POLICY OF THE BANK

(ALBARAKA TURK PARTICIPATION BANK)

ON

COMPLIANCE WITH OBLIGATIONS TO PREVENT MONEY LAUNDERING

AND FUNDING TERRORISM

ALBARAKA TURK PARTICIPATION BANK

ISTANBUL - TURKEY

POLICY OF THE BANK (ABTPB) ON COMPLIANCE WITH OBLIGATIONS TO PREVENT MONEY LAUNDERING AND FUNDING TERRORISM

1. INTRODUCTION

Detailed herebelow is the policy of our Bank (Albaraka Turk Participation Bank=ABTPB) about anti money laundering and combat against funding terrorism. This policy was prepared in light of the "know your customer" motto, and based on current legistlation pertaining to industry rules for due and accurate recording and maintaining the data on our customers.

1.1. Purpose:

a) To ensure our Bank's compliance with obligations on anti-money laundering and prevention of funding terrorism,
b) To determine strategies for reducing our exposure to possible risks by evaluating our customers, transactions and services with a risk based approach, and, to determine internal controlls and preventive actions, operational rules and responsibilities,
c) To create awareness among our personnel about these topics.

1.2. Scope:

The policies, procedures, control and monitoring methods contained in this document are valid for the General Management and all branches of our Bank.

1.3. General Framework:

The Compliance Unit must take necessary actions to ensure that the entire staff members of the Bank have standard level of knowledge and information regarding the following subjects, and update the information when required:

a) Concepts of crime proceeds and laundering crime proceeds.
b) Stages of money laundering.
c) Methods of money laundering.
d) Historical development of the combat against money laundering, international actors and multilateral agreements.
e) Prevention of funding terrorism;
    1) The main sources of funding terrorism. (Legal or illegal activities)
    2) Similarities and differences between money laundering and funding terrorism.
f) Prevention of corruption, and combat against bribery and similar financial crimes;
    1) Concept of corruption and the importance of the struggle against it.
    2) Ethical principles of the Bank.

1.4. Legal Regulations and Responsibilities:

The Bank's personnel are responsible to know all our legal and administrative obligations in combat against the laundery of revenues driving from crime and funding terrorizm, and the regulatory and supervisory agents. These are listed below:

14.1. Laws;

1. Law Nr. 5549: Prevention of Laundering The Proceeds of Crime,
2. Law Nr. 5237: Turkish Criminal Code,
3. Law Nr. 5271: Code of Criminal Adjudication Procedures,
4. Law Nr. 5235: Formation, Duties, Powers of Primary Civil Courts and Regional Justice Courts,
5. Law Nr. 5326: Misdemeanors,
6. Law Nr. 5411: Banking Law,

1.4.2. Regulations

1. Regulation on Compliance Program about prevention of money laundering and funding terrorism.
2. Regulation on the enforcement of Law Nr. 4208.
3. Regulation on Tasks and Working Principles of the MASAK Specialists.
4. Regulation on the Principles and Procedures of Controlled Delivery Application.
5. Regulation on Investigation of Money Laundering Crimes.
6. Regulation on the Working Principles and Procedures of the Coordination Committee for Combat Against Financial Crimes.
7. Regulation on the Preemptive Actions Against Laundering Crime Proceeds and Funding Terrorism.

1.4.3. Communiqués
These are the communiqués published by MASAK (Financial Crimes Investigation Board of Turkey).

1.4.4. Sanctions
1. Criminal Penalties (jail sentences , fiscal judiciary fines)
2. Legal (procedural) Penalties (issues about licencing)
3. Administrative Penalties (monetary fines)

1.4.5. Legal Authorities
1. Financial Crimes Investigation Board (MASAK)
2. Banking Regulation and Supervision Agency (BDDK)
3. Central Bank of Republic of Turkey (TCMB)
4. Capital Markets Board of Turkey (SPK)

1.5. Duties, Responsibilties and Powers of the Compliance Unit:
Duties, responsibilties, and authorities of the Compliance Unit are determined by the Compliance Unit Manual which is approved by the Board of Directors of our Bank (ABTPB).

