ANTI-MONEY LAUNDERING POLICY STATEMENT

In our country, combating against the laundering crime is being conducted principally by Financial Intelligence Unit , Financial Crimes Investigation Board (FCIB) which carries out within the Ministry of Treasury and Finance.

“The Law No.5549 on Prevention of Laundering Proceeds of Crime” was published in Official Gazette No. 26323 dated 18.10.2006, “The Law No. 6415 on the Prevention of the Financing of Terrorism” was published in Official Gazette No.28561 dated 16.02.2013 and “TheLaw No.7262 on Prevention of the Financing of the Proliferation of Weapons of Mass Destruction” was published in Official Gazette No. 31351 dated 31.12.2020 and several arrangements in this respect have also been made in sub-regulations and international enterprises, agreements and regulations to which our country accedes.

With the regulations published by FCIB, the banks have become obliged to develop a compliance program with the purpose of prevention of laundering proceeds of crime and terrorism financing and enabling the required compliance to the related legal regulations and to set out an institutional policy within the scope of this program by paying attention to the scale of their business, business volumes and the nature of the transactions they conduct.

Fibabanka is stringently focusing on core Compliance functions and KYC&AML&CFT Policies and Procedures. Our AML/CFT Policy, which has been set out within the above mentioned framework, contains the risk management, monitoring and control, training and internal audit policies of Fibabanka A.Ş. within the scope of prevention of laundering proceeds of crime and terrorism financing.

The purpose of the corporate policy is to enable the compliance of our Bank to the obligations related to prevention of laundering proceeds of crime and terrorism financing, to define the strategies, controls and measurements within the own entity of the Bank, operational rules and responsibilities by assessing its customers, transactions and services with a risk-based approach as well as raising the awareness of its employees in this respect.

All transactions, activities and services performed by Fibabanka A.S. branches, head office, overseas subsidiaries and similar affiliated units are covered by the Bank’s anti-money laundering policy. (Transactions of overseas units are subject to such policy to the extent allowed by the legislation and authorized bodies of their country of activity).

Adoption and all amendments made in the policy are subject to the approval of Board of Directors. Efficiency and sufficiency of the policy, including risk management, monitoring and controlling and training activities are subject to annual control of both internal and independent audit.

Fibabanka has adopted an Anti- Money Laundering Compliance Program that fulfills all requirements of Law No. 5549 on Prevention of Laundering Proceeds of Crime, Law No. 6415 on the Prevention of the Financing of Terrorism and Law No. 7262 on Prevention of the Financing of the Proliferation of Mass Destruction Weapons.

This program includes at least the followings;

- Establishing and implementing of policies, procedures and internal controls reasonably designed to achieve compliance with AML/CFT regulations, FATF standards and sanctions enforced by EU, UN, UK and OFAC,
- Assigning a compliance officer responsible for implementing anti-money laundering and counter terrorist financing policies and procedures,
- Monitoring and auditing customer activities and transactions as per AML/CFT legislations and regulations,
- Prohibiting accounts /relationships with shell banks,
- Reporting suspicious transactions,
- Training of employees on AML/CFT,
- An audit and review function to test the efficiency and sufficiency of whole compliance program.

Our AML/CFT Policy/Procedures includes basicly the following subjects:

- Customer Due Diligence (Know Your Customer Principles)
- Risk Management
- Monitoring and Controlling Activities & Suspicious Activity Reporting
- Internal Audit
- Training Program

Customer Due Diligence (Know Your Customer Principles):

Establishing the identification, which is the most important part of identifying the customer, is done according to the rules indicated in the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism, which is published in the Official Gazette dated 09/01/2008 with the number 26751.

During KYC process, besides verifying the identification and address, purpose of account opening, source of wealth, customer's occupation, business activity etc. are the main questions.

Customer identification must be completed;

- Regardless of the amount while establishing permanent business relationship,
- When the amount of a single transaction or the total amount of multiple linked transactions is equal to or more than 185.000.-TL
- Regardless of the amount in cases requiring STR;
- When the amount of a single wire transaction or the total amount of multiple linked wire transactions is equal to or more than 15.000.-TL in wire transfers;
- Regardless of the amount in cases where there is suspicion about the adequacy and the accuracy of previously acquired identification information

The identity of the person, for the benefit of whom the transaction is conducted, shall be identified as well.

While establishing a permanent business relationship with legal entities, identity verification is carried out for those holding 25% or more of the shares of the entity.

