International Monetary Fund and the World Bank;
- list of countries or jurisdictions which, according to the Common Understanding of the Committee for the Prevention of Money Laundering and Terrorist Financing, which assists the European Commission, have equivalent AML/CFT systems to the EU;
- inclusion in non-cooperative countries or tax havens;
- inclusion in the EU, UN and OFAC lists;
- FATF membership;
- implementation of EU directives;
- implementation of the Wolfsberg principles; and
- ratification of the UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988.

5.16 Cash transactions

CIs shall examine with particular attention cash transactions of a considerable amount in order to verify the origin of cash and whether the amount and nature of the transaction are compatible with the customer's profile. In addition to taking the CDD measures described in para. 5.4(vi), CIs shall obtain all documents and data required for proving the need to carry out a considerable cash transaction.

If a customer requests to withdraw an amount of over €250,000.00 in cash, it is recommended that the money be delivered to the customer by cheque or an order for payment to a bank account, unless there are specific and adequately proved reasons that warrant a cash withdrawal.

5.17 Simplified CDD

I. According to Article 17 para. 1 of Law 3691/2008, CIs shall apply simplified CDD when the customer is a CI or FI established in the EU or a CI or FI established in a third country that imposes requirements at least equivalent to those of Directive 2005/60/EC and the CI or

FI which is established in a third country is subject to supervision for compliance with such requirements.

II. CIs shall not be required to verify the identity of their customers according to para. 5.5.2 above when the customer is:

(a) a listed company whose shares are traded on one or more regulated markets in the EU, within the meaning of Article 43 of Law 3606/2007, or the legislation of another Member State, compatible with the provisions of Directive 2004/39/EC; or

(b) a company that operates as a UCIT according to Article 2 of Law 3238/2004, is established in the EU and is governed by the legislation of the home country which is compatible with the provisions of Directive 85/611/EEC, as currently in force; or

(c) a Greek public authority or legal person in public law or business or organisation in which the State has an ownership stake of at least 51%;

(d) a public authority or organisation meeting the following conditions:

(i) it has been entrusted with a public function according to the Treaty on European Union, the Treaties establishing the European Communities or the secondarily Community law;

(ii) its identity is publicly known, transparent and fixed;

(iii) its activities and accounting practices are transparent; and

(iv) it is accountable to either a Community institution or the authorities of a Member State, or there are appropriate procedures in place ensuring supervision and control of its activities.

In the cases of paras. I and II above, obligated persons shall collect adequate information to judge whether the customer should be exempted within the meaning of the said paragraphs and shall decide according to the risk management procedures described in Chapters 4 and 5 above.

Natural persons carrying out transactions on behalf of the above customers shall not be exempt from the identification and verification requirements.

III. Moreover, CIs shall apply simplified CDD measures in the case of electronic money, within the meaning of Article 14(3) of Law 3148/2003, provided that the monetary value stored in the electronic device, if it cannot be reloaded, does not exceed €150.00 or, if the electronic device can be reloaded, the total amount of transactions in a calendar year does not exceed €2,500.00. If the bearer redeems, under Article 14(6) of Law 3148/2003, an amount of €1,000.00 or more in a calendar year, identity verification shall be required.

In the cases of paras. I-III above, CIs shall not apply simplified CDD when there are suspicions of ML or FT.

6. PERFORMANCE BY THIRD PARTIES

6.1 CIs may rely on third parties, within the meaning of Article 23 of Law 3691/2008, to carry out the customer and beneficial owner identification and verification procedure, provided that the ultimate responsibility for customer identification and verification remains with the CI relying on such third party. The third party shall have as a customer the person designated by the CI and shall apply the appropriate CDD and record-keeping measures, according to the provisions of this Decision or a similar decision of an EU Member State or a third country with an equivalent supervisory regime. CIs shall verify that the third party is subject to a statutory licensing regime in its country of incorporation/home country and to supervision for AML/CFT purposes.