1.6. Duties, Responsibilties and Powers of the Compliance Officer:
Duties, responsibilties and authorities of the Compliance Officer who is appointed by our Board of Directors, are stated herebelow;
1. To make necessaries preperations in order to conform our bank's compliance to the laws and regulations issued for prevention of money laundering and funding terrorism.
2. To provide necessary liason, communication and coordination with MASAK.
3. To establish related policies and procedures of the Bank and submit them to Board of Directors for approval.
4. To compose the policy on managing the related risk and conduct risk management activities.
5. To compose the policy of monitoring and controlling while conducting related activities.
6. To obtain Board of Directors' approval for works on education programs related with prevention of money laundering and funding of terrorism effectively.
7. To evaluate the information and findings regarding suspicious transactions transmited to him/her or obtained on his/her own within his/her capacity and means, and report to MASAK the transactions which he/she deems suspicious.
8. To take precations for ensuring confidentiality of these reports and other related points.
9. To keep regular records on the information and statistics related to internal audit and education activities and to send them to MASAK every March.
10. In the scope of ensuring necessary liason, communication and coordination with MASAK;
    a) to fulfil the Bank's obligation to provide information and documents to MASAK,
    b) to act honestly, independently, bona fide, reosanably, fairly while exercising his/her job and responsibilities.
11. To call for any information and documents related with his/her job from all units of the Bank.

2. RISK MANAGEMENT POLICY

2.1. Purpose :
Identifiying, rating, monitoring, evaluating and reducing potential risks that our Bank may be exposed to.

2.2. Knowing the Customer
The most effective way to protect the Bank from money launderers is to establish and strict adeherence to policies, principles and rules in compliance with the related legislation, based on "know your customer" motto. The aim is to achieve full clarity about the information and banking operations of customers while creating and maintaining a relationship based on mutual trust.

2.2.1. Admission of Customer - Common Principles
During the admission of customer, in order to prevent our Bank from being exploited for money laundering, the Compliance Unit must have sufficient information about customers regarding the followings:
a) In relation with its identity, to check and verify the information and documents listed/sought in the Regulation On Precautions To Prevent Money Laundering and Funding Terrorism,
b) Consistency of documents and information provided by customer,

c) The purpose of customer in preferring our Bank and opening the account with us,
d) Profession of the customer, the main line of business that generates its income,
e) The capacity and profile of its transaction with our Bank,
f) The business venue, office or workshop of the customer,
g) The reputation of customer in the market,

And, in order to create a sound and trustable relationship between the Bank and the customer the Compliance Unit must make necessary in-house arrangements and issue circulars within the Bank.

In this scope, while keeping in mind the nature of the relationship with the customer, (whether it will be temporary or permanent dealing) and paying attention to the type of banking services we will provide him/her, the following lists must not include any record about these customers:

a) The List of Problematic Customers.
b) The List of OFAC (Office of Foreign Asset Control) (which is published by the United States Treasury Department).

We don't provide banking services if these lists carry the name of such customers (individual or institutional personalities).

Furthermore, utmost attention shall be paid to the following points:

a) Our Bank must be protected against international crimes by transactions of money laundering based on adoptation and application of the principles in this document (policy) by all employees of the Bank.
b) Giving maximum attention and care to the acceptance of persons and institutions as customers of our Bank whose wealth and funds are subject to suspicion of legitimacy.
c) In line with the general principle that a bank's relationship with its customers should be based on mutual trust, clarity and exchange of information, those persons who abstain from filling in the necessary documents and identification forms or who present misleading or non-confirmable information shall not be accepted as customers.
d) It will be made sure that no accounts are opened under symbolic or anonymous names or on behalf of third parties (even if the real clients desire so).
e) A continuous surveillance shall be done to observe whether or not the person literally uses the account which is opened on behalf of him/her.
f) Third party proxy accounts for one or more persons shall not be accepted, even if it is documented that they are clearly and legally authorized by legal authority. (Except, the accounts for persons or children who are under tutelage or guardianship).
g) Proxy statements and general instructions should be attested by the public notary, especially if the customer is not known well. A confirmation will be taken from the offices which prepared these documents.
h) The age limit of accounts which belong to children shall be controlled.
i) Private and retail banking or credit relationship will not be instituted with possible clients if prior assessment yields a suspicion on the documents or information about the assets of the persons and banks indicating that these assets were earned illegally. The guarantee and collaterals of these people will not be accepted even if they are not direct clients.
j) Risky banking services such as;
    ja) Renting safe deposit boxes,
    jb) Admitting personal checks in fx for collection, or giving letters of guarantee against cash blockage, shall not be provided,

to those customers who are not very well known and respectable.

