

Policy for Preventing and Combating Money Laundering, the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction

Version 3.1.

Document Development Control

	Coordinator	Role	Signature	Date
Drafting	Elie Coxe	DORG		2025-11-17
Verification	Pamela Van-Dúnem	DORG		2025-11-17
Approval	Cristiana Lavrador	Board of Directors		2025-12-11

Note: The original document is signed by the Board of Directors and archived under the responsibility of the Compliance Department.

Review Timeline

Version	Date	Reason	Observations
1.0	14-01-2019	Initial draft.	Based on the programme for the prevention of money laundering and the financing of terrorism (<i>Programa de Prevenção BC e FT_V.2.0</i>).
2.0	10-09-2020	Update following the publication of Law no. 5/20.	
3.0	2022-09-05	Update of information on Occasional Transactions	
3.1	2025-12-11	Policy Review	Law 11/24 of July 4

Document

Summary	
Documents to Repeal	n/a
Complementary Documents	Manual of Procedures

Table of Contents

1. Introduction	4
1.1. Legal framework	4
1.2. Aim	4
1.3. Target audience	5
1.4. Compliance	5
2. Policies	5
2.1. Policy for Customer Identification	5
1. Key principles of identity checking	5
2. Required information	6
3. Politically exposed persons (PEP)	9
4. Ultimate beneficial owners	10
5. Legal arrangements	12
6. Non-profit organisations (NPOs)	12
7. Exceptional procedure	13
8. Correspondent banking	13
9. Quality of required documents	14
10. Update and retention periods for records	15
2.2. Customer Acceptance Policy	15
1. Customers whose acceptance should be refused	15
2. Customers subject to conditional approval	16
3. Criteria for determining high level of risk	17
2.3. Analysis and Monitoring of High-risk Entities Policy	17
1. Procedures used in the analysis and monitoring of high-risk accounts	17
2. Opening of high-risk accounts	18
3. Occasional transactions	18
4. Risk management and execution of transactions	19
5. Enhanced active control actions	19
2.4. Policy for Reporting of Suspicious Transactions	20
1. Procedures	20
2. Time frame and forms of reporting	21
3. Formal participants in the reporting process	21
4. BCH's relationship with the customer	22
2.5. Policy for Training and Awareness on the ML and TF risks	23
BCH's Policy on Preventing and Combating ML/TF/FP Acknowledgement Form	24

1. INTRODUCTION

1.1. Legal framework

This document presents a set of policies aiming to prevent the use of Banco Comercial do Huambo for purposes of Money Laundering, Terrorism Financing and Proliferation of Weapons of Mass Destruction.

These policies are by no means exhaustive and are intended for use alongside a plethora of compliance tools and as part of a wider source system, which includes the Internal Procedures Manual, Internal Guidelines and the Code of Ethics and Business Conduct.

In alignment with general principles for preventing and combating money laundering, in compliance with national legislation as well as recommendations from relevant international entities, and taking into account the markets' best practices, BCH is committed to implementing policies, practices and procedures in order to avoid the institution being used for, or the target of, intentionally or otherwise, activities of criminal nature or bound to pose an operational or reputational risk to BCH.

This document was drafted in observance of the following legal documents:

- Law no. 05/20, from January 29 – Law on the Prevention and Combating of Money Laundering, the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction, which repealed Law no. 34/11, from December 12.
- Law no. 1/12, from January 12 – Law on the Designation and Implementation of International Legal Acts.
- Warning 14/20, by BNA, on June 22 – about the Rules for the Prevention and Combating of Money Laundering and the Financing of Terrorism, which repealed Warning 22/12, from April 13.
- Presidential Decree no. 212/13, from December 13 – approval of the organic statute of the Financial Information Unit.
- Law no. 3/14, from February 10 – Law on the criminalization of money laundering offences.
- Law no. 11/24 from July 04 – Law that changes the Law no. 05/20 on the Prevention and Combating of Money Laundering, the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction.

1.2. Aim

This document aims to establish a set of criteria and procedures to guide BCH in combating money laundering, the financing of terrorism and the proliferation of weapons of mass destruction, as well as in complying with regulatory measures.

1.3. Target audience

All of BCH's employees must comply with the policies herein. It is each BCH employee's duty to, in their daily operations and within their scope of duty, bear in mind, and act in accordance with, national and international legislation regarding ML and FT.

1.4. Compliance

All of BCH's employees must read and understand BCH's Policy for Preventing and Combating Money Laundering, the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction – and sign the Policy's Statement of Acknowledgement. Any arising omissions must be referred to BCH's Compliance Department so that appropriate measures for dealing with exceptions can be taken.