For the purposes of this chapter, third parties shall include:

- credit institutions;
- investment firms;
- mutual fund management companies; and
- the insurance companies referred to in Article 4(3)(m) of Law 3691/2008,

situated in an EU Member State or a third country which is a member of FATF or has an equivalent supervisory regime.

6.2 A CI relying on a third party shall ensure that:

- the customer's or beneficial owner's identity data are made available to them immediately; and
- the documents verifying the identity of the customer or beneficial owner and other relevant documents are transmitted to it by the third party upon request without delay.

6.3 In addition to the identification and verification data provided by third parties, CIs shall receive directly from the customer or beneficial owner and/or third sources such additional data and information as are required for formulating and updating the customer's profile, on a risk-sensitive basis.

6.4 If the third party's business relationship with the customer is terminated for any reason whatsoever, the CI shall verify the customer's identity and apply all CDD measures.

7. RECORD KEEPING

7.1 CIs shall keep at least the following records for a period of **at least five years** after the business relationship with their customer has ended or a transaction has been executed, unless they are required by law to keep such records for a longer time period:

- the customer's identification and verification data as at the time of conclusion of every agreement;
- authorisations, copies of customer identification and verification documents, as well as the originals or copies of documentation of any transactions;
- internal documents such as approvals or findings or recommendations on matters relating to the investigation of the offences referred to in Article 2 of Law 3691/2008, whether or not they have been reported to the AML/CFT Commission, as specified in para. 8.6 of this Decision; and
- the relevant correspondence with customers.

7.2 CIs shall have in place record-keeping procedures and systems capable of ensuring, for the aforementioned time period, the reproduction of information on the identification and transactions of customers, with a view to responding without delay to any request by the AML/CFT Commission or any other competent authority. Indicatively, CIs shall be capable of reproducing the following information:

- data certifying the identity of the owners of an account;
- data certifying the identity of the beneficial owners of an account;
- data certifying the identity of the persons authorised to operate an account;
- the authorisations of natural persons of any nature;
- data certifying the identity of managers and legal representatives authorised to operate the account of a legal person;
- the original records and documentation of transactions;
- data on the volume and value of transactions through the account;
- data of all the other accounts of the account owner;
- the source of funds;
- the nature and currency of each transaction;
- the manner of deposit or withdrawal of funds (cash, cheques, wire transfer etc.);
- the identity of the person who carried out the transaction;
- the destination of funds;
- customers' written instructions and authorisations; and

• the nature and number of the account involved in the transaction.

7.3 According to Article 36 of Law 3691/2008, CIs shall apply in their subsidiaries and in their branches in other countries record and data keeping measures which are at least equivalent to those provided for hereunder. Where the legislation of a non-EU country does not allow the implementation of such measures, wholly or partly, CIs shall inform to this effect the AML/CFT Commission, the Central Coordinating Authority and the Bank of Greece.

7.4 Instead of keeping documentation and records in physical form, CIs may keep files in electronic form.

8. DETECTION, HANDLING AND REPORTING OF UNUSUAL OR SUSPICIOUS TRANSACTIONS

8.1 CIs shall examine with due diligence any transaction that is particularly likely, by its nature, to be associated with ML or FT. As a general rule, such transactions are suspicious and unusual transactions within the meaning of Article 4(13) and (14) of Law 3691/2008, as well as any complex or unusually large transaction.

Suspicious transactions are understood as transactions or activities giving rise to sufficient indications or suspicions of actual or attempted commission of the offences referred to in Article 2 of Law 3691/2008 or of involvement of the customer or beneficial owner in criminal activities, on the basis of the assessment of data of the transaction (nature of transaction, financial instrument, frequency, complexity and value of the transaction, use or non-use of cash) and the person (occupation, financial condition, transactional or business behaviour, reputation, past record, level of transparency of customers who are legal persons, and other important characteristics).

Unusual transactions are understood as transactions or activities incompatible with the customer’s or beneficial owner’s profile (transactional, professional or business behaviour, financial condition) or have no apparent purpose or motive of a financial, professional or personal nature.