2.2.2. Customer Admission and Responsibilities

During the process of filing new customers for the Bank, the identity of customer shall have to be determined. His/her address shall be recorded; and legally necessary documents and data shall be sought and taken (eg. Form For Attorneys). Ratification of these data shall be done and kept in physically and/or electronically safe boxes or files.

For this purpose, cross checks are made through MERNİS system, (the Turkish Republic's ID number), and Finance Ministry Tax ID Number. After the control, if the informations don't match or other unfavorable situations occur (eg. death record etc), Head Office authorities only shall make decision about admission of the customer.

2.3. Principles on Identity Check

In the Bank, customer IDs are determined and addresses (as stated) are recorded and confirmed with respect to types of customers. Copies of such documents are attached to transaction files ones their originals are actually seen. After scanning the original samples of legally required identity documents they must be saved and filed in the computer system of the Bank. All the branches must be able to reach these scanned documents.

In terms of the method of identity check,

a) If the truths of documents which are used to verify the customer identity are suspectable, the geniunity of documents must be confirmed by approaching to the person, institution or other public agent issued these documents as long as it is possible.
b) Systematic verification of the information and data about legal existence and structure of the customer (legal person), real name or title, address, directors and licences of company, documents legally binding the company and defining authorities in the company, must be made by comparison with the official public records of the State (MERNİS, TCKN,VKN, etc.).
c) The authorization and ID details of the proxy claiming to be acting on behal of a customer shall be verified.
d) Verification of IDs shall be performed only by obtaining the documents stated in the law.
e) The data and documents regarding the identity of permanent customers shall be updated. Changes in distribution of powers and state of affairs surrounding the client shall be traced from the Trade Registry Gazette and recorded in the Bank's system. List of authorized signatories shall be kept updated.
f) Original ID of a nonclient ordering a transaction through our Bank shall be checked, copied and registered in computer system of the Bank, regardless of its transaction amount.
g) Accounts shall be opened after the data and documents required in the context of "knowing customers & eligiblity of transactions" are verified.

2.4. Persons and Banks Ineligible as Customer

2.4.1. Persons of Unidentified Address and Identity

Persons and institutions who desire to open an account with our Bank under a different name, abstain from filling up the Customer Bio-data Forms or unwilling to provide other explanatory details required for customer identification, or giving misleading and un-verifiable information shall not be accepted as customers. These types of persons and banks shall never be considered among our target customer groups.

2.4.2. Persons and Organizations Blacklisted by Public Authorities in Context of Combat Against Funding Terrorism and Money Laundering

Persons and organizations whose names appear in the lists issued or to be issued by international and/or local public offices and/or legal institutions engaged in combat against crime revenues shall not be accepted as customer. If in later stages any such negativity emerges about persons or organizations (i.e, banks, companies, ect.) among our customers, the relationship with them shall be ended and their transactions shall not be mediated again. Such cases shall be reported to MASAK as suspicious transactions.

2.4.3. Mail-Box Banks

The banks (shell banks) without any physical address, full time employee/s, unbounded to any public authority in terms of banking operations, licencing, registration and auditing, unattached to any reputable banking organization that has regulations and auditing procedures acceptable by banking practices with regard to prevention of laundering the revenues deriven from crime proceeds shall not be accepted as customer and their transactions must not be mediated by our Bank, directly or indirectly.

2.5. Regions, Persons and Transactions Requiring Special Attention for their Admission as Customer

Persons and institutions operating in the sectors and geographical areas stated below, are considered as carrying higher risk for exploiting our Bank with the purpose of money laundering.

2.5.1. Risky Regions

Transactions from domestic and foreign regions which will be determined by the Compliance Unit shall be considered as carrying high risk. Identity checks and verification procedures for customers living or connected to the risky regions shall be applied with utmost care and in a more controlled manner while executing their transactions.

