POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

Introduction and Scope

QNB Bank A.Ş. (hereinafter referred to as "the Bank") is aware of the need of adopting and applying effective measures for anti-money laundering, counter financing of terrorism (AML/CFT) and combating proliferation financing of weapons of mass destruction (CPF) for new and existing customers.

To achieve this aim, the Bank, its subsidiaries, affiliates, and foreign branches adopt the Policy on Anti-Money Laundering and Counter Financing of Terrorism (hereinafter referred to as "the Policy") which includes new customer acceptance policy, is prepared according to Group Compliance Policy on Anti-Money Laundering and Counter Financing of Terrorism and sets principles and rules to protect the Bank from potential money laundering, financing of terrorism and proliferation financing of weapons of mass destruction risks related to its products and services.

The regulatory and supervisory agency that is authorized regarding AML/CFT/CPF is MASAK (Financial Crimes Investigation Board) organized under Ministry of Treasury and Finance. General principles required to be complied with in this regard and risks and penalties in case of violation of such obligations and strategies of struggle are set out in the laws in effects and related regulations, communiqués and guidelines. Main legislations are listed below;

Laws:

- Law no. 5549 on Prevention of Laundering Proceeds of Crime
- Law no. 6415 on the Prevention of the Financing of Terrorism
- Law no. 7262 on the Prevention of the Financing of Proliferation of Weapons of Mass Destruction
- Article 282 of the Turkish Criminal Law No.5237

Regulations:

- Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism
- Regulation on Program of Compliance with Obligations of Anti-Money Laundering and Combating the Financing of Terrorism
- Regulation on Postponement of Transactions Within the Scope of Prevention of Laundering Proceeds of Crime and Financing of Terrorism
- Regulation on the Procedures and Principles Regarding the Implementation of Law on the Prevention of the Financing of Terrorism
- Regulation on the Procedures and Principles Regarding the Implementation of the Law on the Prevention of the Proliferation Financing of Proliferation of Weapons of Mass Destruction

In addition to the local legislation, the Bank adopts recommendations, guidelines and standards published by international regulatory authorities and institutions listed below;

- Recommendations and Implementation Methodologies of FATF (Financial Action Task Force)
- Basel Principles (Know Your Customer Principles for Banks)
- EU Directives
- UN Security Council Resolutions
- Wolfsberg Principles.

This Policy covers risk identification, assessment, monitoring and mitigation activities for the risks of violation, failure to implement and avoidance of asset freezing decisions within the

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

scope of Law No 6415 on the Prevention of Financing of Terrorism and Law No 7262 on the Prevention of Financing the Proliferation of Weapons of Mass Destruction, and advanced controls for the implementation of such sanctions.

The Bank will carry out assessments of the adequacy and effectiveness of current AML/CFT policy on an annual basis at least or whenever necessary. This Policy was prepared in accordance with the national and international legislations, obligations of QNB Group and Group Compliance Policy regarding AML/CFT/CPF. In case of any noncompliance, enhanced measures will apply.

Purpose

The purpose of this Policy is to establish processes regarding AML/CFT/CPF in order to:

- Prevent the Bank's products and services from being used for money laundering, financing of terrorism and proliferation financing of weapons of mass destruction and other illegal transactions,
- Ensure compliance with applicable laws and regulations, avoid administrative fines and legal sanctions that may be imposed on the Bank and ensure, enhance and protect the credibility, integrity and reputation of the Bank,
- Adopt a risk-based approach and ensure that appropriate strategies are prepared to minimize the risks that may be encountered by the Bank,
- Provide guidance to the senior management as well as relevant division managers and employees,
- Ensure that the Bank employees are aware of the rules governing money laundering, terrorism and proliferation financing of weapons of mass destruction and to raise awareness and take responsibility for complying with them.

Responsibilities

Financial Crime Compliance Division is responsible for implementing, developing and reviewing this Policy approved by the BoD and the BoD is ultimately responsible for ensuring the fulfillment of the obligations to which the Bank is subject within the scope of the relevant laws and regulations.

AML/CFT/CPF are the main responsibility of all business units and employees of the Bank.

All employees and executives of the Bank are obliged to comply with this Policy. It is obligatory for managers and employees of the Bank to be aware of and appropriately act with this Policy and relevant procedures to protect the Bank against activities of money laundering, financing of terrorism and proliferation financing of weapons of mass destruction.

