GUIDELINES ON QNB FİNANSBAK INTERNAL ANTI-MONEY LAUNDERING AND COUNTER TERRORIST FINANCING POLICIES

2018

1 Status and Role of Compliance

1.1 Introduction

Compliance Division is an independent function, with a formal status within the Bank that identifies, assesses, advises on, monitors and reports on the Bank's compliance risk, that is the risk of legal or regulatory sanctions, financial loss, or loss to reputation the bank may suffer as a result of failure to comply with applicable laws, regulations, codes of Ethics & Conduct and standards of good practice, which are principally relevant to the business activities of the Bank. These regulations cover local law and regulations, as well as regulatory requirement of every country in which the Bank operates. These regulations inter alia include the regulatory requirements dealing with the prevention of money laundering and terrorist financing.

1.2 Authority

In order for the Compliance Division to carry out its role and responsibilities in most effective and efficient manner, it is empowered to cover the regulatory compliance and AML/CTF issues of the Bank's activities and has been given unrestricted access at any time to information, records, personnel, property and operations. In addition, it has been given the right to conduct investigations for suspicious cases.

1.3 Roles and Responsibilities

The responsibilities of the Compliance Division regarding AML/CTF will be carried out under an AML/CTF program, which sets the Division's planned activities. Such plan will be reviewed by the Compliance Officer, approved by the Audit Committee and executed according to the AML/CTF framework and procedures manual. The responsibilities of the Compliance Division with regards to AML/CTF include the following:

- Establish an Annual Plan for undertaking AML/CTF activities.
- Implement a risk-based AML/CTF Program that governs the Compliance activities and embedding regulatory requirements, internal policies and procedures, and international guidelines and standards.
- Implement appropriate and up-to date policies and procedures regarding AML and CTF giving consideration to the FATF and Basel Committee recommendations, in addition to applicable regulatory requirements.
- Monitor the level of compliance to the AML and CTF regulations and policies by performing regular and comprehensive review and testing of the Bank's activities.
- Ensure that a proper and adequate Know Your Customer (KYC) Policy is in place and perform regular testing to ensure complete compliance.

- Develop and maintain a Sanctions Policy to ensure abidance with international and local sanctions regimes.
- Ensure that adequate customer profiling and on-going monitoring processes are implemented and effective.
- Undertake studies, analysis and research aiming to the enhancement of the AML/CTF framework of systems and controls.
- Act as focal point for the investigation of suspicious reports.
- Report on a regular basis to the Audit Committee and Senior Management on compliance of the bank with regulatory requirements and QNB policies and procedures regarding AML/CTF.
- Establish methods and means for spreading the AML/CTF Awareness through training, e-learning and other appropriate mediums.

2 Compliance Policy

The Compliance Policy is intended to set the bar in terms of regulatory compliance requirements, including AML./CTF, and inform QNB Finansbank stakeholders about their responsibilities and about the role of the Compliance Division. The Policy also intends to satisfy the regulatory authorities that QNB Finansbank is adhering to the applicable regulations. As per the Policy, Compliance starts at the top and concerns everyone within the Bank.

In summary, the policy tackles the following principles related to AML/CTF:

- QNB Finansbank is committed to the preservation of its reputation and integrity through the compliance with applicable laws, regulations and ethical standards in each of the markets and jurisdictions where it operates. All employees are expected to adhere to these laws, regulations and ethical standards. Compliance is therefore considered as an essential component of a solid Corporate Governance framework.
- The Board of Directors, through the Audit Committee (AC), oversees the implementation of the Compliance Policy, including ensuring that compliance issues are resolved effectively and expeditiously by Executive Management with the assistance of the compliance function.
- The AC ensures that an effective mechanism for control, monitoring and reporting on AML/CTF measures and related issues is implemented across the Bank.
- Executive Management is responsible for effective management of the compliance risk and for communicating the relevant compliance procedures to all management members for consideration and implementation.
- Compliance Officer has a direct reporting line to the Audit Committee, which reports to the BOD. Each overseas branch is required to nominate a Compliance Officer.

3 AML/CTF Policy

The purpose of the AML/CTF Policy is to implement programs against money laundering and terrorist financing in order to:

- Protect QNB Finansbank from being exploited as channel for passing illegal transactions arising from money laundering, terrorist financing and any other illicit activities.
- Ensure compliance with applicable laws and regulations and avoid legal penalties and punishments that might be issued and maintain, enhance and protect the credibility, integrity and reputation of QNB Finansbank.
- To minimize risk to QNB Finansbank, and provide guidance to Management as well as all concerned staff on the requirements to be constantly observed.