Employees who, intentionally or otherwise, disrespect BCH's Compliance Policies will incur penalties established by BCH's Internal Rules and Regulations and risk criminal proceedings for crimes under Law no. 11/24, from July 04.

2. POLICIES

2.1. Policy for Customer Identification

Aim: To determine what identity data is required from customers, their representatives and ultimate beneficial owners in order to allow for the correct application of the Policy for Customer Acceptance, as well as subsequent monitoring.

1. Key principles of identity checking

Before accepting a customer, BCH demands a full identity check on the customer as well as their respective representatives and/or ultimate beneficial owners.

The Policy for Customer Identification is based on the following key principles:

- The truthfulness principle:
All data provided to BCH must be assessed on the premise that they are neither purportedly false nor seek to conceal the truth.
- The verifiability principle:

All data provided by the customer must be supported by sufficient compulsory documents in order for the process to be proven truthful and verifiable.

- The differentiation principle:

Information required by BCH is specific to the nature of the entity (natural person or legal entity) with whom the bank intends to establish a business bond and to each entity's different characteristics, which influence risk assessment for money laundering, the financing of terrorism and the proliferation of weapons of mass destruction.

- The validity principle:

Both at the beginning and throughout the business relationship, the documents intended to prove the validity of the required information, provided by the customer in the process of identity checking, must be written and obtained in due time, that is, as closely dated to the act and to the information they are intended to corroborate as possible.

Expired documents standing as proof will not be accepted, and all documents' expiry dates should be continuously updated, except otherwise established by law.

2. Required information

National legislation (in agreement with international best practices) establishes a set of identity-checking rules that must be integrated into the daily operations of all BCH employees, and strictly followed when customer identification is paramount.

In internal regulations, and in line with legislation currently in force, BCH establishes what information needs to be provided by each type of customer at the beginning, and to be updated throughout, the business relationship.

Different requirements apply to natural persons and legal entities, and within those two groups, to nationals and non-nationals, to those in exceptional circumstances (for instance, the Politically Exposed Persons, public limited companies, privately held companies and fiduciary entities established in offshore jurisdictions or otherwise) and to the verification of ultimate beneficial owners of legal entities, when applicable.

Therefore, the required information for identity checking customers in different categories is detailed below, exhaustively and in line with rules of procedure:

Natural Persons

In the case of natural persons, BCH must obtain all relevant information from the customer in order to ascertain their trustworthiness before establishing, and subsequently maintaining, a business relationship:

- i) Full name and signature;

- ii) Date of birth;
- iii) Nationality;
- iv) Taxpayer number;
- v) Marital status;
- vi) Full address, or other contact details considered valid by BCH;
- vii) Occupation and employer, when applicable;
- viii) Any public offices held;
- ix) Type, number, date and issuer of identity document.

BCH must also gather clear and truthful information about:

- i) The purpose of the business relationship to be established;
- ii) The source and destination of the funds to be moved;
- iii) The customer's sources of income, namely their nature and estate, to ensure their lawfulness;
- iv) The customer's expected transaction profile, so as to assess their respective money laundering risk rating and suitability according to the Policy for Customer Acceptance.

In order to verify the customer's identity, in the strictest sense, the customer must present an original, valid and pre-signed form of photo identification containing their full name, signature, address, date of birth and nationality.

If deemed necessary, for customers and transactions which, due to their nature or characteristics, pose a greater money laundering or terrorism financing risk, BCH will apply a set of special procedures and strengthen the Know Your Customer guidelines and monitoring processes. These measures apply to situations such as establishing business relationships or running operations long-distance, as well as to business relationships with Politically Exposed Persons (PEP).

Legal Entities (all types)

Equally, in the case of legal entities, the customer must provide BCH with all relevant information in order to be proven trustworthy before establishing, and subsequently maintaining, a business relationship. BCH must also obtain information and substantiating documentation to identify the entity's ultimate beneficial owner and determine the entity's ownership and control structure and any links with other BCH customers.

BCH must, to this end, obtain the following information:

- i) Full company name;

- ii) Corporate purpose;
- iii) Address – headquarters, management activities centre, representative office, stable facility - Registered office address, representative office, permanent establishment and/or any other address of the main locations where the activity is carried out
- iv) Legal Entity Identifier (LEI);
- v) Company registration number;
- vi) Identity details shareholders owning share capital and voting rights shares of 20% or over;
- vii) Identity of management assignees, procurators and respective mandate;
- viii) Copy of the trust agreement, articles of incorporation or other equivalent document;
- ix) Other reliable information that is publicly available considered relevant.