All employees of the Bank are obliged to assist in identifying activities related to money laundering, financing of terrorism and proliferation financing of weapons of mass destruction. Therefore, the employees of the Bank shall be aware of the fact that a deficiency in implementing the procedures regarding AML/CFT/CPF may be evaluated as gross negligence and result in disciplinary proceedings.

Appointment of Compliance Officer and Assistant Compliance Officer

The Board of Directors (BoD) assigns through the Audit Committee a Compliance Officer and Assistant Compliance Officer to be responsible for managing the risks of money laundering

and financing of terrorism and proliferation financing of weapons of mass destruction with a robust risk-based framework. Compliance Officer reports to the BoD via Audit Committee.

Compliance Officer and Assistant Compliance Officer shall have sufficient seniority, knowledge and authorization to fulfill their responsibilities independently.

Responsibilities of Compliance Officer

The Compliance Officer is responsible for conducting money laundering, financing of terrorism and proliferation financing of weapons of mass destruction risk assessments, implementing AML/CFT framework, reporting suspicious activities, implementing relevant policies and instructions in line with relevant local laws, QNB Group Policies and regulations and recommendations of the FATF and the Basel Committee.

Responsibilities of Branch Managers/Division Managers

Branch Managers/Division Managers are responsible at first level for duly implementing this Policy in their branches and divisions. They shall ensure that their employees examine and adopt this Policy text and that the procedures related to KYC (Know Your Customer) are correctly implemented.

Financial Group Intragroup Information Sharing

Within the scope of Group Compliance Policy on AML/CFT, information can be shared within the Financial Group for customer identification as well as accounts and transactions. Confidentiality provisions written in private laws shall not be applied in intragroup information sharing.

The Bank shares information according to the policy covering information sharing at Financial Group level.

Risk Management Activities

With the National Risk Assessment, the Bank shall ensure that the risks related to money laundering, financing of terrorism and proliferation financing of weapons of mass destruction are defined, taken into account, understood, evaluated, documented, monitored and updated on a regular basis according to the risks of money laundering, financing of terrorism and proliferation financing of weapons of mass destruction. In addition, before launch of the new product, new business practices or new technological products, the risks that may arise from them or the risks identified at the national level shall be taken into account.

The Bank defines the risks that will arise from its customers and the services. The Bank establishes processes to monitor and control risky customers, transactions or services.

The Bank evaluates alarms regarding risky transactions generated by scenarios to be defined in software products by using them to identify risky transactions. The Bank ensures that relevant units are informed to take necessary measures to minimize the risks identified as a result of such engagements.

Risk management activities are continuously reviewed according to changing and developing conditions.

Necessary improvement engagements are performed by following up recommendations, principles, standards, and guidelines introduced by local regulations and international organizations.

Enhanced measures are applied for high-risk customers and transactions.

Risk management, monitoring and assessment results are regularly reported to the BoD via Audit Committee.

Risk-Based Approach and Customer Risk Classification Methodology

Risk-based approach shall be implemented to classify the customers into risk profiles.

The Bank uses a risk assessment methodology that is appropriate for the size of the Bank, business profile and risk profile to minimize the risk of money laundering, financing of terrorism and proliferation financing of weapons of mass destruction.

In risk-based approach, customers are classified according to risk profiles which are based on following components:

- Customer Risk – identifying source of income or transaction types,
- Geographic Risk – involvement of customers with regions associated with money laundering and financing of terrorism or other illegal activities,
- Product Risk – specific products and service types,
- Distribution Channel Risk – how the service is provided

KYC methodology is applied within the scope of relevant risk components based on customer risk classification.

High-risk customers are subject to continuous monitoring regardless of their risk scores.

A separate process is carried out for certain high-risk customers such as Politically Exposed Persons (PEP) and Non-Profit Organizations (NPO) in risk-based approach.

Customer Acceptance

Having sufficient information about KYC and using such information effectively is the basis of all other processes related to AML/CFT/CPF. This helps in prevention of fraud attempts and detection of suspicious transactions and protects the Bank from financial and reputation risks.

Within the scope of KYC principles, business units and branches which establish business relationships with customers are responsible for ensuring that ID authentication and verification of customers and persons acting on behalf of the customers are carried out over documents and data obtained from independent sources, that necessary controls are implemented and measures are taken to identify the ultimate beneficial owners of transactions and that obtain information regarding the purpose and nature of the business relationship.