The elements of the AML/CTF Policy are as follows:

3.1 Risk Based Customer Acceptance Approach

The objective of the risk based approach is to balance the compliance/cost burden with a realistic assessment of the threat of the Bank being used for money laundering or terrorist financing.

The Bank Customers' Customer Due Diligence (CDD) measures shall take into consideration all factors related to the customers, their activities and sources of income, the ultimate beneficial owner(s), the funding mediums, the expected relationship with the Bank, and any other indicators associated with customers' risks according to the degree of relative risk. All elements of the customer relationship should be filtered through sanctions screening processes prior to on-boarding and regularly thereafter. CDD information must then be kept up to date in line with the customer's risk profile and when a major event occurs to enable the Bank to recognise suspicious activity or transactions.

In determining the risk posed by a Customer, the following factors are to be considered in conjunction with each other to provide the basis of the

AML/CTF risk:

- Geographic Risk;
- Entity Risk;
- Industry Risk;
- Political Exposure;

- Product Risk; and
- Distribution Channel Risk.

QNB Finansbank adopted threat assessment methodology to mitigate the risks of ML/TF and assess the risk profile of the business relationship with each customer. The methodology is designed to identify changes in the ML & TF risks, risks posed by new products and services being introduced, and in applying new technologies to services.

The following principles apply to CDD:

- Accounts for natural and legal persons shall be opened according to the applicable laws and regulations.
- Particular consideration should be given when dealing with higher risk customers such as Politically Exposed Persons (PEP), Non-Profit Organizations, and Correspondent Banks.
- Banking services shall not be provided to any natural or legal persons who are not adequately identified.
- It is strictly forbidden to establish anonymous accounts, deal with anonymous customers, shell banks or establish accounts in fictitious names.
- All factors related to the customers, their activities and accounts and any other indicators associated with customer risk should be considered respectively with the degree of risk for each of the customers' categories.
- All new and existing customers shall be screened against blacklists of local and international relevant authorities and hence shall not be listed at any time.
- Non-Face to Face account opening shall be restricted to customers introduced by QNB Finansbank subsidiaries and international branches/representative offices or other financial institutions or intermediaries who are subject to FATF or FATF equivalent customer due diligence measures.

3.2 Product Risks

The AML/CTF Policy addresses specific risks of ML/TF and other illicit activities posed by different types of products offered to QNB Finansbank's customers. These products include:

- Cash Based Services;
- Private Banking;
- Products with Fictitious, False or No Names;

- Correspondent Banking;
- Payable Through Accounts;
- Power of Attorney;
- Bearer Shares and Share Warrants to Bearer;
- Wire Transfers;
- Trade Finance Products (which are further detailed in a separate manual);
- Secured and Unsecured Loans; and
- Financial Transactions Associated with Investment Activities;

3.3 Systems and Controls

The following systems and controls apply to the screening, profiling and on-going monitoring processes:

- Screening

The system integrates international and local sanctions lists, and PEP Lists provided by World-Check, that are automatically updated. Processes are implemented within QNB Finansbank to perform a daily screening of customers and an on-line real-time screening of transactions where a '4 Eyes' structure is implemented. Comprehensive User Manuals are developed to guide users throughout the screening process and investigation rationale.

- World-Check Online

As part of the on-boarding and periodic update processes, the customers and identified linked parties, such as sources of income and related parties, should be screened against World-Check. The screening results should be analyses and retained.

- SAS AML

  SAS acts as a customer risk profiling and on-going monitoring tool. The Risk Profiling module is based on a risk-scoring methodology that incorporates the risk factors detailed in the Banks AML/CTF Policy. The On-Going Monitoring module is scenario-based and mimics suspicious customers' behaviors such as structuring, velocity, layering, change in pattern and unusual transactions.

- Core Banking System

Equation, being QNB Finansbank core banking system, is constantly maintained and upgraded to capture KYC information. The latest additions to the system covered corporate related parties, PEP status, customer risk level, and customer update date.

3.4 Internal and External Suspicion Reports

Based on local and international regulations, all officers and employees of QNB Finansbank have direct access to the Compliance Officer, without any need to follow the reporting hierarchy, to report any suspicion of money laundering or terrorist financing. For the purpose of reporting suspicious transactions, a specific line is established within bank's intranet system.

It is also a regulatory obligation that all QNB Finansbank officers and employees remain vigilant and report any knowledge or suspicion of money laundering or terrorist financing activity, and that failure to do so can result in severe penalties.