In these situations, it is particularly important to identify, and validate through supporting documentation, ultimate beneficial owners (natural persons), drawing on both corporate and personal documentation – in the latter case, following similar procedures to those applied to natural persons. The required elements sole traders must provide before a business relationship is established are the following: tax identification number; full company name; head office address and corporate purpose, as well as the natural person's identification details.

BCH must also obtain clear and truthful information about:

- i) The purpose of the business relationship to be established;
- ii) The source and destination of the funds to be moved;
- iii) The customer's sources of income, namely their nature and estate, to ensure their lawfulness;
- iv) The customer's expected transaction profile, so as to assess their respective money laundering risk rating and suitability according to the Policy for Customer Acceptance.

In order to verify, in the strictest sense, the identity of legal entities, BCH must obtain the legal entity's tax identification number, its respective company registration number, publication in *Diário da República* (or equivalent government gazette from other jurisdictions), permit and a valid license issued by the competent body – or equivalent documents for non-resident entities.

In order to check the identity of holders of share capital and voting rights of the legal entity totaling 20% or over, the minutes of the constituent General Assembly, as well as minutes of any alteration in partner or shareholder structure, must be provided.

If deemed necessary, for customers and transactions which, due to their nature or characteristics, pose a greater money laundering or terrorism financing risk, BCH will apply a set of special procedures and strengthen the Know Your Customer guidelines and monitoring processes.

When conducting Enhanced Due Diligence, in order to confirm the veracity of the information obtained from legal entity representatives, BCH may also draw on complementary sources such as commercial information services, lawyers, independent and open-access databases, bank references, visits to the legal entity's facilities or other sources considered adequate and reasonable.

Simultaneously, BCH must verify the identity and reputation of any entity seeking to establish a business relationship in representation of a legal entity, while also confirming the veracity of any supporting documentation attesting to their rightful representation.

Procurators and legal representatives

BCH must check the identity of representatives and confirm the legality of their representational roles. In order to do that, BCH must obtain the following information:

- i) Written statement declaring that the representative is legally authorized to act on behalf of the customer, and clearly mentioning their scope of activity.
- ii) Valid and pre-signed form of photo identification containing their full name, signature, address, date of birth and nationality.

3. Politically exposed persons (PEP)

Law no. 05/2020 defines politically exposed persons as national or non-national individuals who hold or have held prominent public offices in Angola, or in any other country, jurisdiction or international organisation, namely:

- i) High-ranking political or public positions (President or Head of State; Vice-President; Prime Minister or Head of Government; Subsidiary Bodies or Members of Government, namely Ministers of State, Secretaries of State, Vice-Ministers and other comparable roles; Deputies, Members of Legislative Chambers and other similar positions; higher courts and Court of Appeal Magistrates whose decisions cannot be appealed, bar exceptional circumstances; Public Prosecution Service Magistrates on par with aforementioned magistrates; Ombudsperson and Deputy Ombudsperson; Members of the Council of State, the National Security Council and other State Counsellors; Members of the National Election Commission; Members of the Higher Councils of Magistracy and Public Ministry; Members of Management and Supervisory Bodies of Central Banks and other authorities for the regulation and supervision of the financial sector; Heads of foreign missions and consular posts; General Officers of the Armed Forces and Commissary Officers of Security Forces and Internal Security; Members of management and supervisory bodies of public companies as well as exclusively or predominantly public limited companies, public institutions, public societies and public establishments of all types, including management of companies from local business sectors; Members of the Board of Directors, directors, deputy directors and/or individuals holding similar roles in international organisations; Members of political parties'

executive bodies; Members of local and regional government; Leaders of religious denominations;

- ii) Close family members and other people closely related to PEPs, namely: their spouse or non-marital partner, relatives up to the 3rd degree in the collateral line, kinship by affinity up to the same degree, their respective spouses or non-marital partners; known and close personal connections; known and close corporate and business connections (joint owner of a legal PEP or close business connections);
- iii) Any natural person who owns the share capital or voting rights of a legal entity, or who owns assets pertaining to a well-known unincorporated association for collective interests, the sole beneficial owner of which is the PEP.

Whenever such status is determined at the beginning of a business relationship, as it progresses or before any operation, BCH must:

- i) Question the customer in order to determine if they can be considered a PEP, in accordance with the Law and with Know Your Customer procedures;
- ii) If a PEP is confirmed, ensure an Enhanced Due Diligence process is carried out, so as to obtain detailed information about the source of any involved assets and funds, requesting clear statements regarding:
 - a. the reason for opening the account;
 - b. the source of the funds;
 - c. the exact value of the assets to be deposited in BCH;
 - d. declaration of income.

