ANTI-MONEY LAUNDERING POLICY STATEMENT – 2020

In a global market place, the attempt to use financial institutions to launder Money and for Terrorist financing is a significant problem that has caused great concern in the international community and has resulted in the passage of stricter laws and increased penalties for money laundering.

In order to combat developing methods of money laundering and potential terrorist financing, many countries around the World are strengthening their laws and regulations regarding this subject.

In addition to international enterprises and regulations developed with the purpose of preventing the utilization of the financial system in money laundering and terrorism financing, various legal regulations in this respect have being developed in our country and great importance has been attached to strengthening the current implementations.

Within this framework, "the Law No.5549 on Prevention of Laundering Proceeds of Crime" was published in Official Gazette No. 26323 dated 18.10.2006, and "the Law No. 6415 on the Prevention of the Financing of Terrorism" was published in Official Gazette No.28561 dated 16.02.2013 and several arrangements in this respect have also been made in sub-regulations and international enterprises, agreements and regulations to which our country accedes.

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.

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.

Keeping in view the Global menace of Money Laundering and Terrorist Financing, Anadolubank 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 Anadolubank 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 Anadolubank A.S. branches, head office, overseas subsidiaries and similar affiliated units are covered by Anadolubank A.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 this 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.

Anadolubank A.S. policy includes 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 20.000.-TL
- Regardless of the amount in cases requiring STR;
- When the amount of a single transaction or the total amount of multiple linked transactions is equal to or more than 2.000.-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 done 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 etc.) to which our banks have to comply.

We classify our customers as normal customers, high risk customers and the ones with whom we will not conduct any business relationship.

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

Risk management activities cover the below given points at minimum level:

- To develop risk defining, grading, classifying and assessing methods on the basis of customer risk, service risk and country risk,
- Grading and classifying services, transactions and customers as per the risks,
- To enable the monitoring and controlling of risky customers, transactions or services; reporting them in a way to warn the related departments, developing the required operation and control rules to perform the transaction with the approval of its high authority and to enable the auditing when it is deemed necessary,
- Retrospective assessment of coherence and efficiency of risk defining and assessment methods, risk grading and classifying methods through case samples or performed transactions; reassessment and updating as per the results concluded and developing conditions,
- Following up the national legislation and recommendation, principle, standard and guidelines on the issues falling into the scope of risk introduced by the international institutions and conducting the required improving studies,
- Periodic reporting of risk monitoring and assessment results to the Board of Directors.

As a result of risk rating activities, additional measures are implemented in order to reduce the risks of the groups which are determined as high risk.

Monitoring and Controlling Activities :

The Bank conducts the monitoring and controlling activities by paying attention to the nature of the transactions performed by its customers.

The purpose of monitoring and controlling is to protect the Bank against the risk and continuously monitor and control whether or not the Bank activities are being conducted in line with the Law, regulation and communiques, internal policy and procedures.

In this scope, main monitor and control activities conducted in the Bank within the scope of prevention of laundering proceeds of crime and terrorism financing are given below:

- Customers and transactions in high risk groups are monitored and checked.
- Transactions conducted with risky countries are monitored and checked.
- During the term of business relationship, continuous monitoring of the fact that whether the transactions conducted by the customer are consistent with information of the customer's job, risk profile and fund resources
- Complex and unusual transactions are monitored and checked.
- Transactions exceeding the amounts determined separately for real and legal entities within a certain period are monitored and checked.
- Amounts that need identity verification when considered as a whole are monitored and checked.
- Control and completing the missing parts of the documents and information on the customer which are required to be kept as a soft copy or hard copy and updating thereof are ensured.
- The information in the Electronic Fund Transfer messages is checked, if found missing, it is completed and updated.
- Control of the transactions, which have been performed by using the non face-to-face systems such as internet and ATM
- Cash activities over the pre- determined threshold values are monitored and checked.
- News related to Money Laundering and Terrorism Financing which is reflected to the media is followed up and they are examined whether they pose a risk against our Bank or not. If negative news about our customers are determined, it is ensured to perform the suspicious transaction reporting, stop the transactions in necessary cases or terminate the business relationship with the customer.

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.

Our branches and/or departments cannot abstain from submitting any kind of information or document on time which is requested by the Compliance Officer for the sake of transactions reported or to be reported.

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:

Efficiency and sufficiency of the entire compliance program constituted by the Bank is audited by the Bank's Internal Audit Departments with the purpose of providing assurance to the Board of Directors.

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 representative member/members of the Board of Directors.

Within the scope of internal audit activities, statistical information containing annual transaction volume of the Bank, total number of personnel and number of branches, number of audited branches, dates of audits, total audit period, information on the personnel working in the audit and the number of audited transactions will be reported to FCIB by the Compliance Officer until the end of March every year.

Besides the internal audit, external audit is done annually. KPMG is the external auditor for the year 2019.

Also regulatory examination(s) are being done by FCIB and BRSA (Banking Regulation and Supervision Agency) annually.

Training:

The purpose of the training policy is to enable the compliance to the obligations imposed by the Law and regulations and communiques published on the basis of the Law, to constitute a corporate culture by increasing the responsibility awareness of the personnel about corporate policy and procedures and issues with a risk-based approach and to ensure the information updating of the personnel.

Training text regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism is prepared by the Compliance Officer. This text will be prepared to at least cover the subjects of;

- Concept of laundering crime proceeds and financing of terrorism,
- Stages and methods of laundering and examples of case studies,
- Regulations regarding prevention of laundering crime proceeds and financing of terrorism,
- Risk areas
- Institutional Policy and Procedures,
- Principles on identifying the customer, principles related to notification/reporting of suspicious transactions, Obligation of retaining and submitting,
- Obligation of providing information and documentation, possible 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 will be 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 will be advised to FCIB until the end of the month of March of the following year.

Training is given via the intranet for the existing and newly recruited personnel. In group recruitments face to face training can be given by either the Compliance Officer or an expert trainer.

If necessary, face-to-face meetings can also be organized by gathering the personnel in one place by the Compliance Officer and the Training Department's joint decision.

Training given through the Intranet is repeated at least once in two years' period. The personnel are tested on the subjects at the end of the training. Policies and training methods may be reevaluated depending on the test results.

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

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

E-mail: compliance@anadolubank.com.tr

Thanks and Regards,
AML Unit
Compliance Department