2.5.1.1. Non-Cooperative Countries

Working relationship with citizens, firms and financial institutions of the countries blacklisted by FATF (in the List of Non-Cooperative Countries) for not complying with its recommendations, or, implementing them in part shall not be established. However, if any transaction is made, utmost attention must be given to it. If the visible economic and legal aim of the transaction is not reasonable or logical, necessary investigations shall be conducted, the findings must be recorded and kept in the transaction file.

2.5.1.1. Grey Areas

The procedures of "knowing the customer" shall be applied more carefully in case the customer (or related transaction) is settled in un-democratic countries and territories where the rate of crimes resulting from smuggling and terrorism is high, corruption and bribery is widespread, and which are on illegal drugs manufacturing and distribution routes. Any suspicious situation shall be reported as required legally.

2.5.1.1. Offshore Centers, Free Zones and Financial Hubs

The procedures of "knowing the customer" shall be implemented meticulously in case the customer is settled in or the transaction is connected to offshore centers, free zones or international finance centers where rigid secrecy rules are applied on banking transactions. Such international money orders, in which the ordering party (the name and/or the title of the orderer) is not clearly mentioned, shall not be processed. The transaction shall be reversed to the originator by International Banking Department of our Bank.

2.5.2. Risky Customers

2.5.2.1. Politically Eminent Persons (PEP's)

Since, some heads of foreign states or governments, chiefs of legislature or military, senior executives of public offices and officials/members of important political parties in countries where corruption is particularly widespread may exploit their political influence for self-enrichment through receiving bribes, embezzlement and in similar ways, they are considered among risky customer type. In this contex, further attention must be paid to the transactions involving politically eminent persons in addition to the standart "knowing the customer" procedures. Therefore, our Bank shall;

a) Obtain approval of concerned unit's/department's/branche's manager, and,
b) Determine the sources of assets and funds of such customers before processing their transactions.

2.5.2.2. Persons Known as Involving in Criminal Activities or Dealing With the Activities Considered Suspicious by General Public

2.5.2.3. The Customers who are Located, Operating or Transacting in Countries where Necessary Legal Regulations on Combat Against Criminal Revenues are not in Place

List of such countries shall be circulated throughout the Bank by the Compliance Unit.

2.5.2.4. The Customers who are Living, Operating or Transacting in Countries Listed Among the "Non-Cooparative Countries" announced by the FATF to its Member Countries

List of such countries shall be circulated throughout the Bank by the Compliance Unit.

2.5.2.5. Waqfs (Charity Organizations) and Assocations

While our branches open account/s for the above stated establishments, open identity of the persons or institutions, main line of their activity, purpose of opening the acounts, expected accounts transactions and services, method of opening the accounts, destinations of incoming and outgoing funds (Cash, EFT, Swift, Local and International) and details about their founders, their authorized representatives, and senior managements must be collected. Our branch managements must take necessary precautions to ensure the recording of all information gathered. This information must be checked during branch inspections.

2.5.2.6. Correspondent Banking

The following points must be taken into consideration while establishing a correspondent banking relationship.

About the bank with which the relationship will be established;

a) Its main line of activity, reputation and adequacy of its internal and external audits shall be determined through publicly available data about the bank,
b) Whether the bank has gone under any investigation, inquisition, prosecution, penalized on charges of money laundering and funding terrorism must be surveyed,
c) The methods that it uses to prevent money laundering and funding terrorism shall be checked and its level of appropriateness to the necessity of "know your customer" must be assessed.
d) Approval of Assitant General of our Bank to whom our International Banking Department reports shall be received before starting a new correspondent banking relationship.
e) It must be assessed whether the correspondent bank has any customer directly accessing its accounts, and if so, whether the obligation of special attention to these customers is fulfilled.

In order to prevent faults in the communication and lack of any information in the records, financial institutions which demand to open a correspondent banking account are required to fill up the questionnaire with the above mentioned data through the mediation of the Correpondant Banking Services of International Banking Department of our Bank. The questionnaire shall be obtained with original signature on it or in SWIFT Message format and must be preserved in the correspondant banking file in order to be given to auditors when requested.
Our Bank does not establish any correspondent relationship, if the answers provided in the questionnarie filled by the interested bank are found inadequate in terms of prevention of crime revenues precedents.