CIs shall have adequate information, be familiar with their customers' profiles and have in place a risk assessment system, using their experience and information from other sources, in order to be capable of detecting in time any unusual or suspicious transaction.

A decision of the Bank of Greece shall lay down an indicative typology of unusual or suspicious transactions and activities.

8.2 After the examination of these transactions, if there are any suspicions of actual or attempted commission of ML or FT, the CI shall submit an unusual or suspicious transaction report to the AML/CFT Commission. This requirement shall also extend to attempted unusual or suspicious transactions.

8.3 The submission of an unusual or suspicious transaction report to the AML/CFT Commission shall be preceded by:

(i) Receipt of a report submitted to the Compliance Officer by other management officers or employees of the CI. In branches or special departments or units, this report shall be submitted directly to the manager of the branch or the director of the department or unit, who shall immediately report to the Compliance Officer, provided that he shares the suspicions. If the manager/director or his alternate is unavailable or refuses or neglects or does not share the suspicions of the reporting employee, the employee may report to the Compliance Officer.

(ii) Receipt and processing of alerts of unusual or suspicious transactions produced by the CI's IT system.

(iii) Assessment and examination of the reports and alerts received by collecting information from reliable sources, such as Tiresias, ICAP and recognised databanks. The assessment results shall be recorded and kept in the relevant file.

8.4 Unusual or suspicious transactions reports submitted to the Compliance Officer or produced by the IT system shall include at least the following data:

- date;
- full particulars of the reporting branch or service;
- all the available information on the customer and the transaction;
- the date of conduct of the transaction and establishment of the business relationship and a full record of transactions;
- justification of the transaction; and
- in international transactions, the origin and course of the incoming or outgoing remittance.

8.5 CIs' employees and management officers shall not disclose to the customer involved or any third party that they have officially reported or requested information or that an investigation into ML/FT is being or will be conducted, according to Article 31 of Law 3691/2008. By way of exception to the above prohibition of disclosure, the following shall be allowed: (a) exchange of information on unusual or suspicious transactions between CIs or FIs that belong to the same financial group and are situated in Greece or in another Member State or in a third country with an equivalent supervisory regime; and (b) exchange of

information between CIs or FIs on the same customer and the same transactions or activities in which participate two or more CIs or FIs that are situated in Greece or in another Member State or in a third country with an at least equivalent supervisory, professional confidentiality and personal data protection regime.

If, after the submission of a report, a CI decides to terminate the business relationship with the customer in order to avert the risks from its continuation, it shall ensure that the reason of termination of the business relationship is not disclosed to the customer.

8.6 CIs shall apply specific procedures for keeping records of the reports filed to the AML/CFT Commission, in order to ensure confidentiality and accessibility. CIs shall keep:

- a record in the branch or unit, containing reports by employees to the manager that have been transmitted to the Compliance Officer, including all the accompanying documents;
- a record in the branch or unit, containing reports by employees to the manager that were not transmitted to the Compliance Officer, including all the accompanying documents justifying such non-transmission;
- a record containing all the reports sent by employees, branch managers and unit directors to the Compliance Officer, including all the accompanying documents and any justification in writing for cases not reported to the AML/CFT Commission; and
- a record containing all the reports sent to the AML/CFT Commission by the Compliance Officer, including all the accompanying documents.

All the documents in the report records shall be kept in a special file and shall be dated and signed by the reporting employees, managers/directors and Compliance Officers. Alternatively, the reports may be kept in electronic files, provided that they meet the conditions of controlled access, application of user ID and dating.

8.7 Measures to protect reporting persons

CIs shall take appropriate measures to protect the Compliance Officer reporting unusual or suspicious transactions to the AML/CFT Commission, as well as their employees filing internal reports of their suspicions of attempt or commission of ML/FT, including by keeping their anonymity vis-à-vis reported customers or any third parties, other than the persons or authorities specified by law.

9. INTERNAL CONTROL AND COMMUNICATION PROCEDURES

9.1 In addition to applying the AML/CFT procedures and measures, CIs shall ensure that:

- All employees know the person to whom they must report their information on transactions they believe or suspect are aimed at ML or FT.