If, throughout the business relationship with BCH, the customer becomes a PEP, the manager must re-recategorize the customer's "KYC" document as "PEP".

Before opening the PEP's account, the BCH branch must seek advice from the Head of Compliance and obtain an approval from the Board of Directors, and subsequently register the customer in the system under the "PEP" classification.

Due to an increased risk of ML or FT with certain types of transactions, PEPs are subject to enhanced continuous monitoring by BCH throughout their business relationship.

4. Ultimate beneficial owners

The ultimate beneficial owner (UBO) is the person on whose behalf a transaction or activity is carried out, or who holds an economic interest in the transaction or activity – or, ultimately, who owns the share capital or controls the customer's voting rights.

National Law makes it compulsory to identify ultimate beneficial owners – when they exist – and to obtain information that allows full knowledge of the structure of the asset, the scope of control of the legal entities and the identity of the natural persons who own the asset or ultimately control the entity.

The following procedures must be followed:

A. Gather the required information

The identity of the UBO of an entity, deposit account, business arrangement or transaction must be checked as though they were the account holder themselves. They must provide the required documents and supporting documentation, following the same procedures as those applicable to entities seeking to establish a relationship with BCH.

After gathering the required information, the natural person(s) standing as Ultimate Beneficial Owner(s) of the legal entities concerned and the nature and scope of their relationship must be registered.

- **Natural Persons**

Verify the identity of the UBO as though they were a deposit account holder or the counterparty in a business relationship. They must provide certified supporting documentation to all required identification elements;

- Full name and signature;
- Date of birth;
- Nationality;
- Taxpayer number;
- Marital status;
- Full address, or other contact details considered valid by BCH;
- Occupation and employer, when applicable;
- Any public offices held;
- Type, number, date and issuer of identity document.

Legal Entities

- i) Company's statement containing the identity details of any natural persons owning 20% or more of the share capital or voting rights (full name, address, date of birth, identity document or passport and tax identification number);
- ii) Minutes of the constituent General Assembly, as well as minutes of any alteration in partner or shareholder structure;
- iii) In the case of companies owning 20% or more of the share capital or voting rights, the required information must be gathered as above up to the point of identifying Ultimate

Beneficial Owners, who are intrinsically natural persons and must provide the aforementioned statement.

- iv) Copy of the trust agreement, articles of incorporation or other equivalent document;
- v) Other reliable information that is publicly available considered relevant.

B. Refusal to provide identity details of the Ultimate Beneficial Owner

If the customer refuses to provide identity details regarding the Ultimate Beneficial Owner(s), the account manager must suspend the account opening process, inform the prospective customer and report the incidence to the Compliance Department.

5. Legal arrangements

For trusts or other similar legal arrangements, which administer or distribute funds, the following should be identified:

- i) The beneficiaries of at least 20% of their assets, when the future beneficiaries have already been determined;
- ii) The natural persons in whose main interest the legal person is set up or operates, when the future beneficiaries have yet to be determined;
- iii) The natural persons who exercise control over 20% or more of the assets of the legal person;
- iv) The natural persons who set up the trust (settlers).

6. Non-profit organisations (NPOs)

The non-profit organisations have characteristics which put them at risk of money laundering and terrorist financing abuse.

NPOs have access to considerable sources of funds and are often cash-intensive, which makes it sometimes impossible to immediately verify the source of their funds.

Furthermore, as most NPOs have a global presence, and given the nature of their activity, NPOs necessarily carry out national and international operations near areas exposed to terrorist activity.

For these reasons, with regard to this type of customers, BCH adopts the following procedures in order to assess if the NPO's activity is consistent with its object, structure and operations:

- i) Identifies the geographic location and organizational structure;
- ii) Analyses the nature of the donations and destination of funds;
- iii) Identifies the managers (or equivalent) and the beneficial owners of the operations;
- iv) Analyses the nature and object of the organisation's activities.

7. Exceptional procedure

The verification of the customer's identity must be carried out at the time of the establishment of the business relationship, or in advance, especially in the case of transactions.

In some exceptional situations, in which there is no proven risk of money laundering or terrorist financing, or these risks are low, BCH admits the following possibilities:

- i) Opening an account without completed identification process, within the thresholds provided by law:

In these situations, the accounts are open with total blocking of debit and credit movements, after the initial deposit, with no means of payment made available, nor changes in ownership allowed.

These restrictions will only be lifted after a successful conclusion of the customer due diligence and Know Your Customer process, which must be carried out in the shortest period of time, that is, within 15 days from the outset of the business relationship.