Identifying the Ultimate Beneficial Owners (UBOs) is regulated according to the Article 17/A (Identification of Beneficial Owner) of Regulation On Measures Regarding Prevention Of Laundering Proceeds Of Crime And Financing Of Terrorism.

In cases where customer identification can't be completed or the information on the purpose of the business relationship can't be obtained, the business relationship is not established and the requested transaction is not performed. In this context, an anonymous account or account in a fictitious name can not be opened.

All necessary measures are taken not to establish business relationship with the blacklisted people and institutions as per the international financial system as well as other similar international lists (USA, European Union, United Nations etc.) to which our banks have to comply.

We classify our customers in two categories. we decided that, following customer risk in two categories would provide ease of management in terms of risk management and we came to the conclusion that the binary risk rating system is more efficient and appropriate for Fibabanka AS.

Within the scope of risk rating methodology, we consider all risks under general headings such as customer/counter-party risks country/geographic risks and product/service risks.

The client is ranked as high risk by default, if the client;

- is a PEP,
- is a high-risk country citizen,

- is resident outside of Turkey,
- has a profession or core business classified as high risk (such as precious metal dealer, luxury car dealer, casinos and gambling companies, businesses involving the intense use of cash, manufacturers and distributors of arms and other military products and materials, foundations and associations etc.)
- does business with high-risk countries,
- has a shareholder whose nationality is a high-risk country,

In addition, Compliance team can manually rank the clients as high risk by considering other risk indicators such as required products/services, purpose of account openings, nature of use of the accounts and the compatibility of client's financial profile and transactions etc.

In terms of risk management, Compliance Unit can update clients' risk levels from low to high risk according to results of monitoring controls carried out. The risk identification and rating process is a constantly operating process in Fibabanka A.S.

Our customer database is being screened against sanctions lists / PEP lists with integrated Dow Jones data-file. This batch scan is performed on a daily basis.

Documents regarding customer identity information and transactions are kept for a period of 8 years.

Risk Management:

In the Article 11 of the Regulation on Program of Compliance with Obligations of Anti-Money Laundering and Combating the Financing of Terrorism, Risk Management policy is defined and "Obliged parties shall develop a risk management policy within the scope of the institutional risk management policy, by paying attention to the scale of their business, business volumes and the nature of the transactions they conduct" is indicated. The purpose of risk management policy is to enable the definition, grading, monitoring, assessment and mitigation of financial, reputational and operational risks, which our Bank or employees could expose due to such reasons as benefiting of the services presented by our Bank with the purpose of laundering proceeds of crime and financing of terrorism or non-compliance with the Law and regulation and communiques issued as per the Law. Risk management activities are carried out by the compliance officer under the observation, supervision and responsibility of the Board of Directors.

Activities related to risk management shall cover at least:

- Developing risk defining, rating, classifying and assessing methods based on customer risk, service risk and country risk,
- Rating and classifying services, transactions and customers depending on risks,
- Developing proper operational and control rules for ensuring monitoring and controlling risky customers, transactions or services; taking necessary measures for mitigating risks; reporting in a way that warns related units; carrying out the transaction with ratification of senior authorities and controlling it when necessary,
- Questioning retrospectively the coherency and efficiency of risk defining and assessing methods and risk rating and classifying methods depending upon sample events or previous transactions, reassessing and updating them according to achieved results and new conditions,
- Carrying out required development works through pursuing recommendations, principles, standards and guidelines established by national legislation and international organizations related to issues under the scope of risk,
- Reporting risk monitoring and assessing results regularly to the executive board.

Monitoring and Controlling Activities :

The purpose of monitoring and controlling is to protect the Bank against risks and to ongoing monitor and control whether the operations are carried out in accordance with the Law and regulations and communiques issued pursuant to the Law, and the institutional policies and procedures.

Monitoring and controlling activities carried out in the Bank shall at least include the followings;

- Monitoring and controlling the customers and transactions in the high risk group,
- Monitoring and controlling transactions conducted with risky countries,
- Monitoring and controlling complex and unusual transactions,
- Controlling, through sampling method, of whether the transactions exceeding the amount which the Bank will determine according to the risk policy, are consistent with the customer profile,
- Monitoring and controlling linked transactions which, when handled together, exceed the amount requiring customer identification
- Control of customer related information and documents which are required to be kept in electronic environment or in written form and the information required to be placed in wire transfer messages, getting the absent information and documents completed and updating them,
- During the business relationship, ongoing monitoring whether the transaction conducted by the customer is consistent with information regarding business, risk profile and fund resources of the customer,
- Control of the transactions carried out through using systems enabling the performance of non face-to-face transactions,
- Risk based control of services that may become prone to misuse due to newly introduced products and technological developments.