2.5.2.7. Sensitive Sectors and Professions

Utmost attention must be paid while opening acconts for persons or organizations from sectors and occouputions groups which will be determined by Comliance Unit. Customer identification documents, sector information shall be recorded carefully and completely. The custormers' accounts shall be kept under constant and attentive scrutiny. Account activities of those customers must be controlled in branch audits.

2.5.3. Risky Transactions

Risky transactions are customer funds and transactions resulting from ambiguous activities and the activities unrelated with main business line of the orderer. They are generally cash transactions, electronic transfers and the financial products issued in the form 'to the bearer' (cheques etc.) products.

2.5.3.1. Cash Operations

The controls and documentation of transactions that can normally be processed through the bank accounts are desired to be affected in cash by customers, shall be done with utmost care. Branch operator must pay more attention during approval stage of accounting receipts and payment slips of such transaction.

Cash transfer requests from foreigners without opening an account shall not be accepted.

2.5.3.2. Elektronic Fund Transfers

2.5.3.2.1. International Electronic Fund Transfer Messages of TL 2,000.00 and Above

In case of senders of overseas electronic transfer messages amounting to or exceeding TL 2,000.00 (or its equivalent in foreign currencies);

a) Name and surname, title of corporate entity that exists in the Trade Registry and full name of other corporate entities and unincorporated agencies,
b) Account number,
c) At least one of the informations that help to determine the sender , such as ID number(of Republic of Turkey), passport number, tax identification number,
d) Full name and address informations and/or acoount number of beneficiaries,

must be obtained.

2.5.3.2.2. Local Electronic Fund Transfer Messages of TL 2,000.00 and Above

If amount of domestic electronic transfer messages is equel or exceeding TL 2,000.00 (or its equivalent in foreign currencies) the senders';

a) Name and surname, title of corporate entity that exists in the Trade Registry and full name of other corporate entities and unincorporated agencies,
b) Customer number,
c) At least one identification number (i.e. ID number of Republic of Turkey, passport number and tax identification number) that helps determine the sender,

must be obtained.
If the information about orderers and beneficiaries of incoming money transfers is incomplete, these transfers shall be investigated further in the context of suspicious transactions. The services that process the transfers to the beneficiaries must check, verify and keep their ID and address details with due diligence.

2.5.3.3. Cashing of Personal Checks Drawn on Banks Abroad

Foreign exchange cheques drawn on organizations and/or persons abroad that do not have any bank account with our Bank or are not known by our branches shall not accepted by the Bank for collection. The service of cashing foreign exchange cheques can be rendered only to persons or firms having solid commercial past and credibility, whose physical assets and business volume are in correlation with amounts of the cheques, and whose business ethics and commercial practices are known in detail.

2.5.3.4. Virtual Customers (Internet, Call Center and ATM Customers)

Customers wishing to benefit from Internet Branch of our Bank must apply to our branches and provide required all information and documents. The customers with missing information and documents shall not be allowed to use our Internet Banking Branch:

a) While deciding about a virtual customer; customer determination procedures for a real (face to face interviewed customer) must be followed completely.
b) In order to decrease the risk related to this kind of customers, the Bank shall not provide further services to the customers with missing information and documents.

2.5.3.5. Credits Guaranteed By Cash Deposit

Credit applications made against the balances of bank accounts in free zones shall be rejected. Also the Guarantee Letters from the banks in these regions shall not be accepted as collateral.

2.5.3.6. Safe Deposit Boxes

a) Customers owning frequently used safe deposit boxes must be monitored specially by branches.
b) One safe deposit box shall be used maximum by two people.
c) Customers shall not be left alone in safe deposit boxes' area.

2.6. Suspicious Transactions

2.6.1. Description of Suspicious Transactions

The cases where there is a fact, a doubt or any reason leading to suspicion indicating that the money or any assets representing the value subject to transactions done by or done in the name of obligors is earned through illegal ways and means or there has been an attempt in doing so are considered **Suspicious Transactions.** The responsibility of reporting suspicious transactions belongs to all branches, representatives and similar units of Albaraka Turk Participation Bank in Turkey. If there is no information or a reason proving that the money or assets representing the money subject to the transaction in question is owned through legal means by the obligor, or, any reasonable doubt indicating that the income is connected to a crime of any sort, the transaction shall be considered as suspicious and it must be treated as such.