The Compliance Division is responsible for investigating the internal STRs and is also accountable towards ensuring the embeddedness of a framework for the effective monitoring of the customers' profiles and transactions. The Compliance Division is liable towards ensuring that a comprehensive investigation is undertaken and documented, based on which a decision is taken to submit an external STR to the regulatory authorities (FIU).

3.5 Tipping-Off

Tipping off is prohibited by regulatory requirements. Therefore, all QNB Finansbank directors, officers and employees shall abide by the Law or otherwise be subjected to legal punishments and disciplinary actions.

3.6 Document Retention

In compliance with Banking Regulation and FATF recommendations, QNB Finansbank shall keep records of its customers' accounts for a period not less than 10 years. These records shall include legal identification documents, correspondence, accounts transactions with supporting documents and any other relevant documentation.

3.7 Training

Continuing education and training of employees at all level is a significant element of an effective Compliance Program and an essential pillar of the Internal Controls structure. Comprehensive training and awareness programs are implemented by QNB Finansbank covering Regulatory Compliance and AML/CTF and communicated to Senior Managers and staff through classroom training, e-training.

4 KYC Policy

4.1 Introduction

QNB Finansbank enforces Know Your Customer (KYC) policies to accept customers whose sources of funds can reasonably be recognized to be legitimate, and that are willing to deal with usual patterns of transactions that have apparent economic or visible lawful purpose, hence reducing the likelihood of QNB Finansbank becoming a vehicle for financial crime and suffering consequential losses and reputation damage.

4.2 KYC Principles

- The Bank will maintain sufficient information on customers, their sources of income, their relationship with QNB Finansbank, and their related parties including Ultimate Beneficial Owners. That information should be properly documented within the Bank's records.
- No funds may be received or any account opened and operated unless or until all KYC information is gathered in line with the internal procedures. If this is not satisfied, the business relationship may not proceed.
- Caution and enhanced diligence must be exerted when dealing with higher risk categories of customers such as walk-in customers, non-resident customers, non-profit organizations, correspondent banks and Politically Exposed Persons.
- Customers should remain under on-going monitoring and suspicious activities should be reported to the Compliance Division in line with the internal procedures.

5 Sanctions Policy

5.1 Objectives of the Policy

The Sanctions Policy intends to achieve the following objectives:

- To protect QNB Finansbank's reputation from being involved or conducting business with or on behalf of sanctioned individuals or entities.
- To prevent QNB Finansbank from incurring financial risks by being subject to penalties linked to breach of applicable sanctions programs.
- To protect customers' money from being held blocked or frozen because of breaches to the international or local sanctions.
- Enhance the integrity of QNB Finansbank in the financial markets, with respect to its shareholders, stakeholders, employees and related parties.

5.2 Policy Statement

QNB Finansbank is committed to adhere to economic sanctions in the jurisdictions in which it operates, including compliance with United Nations (UN), United States (US) and European Union (EU) sanctions regimes, along with any other sanctions program being applicable.

To the extent permitted by local law, QNB Finansbank will take necessary steps to prevent the opening of accounts or the execution of transactions for, on behalf of, or for the benefit of, a sanctioned individual, entity, country or organization in violation of the sanctions regulations in place.

As part of its compliance program, QNB Finansbank shall conduct economic sanctions scanning of both customer and transaction data to ensure that no transactions are concluded with, on behalf of or for the benefit of individuals who are the target of economic sanctions programs.
On a risk-based approach, customer data shall be scanned against relevant economic sanctions lists at the time the account is opened, at the commencement of cross-border relationship, upon receipt/change of customer data, or upon updates to the applicable economic sanctions programs.

5.3 QNB Finansbank Compliance Advisory Helpdesk

The policy has provided the role / responsibility of Compliance Sanctions helpdesk in order to receive and answer all the enquiries raised by the business and or operations for transactions (i.e. wire transfer, foreign trade transaction, etc) that is directly / indirectly connected with sanctioned and / or high-risk countries. The list of such countries are regularly being updated and circulated considering the regular changes and challenges in the related laws, regulations and sanctions programs.

5.4 Training

The policy considered implementing effective arrangements to ensure that:

- Training, appropriate for different groups of staff, is accessible and routinely provided;
- Refresher training is included to ensure that knowledge remains current and up-to-date;
- Staff are tested, as appropriate, to ensure that they have understood the training;
- Reference material containing the firm’s financial sanctions policies and procedures is readily available and simple to understand.