- ii) Transactions carried out over the internet:

The electronic forms, regardless of the transaction amount, identify the beneficiary of the transaction, account number, the beneficiary financial institution and the reason for the transaction.

8. Correspondent banking

BCH is not a "correspondent bank" for any other bank, that is, it does not act as an agent or channel for another bank for the execution of banking transactions for customers of that institution.

Should this happen, BCH will take the necessary measures in accordance with existing good practices, regarding the establishment or maintenance of relationships with correspondent banks, by developing specifically defined procedures, in order to ensure the necessary due diligence in relation to these entities.

- i) Gather sufficient information about the respondent bank to understand fully the nature of its activity and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to regulatory action or investigation related to money laundering, terrorist financing or the financing of the proliferation of weapons of mass destruction;
- ii) Assess the respondent institution's AML/CFT/CFP controls;

- iii) Obtain approval from the Board of Directors before establishing new correspondent relationships.

Regarding services provided within cross-border correspondent banking relationship, identified as high risk, BCH, as respondent bank, must:

- i) Know the full path of the funds it entrusts to its correspondents, from the moment they are delivered by the originators of the operations until the moment they are made available, in the country or jurisdiction of destination, to the respective final beneficiaries.
- ii) Know all participants in the transaction path, ensuring that only entities or persons duly authorized to process the transfer of funds by the competent authorities of the countries and jurisdictions involved, intervene in the transaction.
- iii) Develop mechanisms to periodically review and update information on the correspondent institution in question, and to verify its reputation in the market, through analysis of publicly available information.
- iv) Obtain and keep the documentation that attests the fulfilment of the provisions of the previous paragraphs, which must be placed, whenever necessary, at the disposal of the competent authorities.

9. Quality of required documents

Supporting evidence of identification data as defined by the legislation and applicable internal regulations must consist of original documents, which are originally issued by the competent authorities or certified copies, issued by authorised entities or public officials.

For natural persons, at least one official identification document, with clear photograph and signature must be presented as evidence of identity (Angolan identity card, resident card or passport) which is subject to verification by the employees of BCH who receive it.

In case of documents originating outside the country in which BCH operates and where they are presented, enhanced measures must be taken in the analysis of their veracity and nature. The submitted documents must be original or, as with national documents, certified copies, provided by official authorities in this field.

The bank shall not accept, under any circumstances, documents presenting erasures, defects or visible damage in fundamental parts or which, for any reason, may suggest forgery or violation of identifying elements.

With regard to documents in non-Latin script, a transliteration of their content in Latin script should be requested, if there is no other way of proving the elements contained in those documents.

Overall, if there are doubts about the veracity or quality of the presented documents, the customer identification procedure should be considered invalid, until the Compliance Department agrees to the continuation of the process.

10. Update and retention periods for records

BCH undertakes periodic updates of the information and respective supporting documents every 5 years, at the most, with regard to customers classified as low-to-medium risk of ML/TF, and whenever the bank is aware of:

- i) The expiration of a document;
- ii) A fact or an event that alters the situation of the customer, evidenced by the documents previously in its possession;
- iii) Arising doubts as to the precision of the existing data on record.

Customers classified by BCH as high risk of ML/TF are subject to continuous monitoring, thus information should be updated annually.

Within the scope of the applicable legislation, BCH retains the records referred to in this policy for a period of 10 years from the date of the transaction or after the end of the business relationship.

Copies of documents or records related to the training provided to BCH employees under ML/TF/PF are also retained for a period of 5 (five) years.

2.2. Customer Acceptance Policy

Objective: Define criteria that will serve as guidelines for BCH to accept or not engage in relationships with potential customers; define criteria for conditional approval of customers; also define criteria for classification of the level of risk associated with the customers at the outset.

1. Customers whose acceptance should be refused

In order to protect BCH from practices that may put its activity at risk and so as to protect its reputation, BCH does not accept customers that fall into any of the following categories:

- i) Persons whose reputation, in the media or in the market, is usually associated with criminal activities.

- ii) Persons whose activity or source of income is, directly or indirectly, the arms trade, or other equipment of a warlike nature or purpose;
- iii) Persons in relation to whom BCH has grounds to believe that are linked to criminal activities;
- iv) Persons who do not collaborate with BCH in providing the required information or who provide fictitious information;
- v) Shell banks (banks that have no physical presence in the country in which they are incorporated and licensed, and which are unaffiliated with any financial group that is subject to effective and consolidated supervision. BCH demands each bank to submit a valid and proper document that proves the physical location of its headquarters and that it has no relationships with shell banks).