Reporting of Suspicious Transactions:

The definition of suspicious or unusual transaction covers “use of the asset subject to transaction for illegal purposes” in addition to acquirement of it through illegal ways, which demonstrates that it aims essentially to prevent financing of terrorism.

In this scope, cases where there is any information, suspicion or reasonable grounds to suspect that the funds are used for terrorist activities or by terrorist organizations, terrorists or those who finance terrorism, or that the funds are related or linked to terrorist organizations, terrorists or those who finance terrorism, shall be subject to suspicious transaction reporting.

The Suspicious transactions, determined by the Compliance Department during the monitoring and control activities, are sent to the Financial Crimes Investigation Board (FCIB) by the Compliance Officer after the necessary investigation has been conducted.

It is compulsory to report Suspicious Transactions to FCIB in 10 working days time after the suspicion occurred. When new information or findings are acquired about a previously reported transaction, a new Suspicious Transaction Reporting Form is filled in and sent to the FCIB stating that the new report is an addition to the previously reported transaction.

Those who report suspicious or unusual transactions and other bank personnel, who are informed of the transaction, shall not reveal the reporting to anyone other than auditors who are in charge of audit of obligations and courts in course of a trial. Internal reports are also confidential. Attention and care at the utmost level which is required as per the legislation is paid to the issues related to the confidentiality and security of the suspicious transaction reporting and internal reporting performed in the Bank within this scope as well as the protection of the parties of such reporting.

Internal Audit:

The purpose of internal audit is to ensure confidence to executive board regarding efficiency and sufficiency of whole compliance program.

Audit for the purpose of AML-KYC is performed by the Internal Audit in our Bank. Audits are performed on a yearly basis with a risk based approach covering the subjects of risk management of policies and procedures, whether monitoring&control and training activities are sufficient or not, sufficiency and effectiveness of the Bank's risk policies, if the transactions are being conducted in compliance with the related Law and Regulations and to the policies and procedures of the Bank.

The deficiencies determined during surveillance and controls, along with risky customers, services and transactions are included in the audit.

Deficiencies, mistakes and misconducts detected at the end of the audit as well as opinions and suggestions in order to prevent them from occuring again, will be reported to the executive board.

The statistics containing information regarding the annual business volume of obliged party, total number of staff and total number of branch office, agency and similar affiliated units, the number of branch office, agency and similar units which were audited, the dates of audits carried out within these units, total audit period, the number of staff employed during audits and the number of transactions audited shall be reported to FCIB by compliance officer until the end of March of following year.

Training:

The purpose of training policy is ensuring compliance with obligations imposed by Law and the regulation and communiques issued in accordance with Law, creating an institution culture by increasing the sense of responsibility of staff on policy and procedures of institution and on risk-based approach and updating of staff information.

The training activities shall be carried out under the supervision and coordination of compliance officer. The obliged parties shall conduct their training activities within an annual training program including the subjects determined in article 23 of the Regulation.

The obliged parties shall benefit from training methods such as organization of seminars and panels, constitution of working groups, use of visual and audial materials in training activities, computer-aided training programs working through internet, intranet or extranet etc

The trainings to be given to staff by the Bank shall at least cover the following subjects;

- Laundering proceeds of crime end terrorist financing,
- The stages, methods of laundering proceeds of crime and case studies on this subject,
- Legislation regarding prevention of laundering proceeds of crime and terrorist financing,
- Risk areas,
- Institutional policy and procedures,
- In the framework of Law and related legislation;
    - ✓ Principles relating to customer identification,
    - ✓ Principles relating to suspicious transaction reporting,
    - ✓ Obligation of retaining and submitting,
    - ✓ Obligation of providing information and documents,
    - ✓ Sanctions to be implemented in violation of obligations,
- The international regulations on combating laundering and terrorist financing

Regarding the training activities within the year; Information and statistics related to training dates, area or cities the training is given, training method, total training hours, number of personnel to be trained and its ratio against the total number of personnel, breakdown of personnel to be trained according to their departments and titles, contents of the training, titles and expertise areas of the trainers shall be reported to FCIB by compliance officer until the end of March of following year.

In addition to the above, please be informed that you can find US Patriot Certification, Wolfsberg Questionnaire on our web site as well.

Compliance | Fibabanka

If you have any further questions, please do not hesitate to contact the following:

E-mail: compliance@fibabanka.com.tr

Thanks and Regards,

Compliance Unit