2.6.2. Types of Suspicious Transaction

In reporting of suspicious transactions the "Doubtful Processing Types" document attached to the General Communiqué (Nr. 6) published by MASAK as a guide on 27.09.2008, must be observed.

2.6.3. Detecting and Reporting Suspicious Transactions

Employees of the Bank should pay extreme attention while working with customers;

1. Who demand transactions that visibly have no legal or economic aim,
2. Whose income is not in correlation with and related to his/her business,
3. Who are unwilling to or abstaining from providing information and documents required in the context of legal obligations,

4. Who abstain from proceedings required for reporting and record keeping,
5. Who give misleading information or unverifiable data,
6. Who demand credits with no economic logic or without stating the purpose for the credits,
7. Who make transfers of money in large scales and in extraordinary amounts to geographically risky countries and territories,

In case of such transactions "SUSPICIOUS TRANSACTIONS REPORTING FORM (ŞİBF)" must be filled and all related data and documents must be attached to it. Then, form must be submitted to the Compliance Officer after it is signed by the branch manager and the officer that has executed the transaction. ŞİBF tamplate is available on the intranet system of our Bank.

In the process of reporting suspicious transactions, without condisdering whether the subject or the transaction is reported to MASAK by the Compliance Officer, one of the following decisions shall be taken by the senior officer of the Branch/Unit dealing directly with the customer;

a) Continuation of the relationship with the customer,
b) Preservation of the customer relationship through a close examination of its transactions,
c) Terminating the customer relationship by closing the accounts,

2.6.4. Reporting Suspicious Transactions to Public Athorities

Suspicious transactions shall be reported to MASAK via its website maximum within 10 days after the date it was detected. In cases where electronic media (internet) is not viable, ŞİBF form must be faxed to MASAK.

2.6.5. Non-Disclosure and Confidentiality

The information about suspicious transactions shall not be disclosed to related parties and third persons except to the authorities that are legally deemed appropriate to be informed. The information request forms about the subject sent to legal authorities shall be answered by Compliance Officer only, after the necessary investigations are conducted.

2.6.6. Administrative Sanctions Against Violation of Obligations

The fiscal judiciary fines charged on our Bank as a result of any of our staff members for not applying relevant procedures with regard to ID checks and verifications shall be paid by the negligent officer itself. Likewise, the staff members who do not report or repeatedly neglect his/her reporting obligation with regard to the assets acquired illegally or used for illegal purposes or notice any fact, detail, have any doubt or face with anything that may lead him/her to suspicion shall also bear the punitive fines on their own based on their level of involvement in the case (branch managers/branch operation officers etc.).

3. MONITORING AND CONTROL POLICY

3.1. Purpose :

To protect our Bank from risks and constantly inspect and control the compliance of activities of our Bank with the law and the regulations/communiqués drafted regarding prevention of money laundering and funding terrorism, and with the Bank's policies and procedures.

3.2. Monitoring and Control

The following subjects and transactions must be checked based on minimum transaction amount or periods determined by the Compliance Unit periodically:

3.2.1. Risky Customers

1. In respect with information taken while creating customers among PEPs and providing services to them,
2. The transactions made by charity and welfare organizations (voluntary donations and welfare clubs), minimum amount of which will be determined by the Compliance Unit,

shall be monitored, their source, purpose and relevance with the customer profile are determind. The shortcomings detected shall be reported to the related branches/units and their results are must be monitored.

3. About the banks with which we will have correspondent banking transaction;
   a) Their field of activity, prestige and efficiency of their internal and external supervision,
   b) Whether the banks has gone under any investigation, inquisition, prosecution or penalized on charges of money laundering and funding terrorism,

c) Procedures they apply about prevention of money laundering and funding terrorism,
d) Changes in their top managements,
e) Correspondent banks shall be monitored to detect whether any of them has any customers allowed to acces their accounts directly or not. If any of them has such customers, the bank shall be monitored to find out whether it is fulfilling its obligations with regard to giving special attention to such customers or not. Any deficiencies found, must be reported to the related units and the results followed.