Regarding entities whose acceptance as a customer is refused, BCH implements a non-acceptance process that includes all the information collected about the entity, as well as a statement of the reasons that led to the non-acceptance. It is then filed to the BCH's Compliance Department, which will consider, in view of the information received, possible subsequent actions within the scope of the applicable legislation.

2. Customers subject to conditional approval

Customers who fall into any of the following categories need special authorization:

- i) Persons whom BCH has classified as presenting higher level of money laundering risk;
- ii) Persons whose activity or way of life makes it impossible or difficult for BCH to know the origin of their wealth;
- iii) Casinos, gambling entities or other of similar nature, provided they are authorized by a state in matters relating to anti-money laundering and terrorist financing.
- iv) Currency exchange bureaus or any other establishments that carry out domestic or cross-border currency trading;
- v) Politically exposed persons (PEPs).

The conditional approval process covers the cases in which the potential customer is a manager, shareholder or owner of any entity that pursues any of the above-mentioned activities.

A potential customer who falls under any of the conditions referred to above will always be expressly warned of the condition governing his/her acceptance by BCH.

For these situations, BCH creates a special acceptance process for potential customers.

The decision to accept or refuse a customer shall be adopted by BCH on a proposal from the Commercial Director to the Compliance Department of which the Board of Directors must be informed.

3. Criteria for determining high level of risk

Classifying potential customers as high risk upon acceptance is carried out by the Compliance Department, according to the following relevant factors:

- i) If the geographical area of residence or operation of the potential customer or the origin/destination of the transaction funds is in countries:
 - Subject to embargoes or sanctions imposed by any entities with international legal standing and competence in the matter;
 - That cannot be ranked, in terms of money laundering or terrorist financing.
- ii) Customers whose acceptance is subject to a special authorization process (section 2 above);
- iii) The activity/profession of the potential customer is subject to anti-money laundering legislation:
 - Financial Institutions;
 - Casino concession holders; lottery enterprises;
 - Entities engaged in real estate brokerage activities;
 - Merchants transacting goods which involve cash payments of over USD 15,000.
 - External auditors and chartered accountants, auditors, tax advisors; notaries, registrars, lawyers or solicitors, when they intervene on behalf of the customer.
- iv) The presence of other factors and circumstances as defined by the Compliance Department.

2.3. Analysis and Monitoring of High-risk Entities Policy

Objective: Define the set of criteria that should guide BCH on the procedures of acceptance, analysis and monitoring of accounts, considered to be high risk and which require enhanced due diligence or application of enhanced ongoing monitoring measures.

1. Procedures used in the analysis and monitoring of high-risk accounts

The procedures followed by BCH are based on methods for the control and prevention of risks related to ML, TF and PF, which simultaneously contribute to the reduction of the risk of fraud, while also reducing potential financial losses.

Thus, for customers classified as having a high risk of ML, BCH:

- i) Defines in its Customer Acceptance Policy, categories of customers for whom the opening of an account or its maintenance should be refused or subjected to a special authorization process.

These must be submitted to a KYC process with detailed information, requiring prior authorization from a senior level;

- ii) Requires prior confirmation by the Compliance Department of the documentary compliance of the account opening, Customer Due Diligence and Know Your Customer (KYC) process;
- iii) Uses monitoring processes through alerts issued by the system in order to monitor situations considered to be of high risk;
- iv) Allows any employee to inform the Compliance Department about situations or transactions with a high level of suspicion, particularly in the case of high-risk entities. The information in this compilation and its consultation is available only to employees of the Compliance Department.

Most of the monitoring and control activities are performed by the Compliance Officer's team which has access to any type of information on BCH. Following the monitoring and control actions, recommendations to the Board of Directors are issued, whenever appropriate, which are properly dealt with for the purposes of execution control.

2. Opening of high-risk accounts

As part of the assessment and prevention of the aforementioned risks is based on the ongoing monitoring of the customer and the customer's activities, BCH establishes that all applicants for an account whose risk is considered to be high shall be submitted to the Compliance Department's pre-validation.

In these cases, and prior to opening an account, analysis of the documentary compliance as well as of the Due Diligence/Know Your Customer process must be carried out, with the opening of the account deemed suspended until all these elements are validated and approved.

In the case of PEP and beneficial owners, compliance also involves ensuring the conformity of the respective entry into the computer system, in order to guarantee the set of consequences that these ranks have on the classification and monitoring system.

Failure to obtain or refuse to supply the elements deemed necessary, should determine the BCH's refusal to accept the commercial relationship, and the occurrence should result in a thorough analysis process to be submitted to the Board of Directors for approval.

3. Occasional transactions

The Angolan law defines as occasional, the transaction that is carried out by the Bank outside the scope of an already established business relationship, characterized precisely by its expected casualness, regardless of the specific number of operations.