Ultimate Beneficial Owner is defined legally as real person or persons who controls the real persons making transaction and/or real person, legal person or unincorporated organizations on behalf of which transaction is made or who have authority on them.

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

In establishing a permanent business relationship, the ultimate beneficial owner is identified with a risk-based approach.

ID authentication and verification of real persons who have 25% or more control or ownership shall also be made.

It is also important to have information about financial situation and income/asset sources of customers. Additional information shall be obtained from high-risk customers, including information about the source of their assets.

Potential customers shall be subject to risk assessment and a risk profile shall be created. Transactions and activities to be made in the future shall be evaluated according to this profile.

Information and documents required to be obtained within the scope of risk assessment and KYC shall be kept up-to-date.

The Bank regularly controls whether their customers are included in any international sanctions lists issued by UN, EU, UK, OFAC and other regulatory institutions.

Within the scope of this Policy, the Compliance Officer of the Bank and Financial Crime Compliance Division reporting the Compliance Officer are responsible for establishing a business flow regarding KYC principles to implement customer acceptance policy. Customer acceptance and whether to continue business relationship shall be determined within the scope of KYC principles.

Within the scope of this Policy, the Bank shall open accounts for their natural and legal customers that comply with the Bank's targets and objectives.

Such customers shall be eager to continue the business relationship in line with relevant rules and shall have reasonable information and awareness about banking activities, products and tariffs. The senior management may establish other specific instructions about these criteria as it may vary in time.

The Bank shall not provide banking service to natural and legal persons whose ID authentication is not performed in an adequate manner.

The Bank shall not form business relationships with natural and legal persons who do not comply with the Bank Policy which is in line with Group Compliance Policy and/or other relevant local/international regulations. The Bank shall be careful and attentive in customer acceptance and permanent business relationships with high-risk persons and organizations, including but not limited to PEPs and NPOs.

According to this policy, it is forbidden to open anonymous accounts, deal with anonymous customers and shell banks or open accounts in fictitious names.

All existing and new customers shall be checked to determine whether they are included in local and international sanctions lists.

Simplified KYC Principles

Simplified KYC principles are basic customer due diligence, which is applied when the probability of money laundering, financing of terrorism and proliferation financing of weapons of mass destruction risk may be very low, or where the customer's risk category is low.

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

Enhanced KYC Principles

High risk customers are subject to enhanced KYC principles and continuous monitoring.

Such activities shall be generally carried out for following customer categories:

- Transactions that are not performed face-to-face and new technologies,
- Politically Exposed Persons (PEPs),
- Correspondent banking relationships and financial institutions operating in high-risk regions,
- Non-Profit Organizations, Charities (clubs, societies, foundations etc.)
- Regional risks (regions that are not internationally collaborative enough, that do not cooperate or are subject to sanctions as per FATF or that have a tendency for corruption),
- Customers who do not reside in Turkey,
- Complex legal entities, legal arrangements& facilities,
- High net-worth individuals within private banking services,
- Dealers in precious metals and stones,
- Real estate agents,
- Special purpose vehicles (SPVs),
- Lawyers, notaries and other independent legal professionals and accountants,
- Trust and company service providers,
- Other high-risk customers as per customer risk assessment methodology.

Prior to opening accounts for PEPs, the approval of the Senior Management shall be obtained through the Financial Crime Compliance Division.

Business relationships shall not be continued with PEPs or persons who have a connection with them, unless the approval of the Senior Management is obtained.

Situations Requiring Customer Due Diligence

Customer Due Diligence shall be applied as a general principle when establishing business relationship with new customers. In case of the following conditions, initially obtained customer information of customers with completed due diligence shall be reviewed and updated, customer shall be re-visited or re-evaluated (including but not limited to them);

- Change of ultimate beneficial owner or authorized signatory of the existing business relationship and/or accounts,
- Realization of an important (unusual) transaction,
- Transactions with values larger than the threshold values specified in the customer acceptance process,
- Significant changes in implementation of the business relationship or the operation of the customer account,
- Significant changes in customer documents,
- Suspicious about the accuracy or adequacy of the information and documents previously obtained within the scope of KYC,
- Electronic transfers above the specified threshold values,
- Suspicion about money laundering, financing of terrorism and proliferation financing of weapons of mass destruction regardless of the transaction amount,
- Procurement of a new product or service.