- There is a clear and short channel of communication for reporting information on suspicious and/or unusual transactions to the Compliance Officer. The internal AML/CFT practice, procedures and controls shall be recorded in a manual, to be distributed to all the employees that handle, monitor and control customers' transactions in any manner.
- There shall be a clear assignment of duties and responsibilities within the CI in order to ensure effective management of the AML/CFT policy and procedures and compliance with this Decision. In particular, the Board of Directors shall adopt and approve an effective AML/CFT policy and shall monitor its proper implementation via the Control Committee referred to in Bank of Greece Governor's Act 2577/2006. The Compliance Officer's duties and responsibilities are set out in detail in Chapters 2 and 3 of this Decision.

9.2 CIs shall ensure that the Internal Audit Unit carries out specialised controls which are adequate for the purposes of identifying, assessing, monitoring and managing ML/FT risk. In addition, the Compliance Officer's Special Service shall monitor and assess the proper and effective implementation of the CI's AML/CFT policy and procedures. The nature and scope of both systems and controls shall depend on the following factors, without limitation:

- nature, scope and complexity of the CI's operations;
- differentiation of the CI's activities, including by geographical area in which such activities are conducted;
- customer profile and the CI's products and activities;
- distribution channels of the CI's products;
- volume and size of the CI's transactions; and
- risk level associated with each field of the CI's activity.

9.3 The above-mentioned controls shall cover, *inter alia*, the following:

- appropriate AML/CFT training with a view to ensuring that employees are aware of and understand their obligations stemming from legislative and regulatory provisions and their role in AML/CFT risk management;
- appropriate documentation of AML/CFT risk management strategy and its implementation by the CI;
- appropriate measures to ensure that AML/CFT risk has been taken into account in the CI's daily transactions, including measures in relation to:
  - development of new products;

– customer acceptance; and
– changes in the CI's business profile.

9.4 The assessment of the AML/CFT system in terms of adequacy and efficiency shall be included in the external auditors' report prepared in accordance with the provisions of Bank of Greece Governor's Act 2577/2006, Annex 3, Chapter IIe.

10. STAFF TRAINING

10.1 The successful implementation of efficient policies and procedures is based on understanding the need to prevent ML and FT. Developing and monitoring comprehensive and modern training courses contributes considerably to the efficiency of the AML/CFT system.

10.2 CIs shall provide training to their staff, including web training, allowing:

- staff to be updated on legislation and on their obligations stemming from the provisions in force and the procedures adopted by the CI, including those related to issues such as customer identification, record keeping and internal reporting;
- for adequate flexibility in terms of training time and content, depending on the individual staff categories and their tasks (new staff, staff serving customers, compliance function staff, staff engaged in attracting new customers);
- for the regular repetition of training in order to ensure that staff are aware of their tasks and duties and are kept abreast on any new developments.

11. WIRE TRANSFERS

11.1 CIs shall apply Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds. In order to properly implement this Regulation, CIs shall take into account the relevant Common Understanding (CEBS 2008 156/CEIOPS-3L3-12-08/CESR/08-773/16.10.2008) reached by the AML Task Force.

11.2 The following paragraphs set out, without limitation, the major obligations stemming from the provisions of the above-mentioned Regulation, which shall apply in conjunction with the guidance provided for in the Common Understanding referred to above.

11.2.1 CIs providing payment services shall ensure, in accordance with Articles 4 and 5 of the above-mentioned Regulation, that transfers of funds are accompanied by complete information on the payer consisting of his name, address and account number. The address may be substituted with the date and place of birth of the payer, his customer identification number or national identity number. Where the payer does not have an

account number, the payment service provider of the payer shall substitute it by a unique identifier which allows the transaction to be traced back to the payer.