Banco Commercial do Huambo defined and implemented the non-acceptance of occasional transactions, considering that these transactions are characterized by their high level of MLTF risk, namely resulting from:

- Difficulty in verifying the beneficial owner(s) or the person acting on their behalf;
- Difficulty in determining the origin of the declaration of assets and funds involved in the transaction;
- Difficulty in monitoring the transaction.

Therefore, it is not allowed nor it is possible for third parties that have not established a business relationship with the Bank to execute any transactions. BCH ensures in its internal procedures and in the use of technological means that these transactions cannot be executed.

4. Risk management and execution of transactions

The detected transactions which non-conformity is not justified or where there are relevant indications or suspicions of crime, should result in BCH, regardless of other measures, taking immediate action on the account and on the customer.

The actions to be taken include, without prejudice to other appropriate measures:

- i) Suspension of the transaction, the execution of which is conditional upon its examination, with a view to obtaining elements that justify its possible conformity;
- ii) Placement under a special monitoring process, allowing greater control over the transactional flows that may occur;
- iii) Adding the entity to the internal list, which will allow greater control over the completion of future transactions, namely international transactions.

Also, when there is a proposal for the acceptance of potential customers and in accordance with the Customer Acceptance Policy:

- i) The opening of an account to customers specified in that document should be refused;
- ii) It must be suspended until a special approval is obtained from the Compliance Office, regarding customers who should be subject to conditional approval.

5. Enhanced active control actions

BCH defines a set of procedures that aim to ensure enhanced ongoing monitoring of entities considered to be at high risk. In addition to the situations listed above, whenever it becomes aware through reliable sources of information, within the scope of preventing and combating money laundering and terrorist financing and in order to preserve and defend its reputation, BCH reserves the right to, among other possible actions:

- i) Suspend transactions for which there are significant doubts as to their legitimacy or compliance, and do not proceed with their execution until the conditions deemed necessary are met;
- ii) Undertake enhanced diligence and scrutinise transactions, requesting supporting evidence of the presented economic justification, proceeding to its refusal in the event that the information and documentation deemed necessary are not provided;
- iii) Proceed to the return of transactions to their origin whenever the bank considers that the conditions of legal or regulatory compliance are not met, as well as those, the context of which it may perceive as jeopardizing to its reputation.
- iv) Refuse the execution of transactions in which it believes that principles and values generally accepted by the financial system are being violated.
- vi) Communicate to the competent authorities any suspicious transaction or situation, whenever the evidence that contributed to the formation of this conviction is not cancelled out by the information or documentation provided by the customers.

2.4. Policy for Reporting of Suspicious Transactions

Objective: Define a set of procedures for reporting of suspicious transactions

1. Procedures

If there are reasonable grounds to suspect that a customer or potential customer is using or intends to use BCH's products or services to launder proceeds of crime or to finance terrorism, the following procedures are followed:

- i) These transactions or activities will be reported by employees or their respective departments to the Compliance Department, which is responsible for their in-depth analysis;
- ii) While the analysis is taking place, any activity related to that customer must be reported to the Compliance Department;
- iii) The Compliance Department assesses the analysed processes and decides whether there is a basis for reporting possible suspicious transactions.

Within the scope of Law 05/20, BCH must also report to the Financial Intelligence Unit, all cash transactions, equal to or greater than, in national currency or another currency, the equivalent of:

- a) USD 15 000 (fifteen thousand American dollars);
- b) USD 5 000, when exchanging low denomination banknotes for high denomination ones;
- c) USD 5 000, when the exchange involves different currencies;
- d) USD 5 000, when a customer buys and/or pays checks, traveller's checks or similar payment methods;
- e) USD 5 000, when involving securities;
- f) USD 5 000, when they satisfy two or more of the following indicators:
 - i. Uncounted amounts;
 - ii. In foreign currency;
 - iii. Not deposited in own account;
 - iv. Which are transferred to an account abroad;
- g) USD 5.000, when related to a specific country or jurisdiction subject to additional countermeasures by the Angolan State, competent international organizations or supervisory and inspection authorities.

2. Time frame and forms of reporting

After deciding on the existence of grounds for possible suspicious transactions, BCH reports this fact to the BNA's Financial Intelligence Unit (FIU), using the Suspicious Transaction Report (STR) form. The transactions referred to in the paragraphs of section 1 must be immediately communicated to the FIU.

3. Formal participants in the reporting process

The following are formal participants in the suspicious transaction reporting process:

Commercial Department

The Commercial Department is responsible for receiving the transaction and making a pre-analysis of it. If the Commercial Department considers that the transaction is part of a suspicious activity, it must immediately inform the Compliance Department, providing all the documentation related to the transaction and the reasons that led it to consider a suspicious transaction.

