Banco Nacional Ultramarino
大 西 洋 銀 行

PREVENTION OF MONEY LAUNDERING AND COMBATING TERRORISM FINANCING

Customer Acceptance and Maintenance Principles

INTRODUCTION AND SCOPE

In order to comply with laws and regulations issued by Macao Special Administrative Region (Macao S.A.R.) and Guidelines issued by Monetary Authority of Macao (AMCM) [1] and international institutions related to anti-money laundering and countering the financing of terrorism (AML/CFT), such as Financial Action Task Force (FATF) and others, BNU has adopted policies, procedures and IT systems to mitigate the risk of money laundering and the financing of terrorism.

The knowledge of the customer (*KYC - Know Your Customer*) is one of the fundamental pillars in the assessment of the customers' propensity to carry out money laundering (ML) operations and in the consequent classification of his/her risk profile.

This knowledge starts with his/her full identification and may involve the need to look further into the available information if, after its classification, analysis and monitoring, it is found out that the risk is high for BNU to be liable to be used as the vehicle for money laundering and/or financing of terrorism.

OBJECTIVE

Therefore, the Principles for Accepting and Retaining Clients aims to define the requirements and criteria for accepting, maintaining, or refusing client relationships, detailing the different risk categories that can be assigned to them.
By classifying each client's risk profile, the aim is to prevent the abusive use of the financial system in attempts to obtain, conceal, or invest funds originating from criminal or illicit activities.
This document serves as a guiding basis for the set of criteria applicable to accepting, maintaining, or refusing clients and constitutes an essential part of risk management on money laundering and the financing of terrorism.

- Classifies all customers in its database according to the risk factors defined;
- Adjusts the surveillance levels (simplified and enhanced) according to the customer's risk level;
- Defines specific procedures with the purpose of monitoring customers and accounts that may constitute a higher risk from the money laundering and financing of terrorism perspective;
- Carries out the periodical confirmation and update of the customers' data.

CLIENT CATEGORY AND ACCEPTANCE CRITERIA

BNU adopts a risk-based approach in identifying and classifying clients, with the objective of managing and mitigating the risk of money laundering and terrorist financing (ML/TF).

[1] AMCM AML/CFT Guidelines

Hence, a dynamic system of risk classification in terms of money laundering is implemented through the attribution of a risk profile to all BNU customers.

The attribution of a risk profile to BNU customers begins at the time of establishment of the business relationship and their classification may change due to alterations related to the operating pattern of the customer or group of related customers and/or other relevant factors for this reclassification.

CUSTOMERS NOT ACCEPTED

With the purpose of protecting BNU from practices that may put its activity at risk and in order to defend its reputation, the following types of customers, among others, should not be accepted:

a) Individuals or entities listed on Sanctions Lists by United Nations (UN), European Union (EU), Office of Foreign Assets Control (OFAC) or by Macau S.A.R.
b) Individuals or entities who refuse to submit the legally required information or documentation;
c) Individuals or entities on whom there is reliable information indicating they are connected with criminal activities;
d) Individuals or entities who refuse to submit information or documentation regarding the Ultimate Beneficial Owner[2];
e) Shell banks[3] or entities;
f) Payable through accounts;
g) Anonymous accounts, numbered accounts or with fictitious names;
h) Non-licensed Financial Institutions or similar entities;
i) Non-licensed Gaming entities;
j) Corporate customers with bearer shares.
k) Legal persons, who do not carry out banking activities and who carry out activities with virtual assets, which include i) Exchange services between virtual assets and fiat currencies or between one or more virtual assets, ii) Virtual asset transfer services, iii) custody or custody and administration of virtual assets or instruments that allow to control, hold, store or transfer these assets, including private cryptographic keys.

---

[2] «Ultimate beneficial owner» *Beneficiary or Beneficial owner:* refers to: i.The natural person who ultimately owns or controls a customer; and/or ii. The person on whose behalf an account, transaction is being conducted; and/or iii.The person who exercise ultimate effective control over a legal person or arrangement.

a) If the customer is a corporate body:
i) The natural persons who in last instance, own or have the control, direct or indirect, of at least, the equivalent to 10% of the equity capital or the voting rights of the corporate body, that is not a listed company in a regulated market subject to information requirements in accordance with the community legislation or equivalent international standards;
ii) The natural persons who, in any other way, exercise the management control of the corporate body;
b) If the customer is a legal entity of a non-corporate nature, such as a Foundation, or a collective interest center without being a corporate entity, that manage and distribute funds;
i) Natural persons beneficiaries of at least 10% of their assets, when the future beneficiaries were already established;
ii) A category of persons on whose main interest the legal entity or the collective interest center without being a corporate entity was incorporated or exercises its activity, when the future beneficiaries were not established yet;
iii) Natural persons exercising control on at least 10% of the assets of the legal entity or the collective interest center without being a corporate entity

[3] "Shell bank" refers to a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.

l) Activities related to adult entertainment (Red Light Business)[4]
m) Non-regulated charities / NPOs;
n) Activities related to the production and trade of drugs, with the exception of situations related to therapeutic/medicinal purposes duly authorized by the competent authorities.

CUSTOMERS WITH HIGH RISK PROFILE FOR MONEY LAUNDERING

For all customers with a high money laundering risk profile, BNU has defined a set of monitoring and control procedures in order to comply with the legal obligation of enhanced surveillance and the consequent monitoring of all accounts in which they are involved.