11.2.2 In the case of transfers of funds not made from an account held with a CI and as long as there is no suspicion of ML or FT, the CI shall, in accordance with Article 5(4) of the Regulation, verify the information on the payer only where the amount exceeds €1,000.00, unless the transaction is carried out in several operations that appear to be linked and together exceed €1,000.00. It is hereby clarified that where the amount being transferred exceeds €15,000.00, the relevant provisions of Chapter 5 of this Decision on customer identification shall apply.

11.2.3 In accordance with Article 6(1) and (2) of the above-mentioned Regulation, by way of derogation from Article 5(1) thereof, where both the payment service provider of the payer and the payment service provider of the payee are situated in the Community, transfers of funds shall be required to be accompanied only by the account number of the payer or a unique identifier allowing the transaction to be traced back to the payer. However, if so requested by the payment service provider of the payee, the payment service provider of the payer shall make available to the payment service provider of the payee complete information on the payer, within three working days of receiving that request.

11.2.4 In accordance with Article 8(1) of the above-mentioned Regulation, the CI shall detect whether, in the messaging or payment and settlement system used to effect a transfer of funds, the fields relating to the information on the payer have been completed using the characters or inputs admissible within the conventions of that messaging or payment and settlement system. The CI shall have effective procedures in place in order to detect whether information on the payer is missing as specified in Article 8 of the Regulation. Under Article 9(1) thereof, if the CI becomes aware, when receiving transfers of funds, that information on the payer required under the same Regulation 1781/2006 is missing or incomplete, it shall either reject the transfer or ask for complete information on the payer. Detailed guidance on such obligation on behalf of the CI is set out in Chapter 3 of the above-mentioned common understanding.

11.2.5 Under Article 9(2) of the above-mentioned Regulation, where a CI identifies that a payment service provider regularly fails to supply the required information on the payer, it shall take steps, which may initially include the issuing of warnings and setting of deadlines, before either rejecting any future transfers of funds from that payment service provider or deciding whether or not to restrict or terminate its business relationship with that payment service provider. In cases where a payment service provider regularly fails to supply the

required information, the CI shall inform the AML/CTF Commission and the Bank of Greece accordingly. It is hereby clarified that informing the authorities on a particular payment service provider does not amount to reporting an unusual or suspicious transaction. More detailed guidance on the application of Article 9(2) of the Regulation in question is set out in Chapter 4 of the above-mentioned Common Understanding.

11.2.6 The CI shall further assess whether the missing information on the payer indicates a suspicious transaction to be reported to the AML/CTF Commission in accordance with the provisions in force and the internal procedures in place.

12. APPLICATION OF THIS DECISION TO FINANCIAL INSTITUTIONS

12.1 In accordance with Article 6(2)(a) of law 3691/2008, the Bank of Greece is the competent supervisory authority for the following financial institutions:

1. leasing companies;
2. factoring companies;
3. bureaux de change;
4. funds transfer intermediaries;
5. credit companies;
6. undertakings other than a credit institution, the principal activity of which is to acquire holdings or to carry on one or more of the activities listed in items (b) to (l) of Article 11(1) of Law 3601/2007; and
7. postal companies to the extent that they conduct the business of a funds transfer intermediary.

12.2 The above-mentioned financial institutions shall adjust the application of the provisions of this Decision to the nature of their business activities (non-acceptance of deposits from the public, exclusive provision of specific products etc.), taking into account the risk level which is inherent in such activities and the legal framework governing them.

12.3 In accordance with the principle of proportionality, as set out in Article 6(4) first sentence of law 3691/2008, the following shall also apply specifically to FIs:

12.3.1 FIs and their authorised representatives shall be responsible for implementing the policies and procedures adopted under Chapter 1 of this Decision.

12.3.2 The Board of Directors of a FI shall, in accordance with the provisions of Chapter 1 of this Decision, be responsible for monitoring and assessing on an annual basis the adequacy of the AML/CTF policy, taking into account the data and information provided for in the Compliance Officer’s Annual Report and the Internal Auditor’s reports and observations, as well as the supervisory authorities’ observations.