4. The transactions related to the custpmers in high risk sectors and bussiness lines identified by the Compliance Unit, their documantation, purpose of transactions and relevance of the stated purpose to customer's main field of activity, the source of the transaction amount must be monitored and any missing information detected must be reported to related branch or unit for appropriate action.

3.2.2. Risky Transactions

a) The system approval shall be taken from branch operators for any cash transaction exceeding the the lower limit determined by the Bank.
b) The system approval shall be taken from branch authorities for electronic fund transfers.

The relevance of the transactions to customer profile, to its purpose, the information and documents about transfer orderer and beneficiary shall be controlled. The shortcomings detected shall be reported to relevant branches/units for taking necessary measures.

c) Regarding personal cheques drawn on banks abroad; The service of cashing foreign exchange cheques can be rendered only to persons or firms having solid commercial past and credibility, whose physical assets and business volume are in correlation with amounts of the cheques, and whose business ethics and commercial practices are known in detail.

The relevance of transactions to the prupose of the ones declared by the customer earlier shall be controlled. The shortcomings detected shall be reported to relevant branches/units for taking necessary measures.

d) The credits with cash blockage guarantee may be allocated to the companies and people that we have detailed information about their trading operations and business ethics. The transactions effected by such customers must be controlled in accordance with the procedures and periods determined by the Compliance Unit.
e) Branches are obliged to monitor the frequent users of safe deposit boxes to find out whether they are involved in any illegal activity or not.

3.2.3. Risky Regions

a) The transactions from the regions described as risky by our System which exceeds the lower limit determined by the Comliance Unit,
b) The transactions chosen by sampling method about the citiziens, companies and financial institutions in the countries which appear in the FATF's list of non-cooperative countries for not applying FATF recommendations or applying them imperfectly,
c) The transactions that are chosen by sampling method about the persons settled in the anti-democratic countries and regions which are situated on illegal drug production-distribution routes and where the rate of crimes such as smuggling and terrorism is high and corruption and bribe is common,
d) The transactions about the people settled in offshore centers, free zones and international finance centers where strict confidential laws are applied on banking practices,

shall be scrutinized; the documents declared, the purpose of the transaction, its connection with the customer's business line, the sources of the amount shall be created while creating a customer relationship with any of these people and the shortcomings detected shall be reported to the concerned branch/unit for appropriate actions. Results of the actions taken must also be controlled.

3.2.4. Complicated and Unusual Transactions

The transactions which are of complicated or unusual nature shall be monitored in accordance with the procedures and periods determined by the Comliance Unit.
A report must be prepared about the shortcomings found in the course of the controls of these types of transactions. The report shall be given to the concerned branches/units for taking necessary actions. Results of the actions taken must also be controlled.

3.2.5. Connected Transactions

The following banking transactions which do not require permenant customer relationship shall be monitored in accordance with the procedures and periods set by the Compliance Unit:

1. Transfer/EFT.
2. Cheques/bills/notes collection.
3. Bill payments.
4. Foreign exchange transactions.
5. Other payments.

Beginning from 01.04.2008, if a customer does the transactions mentioned above and the total amount of these transactions equals or exceeds TL 20,000.00 (or its equivalent in foreign currencies), ID checks and verification must be applied. Whether the checking and verification in this regard is fulfilled or not must be controlled. The discrepancies and shortfalls detected shall be sent to the relevant branches/units for appropriate action and the results shall be monitored.

3.2.6. Virtual Transactions/The Transactions Done Using New Products and Recent Techonological Developments which are Prone to Abuse (Internet, Call Center and ATM transactions)

The transactions of those customers which frequently prefer internet banking or telephone banking instead of using the branch network shall be monitored in accordance with the procedures and periods established by the Compliance Unit.

A report must be prepared about the missing data and documents found in the course of the controls of these types of transactions. The report shall be given to the concerned branches/units for taking necessary actions. Results of the actions taken must also be controlled.

4. TRAINING POLICY

4.1. Purpose :

To ensure compliance with the obligations resulted from State Law, regulations and communiqués regarding prevention of money laundering and funding terrorism and to create a corporate culture by enhancing the sense of responsibility among our staff about the Bank's policy and procedures with a risk-based approache, and, to keep updated.