For all cash transactions, equal to or greater than the equivalent, in national currency of USD 15 000, the customer is requested by the Commercial Department to fill out a Declaration of Origin and

Destination of Funds, where he/she declares the reasons for carrying out a cash transaction instead of using other means of payment.

Compliance Department

The Compliance Department is responsible for analysing the transaction. After receiving the transaction that is indicated as being related to a suspicious activity, it validates the documentation received and proceeds to its analysis, in accordance with the bank's internal rules and legislation in force.

If the Compliance Department considers that this is a suspicious transaction, it must place alerts in the internal system, and subsequently the Compliance Officer must report it to the Financial Intelligence Unit, by completing the Suspicious Transaction Report (STR).

For the process of reporting suspicious transactions, BCH has an AML solution integrated into the bank's core computer system that allows:

- Extraction of the Suspicious Transaction Report (STR): for situations where there is suspicion of a suspected ML/TF transaction.
- Extraction of the Declaration of Identification of Designated Persons (DIDP): for situations in which the entity is subject to a sanction or investigation;
- Extraction of the Declaration of Cash Transactions (DCT): for situations in which transactions are carried out in amounts equal to or greater than the equivalent of USD 15,000.

4. BCH's relationship with the customer

During identification and identity verification, customers will not be alerted to the fact that an internal reporting is taking place or that a suspicious transaction declaration has been filed, as it may jeopardize future efforts on the part of the competent authorities.

BCH and its employees do not, at any time, disclose the suspicious activity processes submitted for the Compliance Department's consideration and/or the STR submitted to the FIU.

This obligation of secrecy is maintained in relation to the customer and third parties and the disclosure of the identity of the person who reported information on suspicious transactions is a crime, within the scope of Law 05/20.

2.5. Policy for Training and Awareness on the ML and TF risks

Objective: Ensure the compliance of the bank with the legal framework and develop a company culture, by increasing the sense of responsibility of all employees regarding the risk of ML and TF.

A continuous training program on ML and TF Prevention has been implemented for all BCH employees. This program covers the measures and procedures necessary to ensure the prevention of ML and TF, namely, the steps necessary to identify suspicious transactions.

This program covers all employees of BCH and is provided in bespoke training sessions to small groups, with relevance to certain matters depending on the department. The training program includes in-room training by in-house trainers, namely people with high level of experience and training in the field.

The program aims to raise the awareness of all employees in order to allow that when faced with suspicious situation which is highly probable to constitute a crime of ML, TF or PF, the legal provisions to which BCH is bound are complied, by seeking advice from respective senior level and the Compliance Department on the procedures to be followed.

Employees also receive training on how to conduct due diligence procedures, namely, the precautions to be taken to prevent customers from becoming aware of the referred diligence.

At the end of each year, together with the Human Resources Department, the Compliance Department prepares the ML/ TF training calendar for the following year and sends it to all employees to inform them of the times and dates the training is to be held, while the presence of all is mandatory.

BCH's Policy on Preventing and Combating ML/TF/FP Acknowledgement Form

I, _____, a holder of an ID card n° _____, employee of BCH, with Personnel N° _____, hereby declare that I acknowledge and agree to the following:

1. To be alert to all situations that, within the scope of ML and TF, may give rise to a suspicious transaction.
2. I undertake not to disclose to customers or third parties that any information about the customer or beneficiaries has been reported, or that a criminal investigation is underway.
3. I declare that I have obtained access to a copy of the BCH's Policy on Preventing and Combating Money Laundering, the Financing of Terrorism & Proliferation of Weapons of Mass Destruction, I have read, understood and understand how this information impacts my work.
As a condition for the continuity of my employment contract, I agree, without restrictions, with the policies contained in that document. I understand that non-compliance with the policies may give rise to administrative measures, internal disciplinary actions and I will be subject to the applicable penalties or labour, civil or criminal sanctions provided for in the laws in effect for this purpose.
4. I agree to report all situations that may give rise to reasonable grounds for suspicion within the scope of ML, TF and PF, to my hierarchical superiors and to the Compliance Department.
5. Ensure compliance with the legal provisions imposed on BCH and protect its reputation.

I declare that I have read and understood the Acknowledgement Form of BCH's Policy for Preventing and Combating Money Laundering, the Financing of Terrorism & Proliferation of Weapons of Mass Destruction, so I sign it in two copies, of my own free will, in agreement with its content.

Signature: _____

Date: _____ / _____ / _____