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

Updating KYC Information

Information and documents of existing customers obtained within the scope of KYC shall be regularly reviewed and updated. The update period shall be applied as follows according to the risk levels of the customers within the scope of money laundering, financing of terrorism and proliferation financing of weapons of mass destruction;

- Once a year in high-risk customers,
- Once in three years in medium-level customers,
- Once in five years in low-level customers.

Monitoring and Control Activities

The Bank integrated some programs into its system to check whether existing or new customers are included in international sanctions lists in accordance with legal regulations. It benefits from these programs manually and automatically to identity suspicious customers and transactions and to prevent risks of money laundering, financing of terrorism and proliferation financing of weapons of mass destruction.

Measures are taken to continuously monitor customers and transactions, taking into account asset freezing decisions and potential matching criteria. In this context, the sender and recipient information in electronic transfer messages are also taken into consideration.

It installs necessary systems and carries out effective processes for continuous monitoring of accounts and transactions with the aim of detecting, monitoring and evaluating high risk customers and transactions.

Any deficiencies detected upon such controls are reported to relevant business units so that necessary measures are taken and results are followed up.

Employees responsible for carrying out these activities are given access to internal information sources and systems within the scope of monitoring and control.

These systems shall be accessed by the employees in Financial Crime Compliance Division, relevant divisions and branches.

The Bank may terminate their business relationships with customers they deem to bear suspicion in terms of being included in international sanctions lists. The Bank's AML/CFT Committee decides whether the business relationship is to be terminated and deter mines how the customers are to be notified about this issue.

Obligation to Report Suspicious Transactions

All employees are made aware via training and briefings that they are personally obliged to report any suspicious activity or knowledge within the scope of AML/CFT and proliferation financing of weapons of mass destruction and that failure to fulfill this obligation will have penal consequences.

Employees in the Bank shall report suspicious transactions via the related special line in intranet system of the Bank to Compliance Officer/Assistant Compliance Officer. The Compliance Officer and Assistant Compliance Officer review the suspicious transaction notifications and report to MASAK when necessary.

No information is shared about suspicious transaction notifications at Financial Group level.

All employees are prohibited from sharing confidential information within the scope of the relevant Law. In case of violation of these regulations, legal penalties are imposed and disciplinary measures are applied.

Training Activities

Continuous education and training of employees at all levels is an essential component of an effective compliance program.

Training activities are conducted under the supervision and control of the Compliance Officer. These activities shall be reviewed by relevant business units based on evaluation and measurement results and they shall be repeated regularly and upon requirement.

The Bank carries out training activities by organizing seminars and panels, establishing working groups, using audio-visual materials and providing computer aided training programs. All employees are included in the scope of such training programs (except drivers, executive and platform assistants, technical personnel, security guard, etc.).

Trainings cover the following issues;

- Concepts of money laundering, financing of terrorism and proliferation financing of weapons of mass destruction,
- Money laundering stages, methods and case studies,
- Legislation regarding AML/CFT/CPF,
- Risk areas,
- Corporate policies and procedures,
- Know Your Customer principles,
- Principles related to suspicious transaction reporting,
- Obligation of keeping and submitting,
- Obligation of providing documents and information,
- Penal sanctions to be imposed in case of failure to fulfill obligations,
- International regulations on AML/CFT.

Record Keeping

Within the scope of the laws on AML/CFT and proliferation financing of weapons of mass destruction, the Bank and the companies of the Group are obliged to keep for eight years the documents related to the customer accounts and transactions regarding the obligations in the relevant Laws and transactions from the date of issuance; books and records from the last registration date; and ID authentication documents from the last transaction date and to present it to the authorities if requested.

The Bank shall keep the records related to customer accounts and transactions for at least 10 years pursuant to the Banking Law and relevant regulations.

Sanctions Policy

Complying with the sanction decisions of UN, EU, UK and the Office of Foreign Assets Control (OFAC) of the US Department of the Treasury applicable for any business or transaction under all conditions and operating in accordance with best practice guidelines issued by regulatory

institutions are a separate policy of the Bank. Thus, Financial Crime Compliance Division is responsible for preparing the necessary procedures, guidelines and mechanisms to comply with such regulations and to prevent any violation that may result in sanctions.

Audit

Internal Audit Department carries out audits to evaluate adequacy and effectiveness of measures taken by the Bank to assess, monitor and manage the risks of money laundering, financing of terrorism and proliferation financing of weapons of mass destruction.