12.3.3 In addition to his duties, as defined in Chapter 2 of this Decision, the Compliance Officer of a FI shall assess the adequacy of any authorised representatives in terms of AML/CTF training and knowledge prior to the commencement of their cooperation. The results of such assessment shall be recorder and filed.

12.3.4 A FI's annual report referred to in Chapter 3 of this Decision shall contain information in line with their activities and shall be directly submitted to the Board of Directors for approval and assessment prior to being forwarded to the Bank of Greece.

12.3.5 FIs shall have in place adequate IT systems capable of:

- Controlling the CI's clientele and transactions on the basis of lists of persons or entities subject to sanctions under EU Regulations and Resolutions of the UN Security Council. Control shall be carried out on a real-time basis at the commencement of the business relationship or during the conduct of the transaction. By entering every new list, the IT system shall check all the clientele of the CI.
- Controlling the clientele and transactions on the basis of local lists of persons or entities that have committed criminal offences, prepared by the competent police and judicial authorities. Control shall be carried out on a real-time basis at the commencement of the business relationship or during the conduct of the transaction. By entering every new list, the IT system shall check all the clientele of the CI.
- Controlling all transactions on the basis of the international typology of suspicious transactions communicated regularly by the Department for the Supervision of Credit and Financial Institutions of the Bank of Greece.
- Issuing alerts of unusual or suspicious transactions on the basis of the criteria defined hereinabove.

12.3.6 FIs, other than leasing, factoring and credit companies which are subject to the provisions of this Decision on CIs, shall apply the following identification and certification procedure in relation to natural persons:

- for transactions of up to €1,000.00, the customer shall merely present a valid identity card or passport (or equivalent document); persons employed in the law enforcement agencies and the armed forces shall present their special identity cards;
- transactions from €1,000.00 to €15,000.00 shall require verification of the data of the persons listed in items 1 to 4 of para. 5.5.1 of this Decision on the basis of the above-mentioned documents, photocopies of which shall be kept for a minimum period of 5

years after the end of the business relationship, in a manner ensuring confidentiality of the data obtained;

- transactions of over €15,000.00 shall require full certification of the identity of natural persons in accordance with paragraph 5.5.1 above.

12.3.7 Bureaux de change and funds transfer intermediaries shall apply the provisions of Chapter 11 of this Decision.

12.3.8 For the purposes of assessing the proper implementation of the policy determined by the Board of Directors of the FI, its Internal Audit department shall carry out controls, which shall also extend to any authorised representatives of such FI.

13. OTHER PROVISIONS

13.1 As of the date of entry into force of this Decision, the provisions of Annex 4 of Bank of Greece Governor's Act 2577/2006 (Decision 231/4/13.10.2006 of the Banking and Credit Matters Committee, as currently in force) on the prevention of the use of the financial system for money laundering or terrorist financing shall be repealed. Table III (Typology of transactions giving rise to suspicions of money laundering and terrorist financing) of the above-mentioned Annex shall remain in force until its replacement by a relevant decision to be issued by the Bank of Greece.

13.2 The following sentence shall be added at the end of para. 4 of Chapter III of Bank of Greece Governor's Act 2541/27.2.2004, as in currently force: ''For the purposes of filling in the data of the above-mentioned documents, the identification data referred to in para. 12.3.6 of Banking and Credit Matters Committee Decision 281/17.3.2009 shall be obtained and verified''.

13.3 The following sentence shall be added at the end of para. 4 of Chapter II of Bank of Greece Governor's Act 2536/4.2.2004, as currently in force: ''For the purposes of filling in the data of the above-mentioned documents, the identification data referred to in paragraph 12.3.6 of Banking and Credit Matters Committee Decision 281/17.3.2009 shall be obtained and verified''.

13.4 For the purposes of implementing the provisions of this Decision, the Department for the Supervision of Credit and Financial Institutions of the Bank of Greece is authorised to issue circulars aimed at providing clarifications and guidance to the supervised entities.

The Government Budget shall not incur any expenditure due to the provisions of this Decision.

This Decision shall be published in the Government Gazette (Issue B).