4.2. In-House Training Programs

Regular training about recognizing laundering transactions and preventing them shall be given to the following personnel under the supervision and coordination of the Compliance Officer:

1. The personnel in managerial positions,
2. The personnel in marketing positions,
3. The operational personnel in contact with the customer

Training programs shall be approved by the Board of Directors. The principles and methods of choosing the content of training programs and the audience (the branches) will be determined by the Compliance Unit. Trainings shall be given within the framework of our Bank's Training Policy, in the form of formal education, in-branch training, seminars and conferences. In addition to these, our staff must be frequently informed about the changes in national and international law, regulations and laundering typologies through our intranet system.

Our staff members are trained about the following subjects:

a) Regulations on laundering proceeds of crime and funding terrorism
b) The Bank's principles, policies and applications about proceeds of crime
c) The identification of the customer, the accuracy and verification of related documents and information
d) International regulations and standarts
e) Recognition and reporting of suspicious transactions
f) Risky sector, regions and transaction types
g) Safeguarding and disclosure obligation
h) Legal and administrative responsibilities

The personnel undergone the training programs will take an exam following the program to asses whether they have reached the required knowledge level or not.

Moreover, the training materials prepared and updated by the Compliance Officer will be available on our intranet system and easily accessable by all personnel of the Bank. All developments, regulations, communications and lists of objectionable persons and organizations about prevention of laundering,

funding terrorism and customer identification will also posted on the intranet and computer automation system where they can easily be accessed by all our personnel.
The statistical results (number of the personnel that have attended the training and the total training hours etc.) of training programs shall be given to the Compliance Officer by our Human Resources Department. The results, then, shall be submitted to MASAK by the Compliance Officer before 15th of March, in the following year with a cover letter.

a) Training programs shall be submitted to Board of Directors for approval in its last meeting of each year.
b) In case of training services which will be procured externally, a request shall be made to Human Resources department after the instructor's and suppliying firm's efficiency is assessed by the Compliance Unit.

4.3. Training Programs Organized by Financial Crimes Investigation Board (MASAK)

The Compliance Unit will organize the training programs that MASAK will offer to the staff members of our Bank. The Bank's officer that will give in-house training for our staff members must have the "instructor" certificate provided by MASAK.

5. AUDIT POLICY

5.1. Internal Audit and Reporting Activities

Inspectors and auditors of Inspection Committee and Internal Control Unit, conduct inspections and examinations with a risk-based approach, through out the year to ensure the Board of Directors that the Compliance Policy is efficient and aqequate, covering the following areas;

1. Bank's policy and procedures,
2. Risk management activities,
3. Monitoring and controlling activities,
4. Training activities;
   a) Whether they are adequate or not
   b) Their efficiency
   c) Whether the transactions are conducted in accordance with Law, regulations and communiqués.

In this context the control points of the Compliance Policy's monitoring/controlling and risk management parts are audited.
The statistical lists prepared jointly by Inspection Committee and Internal Control Unit with regard to inspection and monitoring activities (showing the number of the branches audited, and the number of transactions monitored with the aim of identity verification and detection of suspicious transactions) shall be submitted to the Compliance Officer by 15th of March in the following year.
Then, the lists shall be forwarded to MASAK with a signed cover letter by the Compliance Officer before the end of March.

6. OTHER POINTS

6.1. Safe Keeping and Submitting of Records

The following records shall be kept for at least 10 years:

1. IDs and documents for recognition of customers and transaction profiles (from the closing dates of accounts),
2. The documents and records related to transactions (from the last dates of the transactions)
3. Control and monitoring reports, the lists and documents regarding investigation of the transactions (from their editing date),
4. Reports of suspicious transactions forwarded to Public Authorities and the documents used to prepare such reports (from their editing date),
5. Training documents and attendance lists (from their editing date),
6. Other documents containing legal reports, correspondance and information (from their editing date).

6.2. Obligation of Providing Information and Documents

Staff members of the Bank are obliged to provide any information and documents that may be requested by:

1. The Compliance Officer and Compliance Unit,
2. Members of the Inspection and Internal Control Committees,
3. Staff members of General Management of the Bank,

in writing or verbally. The time elapsed due to related regulations for responding the information requests shall be taken into consideration.