The following types of customers are automatically classified as high money laundering risk:

- Individuals or legal entities whose scoring application classifies them as such, considering their risk in terms of ML/TF;
- Correspondent banks, whose establishment of the business relationship is subject to a risk rating process that aims to assess the risks inherent to the jurisdiction where they are headquartered, corporate structure, business developed and the existence of possible negative references within the scope of ML/TF;
- Politically Exposed Persons (PEPs), whose acceptance of the establishment or maintenance of a business relationship requires intervention from higher hierarchical levels. The same applies to "close family members" and "persons known to be closely associated" (RCA) with PEPs;
- Customers who are nationals of a third country includes the country of residence, Nationality and Country of Birth.
- Customers with occupation or business activity considered to be high risk for ML/TF;
- Corporate Customers, associated with PEP, as Shareholders, Directors & Authorized Signers;
- Customers under the management segment Private Banking;
- NPO with business activity considered to be high risk for ML/TF and / or associated with PEP, as Shareholders, Directors & Authorized Signers;

On a case-by-case basis, the following clients may also be subject to classification as having a high money laundering risk profile:

- Individuals or legal entities resident in countries or jurisdictions subject to sanctions, embargoes or other restrictive measures;
- Individuals or legal entities involved in the production or distribution of weapons and similar products;

[4] Activities linked to the crime of pimping (prostitution)

- Individuals or legal entities resident or operating in areas of higher geographic risk, in particular those that do not have effective AML/CFT systems, show a higher level of corruption or other criminal activities;
- Individuals resident in countries considered by the FAFT lists as non-cooperative;
- Individuals or legal entities whose activity is inconsistent with the knowledge that is available about them;
- Individuals or legal entities involved in activities likely to involve a higher risk of ML/TF, such as casinos, betting entities, payment institutions, and currency exchange bureaus and other similar entities, even if duly authorized;
- Customers with activities that involve intensive cash transactions;
- Customer ownership or control structures that appear unusual or overly complex, considering the nature of the customer's activity;
- Customers from high-risk countries or territories according to the European Banking Authority guidelines;
- Customers for whom, based on the analysis performed and considering the identified risk factors, enhanced due diligence is considered relevant.

The following categories are automatically classified as high risk through the SAS CDD model:

- Controller of a High Risk business, including Sole Proprietors of high risk business;
- PEP/PEP Related (RCA);
- SIP/SIE;
- Reported customer;
- Confirmed Match in Factiva.

CUSTOMER CATEGORY REVIEW AND BUSINESS RELATIONSHIP MAINTENANCE

The monitoring procedures applied to customers must comply with the risk profile assigned to them and the risk associated with a customer may be aggravated in the face of evidence that justifies it or in line with the legislation and regulations in force.

The reclassification of the risk profile is in line with the relationship that the customer establishes with BNU, taking into account the type and frequency of operations carried out and the respective associated risk and moreover the possible change in the customer's situation with regard to its inclusion or exclusion from the sanctioned or PEP lists.

Within the scope of the exercise of the specific duty of enhanced due diligence and in addition to situations related to customers with a high money laundering risk profile or whose criteria is so determined.

BNU will carry out increased due diligence measures whenever it is deemed necessary for potentially higher risk situations and in situations that determine to proceed with the refusal to establish or the termination of the business relationship.

Under the terms of the legislation and regulations in force[5], BNU may terminate the business relationship if it becomes aware, has doubts or suspects that it is related to the practice of

5 AMCM AML/CFT Guidelines

ML/TF crimes and also refuses or suspends the execution of a certain operation ordered by the account holder or by its representative[6], when the information required under the law, including information on the origin and destination of the funds, is not provided.

KNOW YOUR CUSTOMER (KYC) MEASURES

Knowledge of the customer (*know your customer – KYC*) is one of the fundamental pillars in assessment the customer's appetite for carrying out money laundering operations and the consequent definition of their risk profile. The adoption of effective KYC measures is an essential part of managing the risk of money laundering and terrorist financing and, in this context, BNU:

- Classifies all customers in its database according to their money laundering risk profile;
- Adjusts the levels of surveillance (simplified or reinforced) according to the client's money laundering risk profile;
- Defines specific processes with a view to monitoring customers and accounts that may constitute a higher risk from a money laundering and terrorist financing perspective;
- Perform periodic confirmation of customer data.

In accordance with applicable legislation, BNU takes appropriate and sufficient steps to ensure the timeliness, accuracy and completeness of information regarding customers, representatives and ultimate beneficial owners.

When implementing appropriate KYC measures, BNU proceeds to the detailed identification of each client, to the knowledge of the nature of the economic activities carried out by them and, also, to the necessary diligences for the effective knowledge of the ownership and control structures of legal persons.

Prior to the establishment of a business relationship and during its course, it is mandatory to provide information on all the requirements established in the legislation and regulations in force and the respective proofs, and, during the course of the business relationship, the prioritisation of the updating of information should be defined according to the degree of risk associated with each client by BNU, varying the time intervals in the inverse order of the degree of risk identified.

The implementation of KYC policies and measures thus assumes the essential role of identifying, assessing and monitoring customer risk in terms of AML/CFT, allowing for a more efficient assessment of risks and becoming an important tool to maintain trust, stability and reputation of BNU.

6 It includes the different types of representatives, namely attorneys, representatives with a POA, agents or other forms of representation.